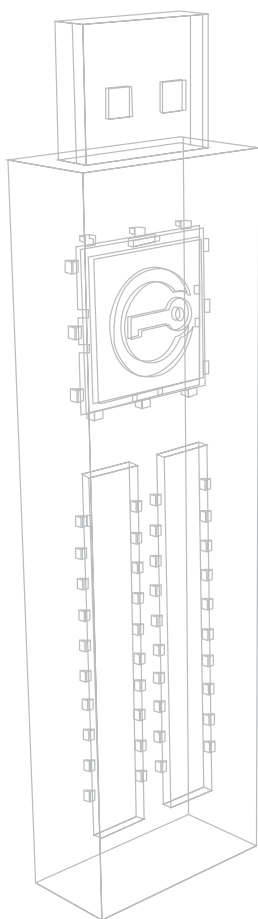


IronKey Personal

Руководство пользователя
Модели: S200, D100, D200



Не используйте русские символы для пароля (их использование приводит к невозможности разблокировать устройство).



БЛАГОДАРИМ ВАС ЗА ПРИОБРЕТЕНИЕ ПРОДУКЦИИ IRONKEY

Наша продукция – результат долгих исследований и миллионов долларов, инвестированных в разработку.

Наша цель – сделать технологии безопасности простыми в использовании и доступными широкому кругу пользователей.

Для краткого обзора возможностей продукта вы можете ознакомиться с материалами на сайте www.humansolutions.ru

Мы будем рады любым отзывам и предложениям.

Отзывы:

feedback@humansolutions.ru

ОГЛАВЛЕНИЕ

ЧТО ТАКОЕ IRONKEY?	4
Познакомьтесь с IronKey	4
Ключевые особенности	5
Изображения устройства	7
Средства обеспечения безопасности	8
Безопасность устройства	8
Безопасность сетевых служб IronKey	9
КАК РАБОТАЕТ IRONKEY?	11
Обзор устройства	10
Начало работы и инициализация IronKey в среде Windows	11
Работа с IronKey Unlocker для Windows	13
Начало работы и инициализация IronKey в среде Mac	14
Работа с IronKey Unlocker для Mac	15
Начало работы и инициализация IronKey в среде Linux	16
Работа с IronKey Unlocker для Linux	16
Работа с панелью управления IronKey Control Panel для Windows и Mac	18
Работа с виртуальной клавиатурой IronKey Virtual Keyboard для Windows	21
Работа со встроенным интернет-браузером Firefox и режимом Защищенных Сессий для Windows	22
Работа с IronKey Identity Manager для Windows	23
Работа с Secure Backup для Windows	25
Импортирование цифрового сертификата на накопитель IronKey в среде Windows	26
Работа с my.ironkey.com для Windows и Mac	27
Работа с накопителем в режиме чтения в средах Windows, Mac и Linux	29
Технические характеристики	31
ЧТО ДАЛЬШЕ?	32
Как получить дополнительную информацию?	32
Команда IronKey	32
Контактная информация	33

Что такое IronKey?

ПОЗНАКОМЬТЕСЬ С IRONKEY

Флэш-накопитель IronKey Personal – это самый безопасный USB-накопитель в мире, созданный для защиты пользовательских данных и обеспечения безопасного пребывания в интернете. Даже если накопитель потерян или украден, данным ничего не угрожает, и их можно восстановить на новом IronKey из зашифрованной резервной копии. При всей сложности и многообразии реализованных технологий, IronKey прост в использовании: для его разблокирования достаточно помнить пароль.



КЛЮЧЕВЫЕ ОСОБЕННОСТИ

Флэш-накопитель с аппаратным шифрованием данных IronKey может хранить 1, 2, 4, 8, 16 или 32 гигабайт пользовательских данных, будь то документы или приложения. Эти данные зашифровываются с помощью встроенного в накопитель крипточипа, который обеспечивает уровень защиты, применяемый к информации государственной важности, и не отключается никакими методами.

Механизм самоуничтожения

Крипточип отслеживает попытки физического воздействия на накопитель, и, в случае обнаружения таких попыток, запускает механизм самоуничтожения. Встроенный в крипточип счетчик попыток ввода пароля препятствует атакам по методу тотального перебора: после десяти неверных вариантов IronKey уничтожает данные по технологии «flash-trash».

Защита от запуска вредоносного программного обеспечения

IronKey защищает данные от вредоносного ПО, запускающегося по USB. Он предотвращает автоматический запуск неавторизованных программ, а при необходимости может быть разблокирован в режиме «только чтение».

Доступ к данным на различных платформах

Приложение IronKey Unlocker позволяет получить доступ к зашифрованным файлам на платформах Windows 2000, XP, Vista, Mac OS X и различных дистрибутивах Linux.

Простота управления

В комплект поставки IronKey входит программное обеспечение IronKey Control Panel, позволяющее запускать приложения, производить настройку и блокировать накопитель.

Безопасное восстановление данных

Приложение IronKey Secure Backup позволяет создать резервную копию данных, содержащихся на накопителе IronKey. В случае утраты накопителя, эти данные можно восстановить на новом IronKey, а также синхронизировать между несколькими IronKey.

Приватность доступа в интернет

Режим Безопасных Сессий IronKey обеспечивает безопасное нахождение в интернете вне зависимости от используемой сети (к примеру, при выходе в интернет через

незащищенную Wi-Fi точку доступа). Безопасный режим включается нажатием одной кнопки во встроенном браузере Mozilla Firefox.

Самообучающаяся система хранения паролей

Приложение IronKey Identity Manager предназначено для хранения и резервного копирования сетевых паролей. С его помощью авторизация в сетевых сервисах происходит автоматически, а пользователь получает защиту от фишинга и программ-клавиатурных шпионов.

Учетная запись на сайте my.ironkey.com

Сервис безопасного резервного копирования на портале <https://my.ironkey.com> позволяет восстанавливать забытые пароли, создавать резервные копии данных, отключать те или иные возможности устройства и т.д. Работа с сервисом осуществляется в безопасном режиме с двухэтапной авторизацией.

Хранилище данных учетных записей

Даже если накопитель потерян или украден, вы можете восстановить пароли и прочие данные учетных записей из зашифрованной резервной копии.



Водонепроницаемость и защита от внешнего воздействия

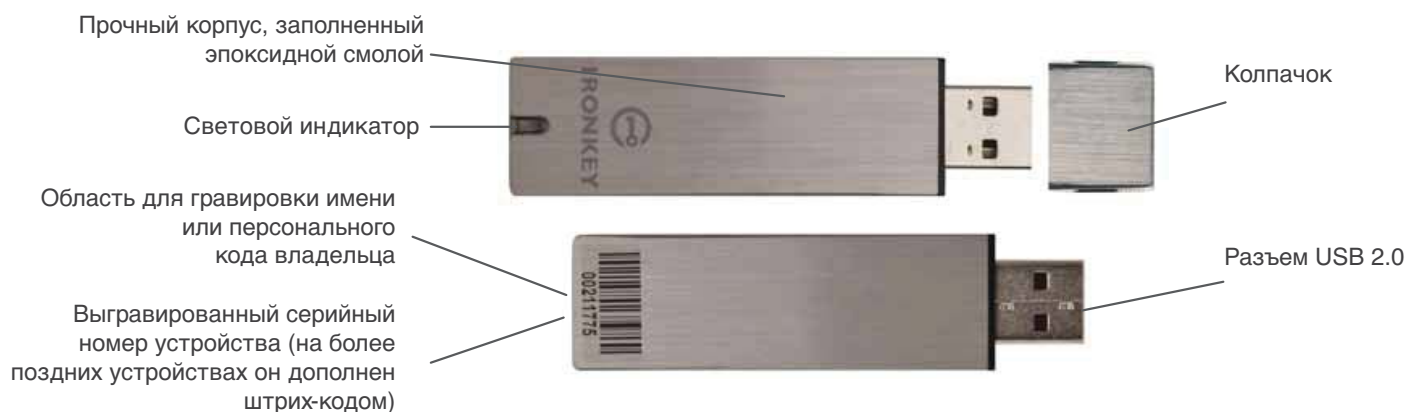
IronKey способен выдержать любые испытания. Сверхпрочный корпус накопителя заполнен эпоксидной смолой, что не только защищает его от вскрытия, но и обеспечивает водонепроницаемость по военному стандарту США MIL-STD-810F.

Соответствие стандартам Статьи 508 (США) для людей с ограниченными возможностями

Программное обеспечение IronKey Control Panel соответствует стандартам Статьи 508 (США). Для пользователей с ограниченными возможностями реализовано управление с клавиатуры и совместимость с программами для чтения экрана.

ИЗОБРАЖЕНИЕ СХЕМЫ УСТРОЙСТВА

Накопитель IronKey – это воплощение безопасности. Передовые технологии шифрования обеспечивают непревзойденную защиту данных, а крепкий корпус помогает предотвратить прямое вскрытие устройства и продлевает срок его службы. Если вы храните данные на IronKey, то можете быть абсолютно уверены в том, что они надежно защищены.



Крипточип IronKey выдерживает физические атаки, в том числе прослушивание шины данных и подмену защищенных данных или счетчика паролей. При обнаружении попытки физической атаки он уничтожает ключи шифрования, и зашифрованные файлы становятся недоступными.

САМЫЙ ЗАЩИЩЕННЫЙ USB-НАКОПИТЕЛЬ В МИРЕ



СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

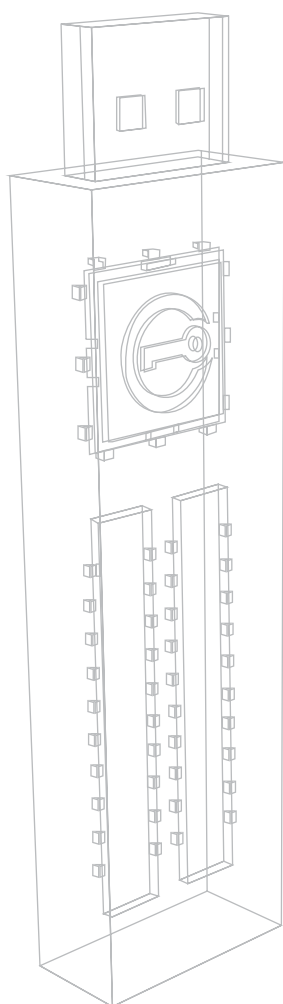
Компания IronKey стремится как можно подробнее освещать вопросы архитектуры и технологий, используемых в устройствах и сетевых сервисах. Мы используем проверенные криптографические алгоритмы, моделируем угрозы и проводим анализ систем безопасности с привлечением сторонних специалистов на этапах проектирования, разработки и внедрения.

БЕЗОПАСНОСТЬ УСТРОЙСТВА

Ключи шифрования данных

Ключи шифрования AES (улучшенный стандарт шифрования) генерируются аппаратным генератором случайных чисел.

- » Ключи генерируются и зашифровываются в момент инициализации устройства.
- » Ключи никогда не переносятся во флэш-память устройства или в компьютер.



Защита данных с механизмом самоуничтожения

- » Накопитель не определяется системой до момента установления подлинности пароля.
- » Счетчик попыток ввода пароля реализован в виде аппаратного модуля.
- » При превышении максимально допустимого значения счетчика все данные стираются с применением аппаратных средств.

Дополнительные средства безопасности

- » Данные передаются в накопитель по зашифрованному USB-каналу.
- » Микропрограмма накопителя и сопутствующее программное обеспечение обновляются через интернет в безопасном режиме.
- » Проверка подлинности обновлений осуществляется на аппаратном уровне.

Физическая защита

- » Прочный корпус.
- » Ключи шифрования хранятся внутри крипчипа.
- » Компоненты устройства окружены герметичным слоем эпоксидной смолы.
- » Устройство водонепроницаемо по военному стандарту США MIL-STD-810F.

Защита пароля IronKey

Пароль IronKey хешируется по алгоритму SHA-256 перед передачей на устройство, затем передается по защищенному USB-каналу и никогда не сохраняется во флэш-памяти, что делает его абсолютно недоступным. Проверка пароля осуществляется аппаратно (без использования функции типа «getPassword», которая возвращала бы его хеш-свертку), и только после проверки разблокируются ключи шифрования AES. Счетчик попыток ввода пароля также реализован аппаратно, что делает невозможными атаки, изменяющие значения счетчика в памяти. При превышении максимально допустимого значения счетчика запускается запатентованная аппаратная функция самоуничтожения «flash trash», которая гарантирует полное и бесследное уничтожение информации.

Защита Identity Manager

Приложение IronKey Identity Manager и сайт my.ironkey.com позволяют создать резервную копию паролей к сетевым учетным записям.

Для получения доступа к my.ironkey.com вы должны разблокировать IronKey посредством двухэтапной авторизации. Пароли безопасно хранятся в скрытой области устройства вне файловой системы и зашифрованы в два этапа. На первом этапе применяется 256-битный алгоритм AES, ключи которого генерируются на основе пароля к IronKey по алгоритму SHA-256. На втором этапе все данные дополнительно шифруются по 128-битному алгоритму AES. Это самая надежная защита паролей на сегодняшний день.

При создании резервной копии паролей IronKey проходит авторизацию в инфраструктуре IronKey на основе асимметричного шифрования с ключами RSA-2048. После успешной авторизации зашифрованный блок с паролями пересылается в защищенное резервное сетевое хранилище по протоколу SSL. Сетевые хранилища IronKey размещаются в высокозащищенных центрах сбора данных.

БЕЗОПАСНОСТЬ СЕТЕВЫХ СЛУЖБ IRONKEY

Защищенная инфраструктура

Сервера IronKey размещаются в самых передовых центрах сбора данных. Физический доступ к серверам защищен многоуровневой системой безопасности с применением сканеров отпечатков пальцев, шлюзовых кабин и идентификации по фотографии и личной учетной записи. Каждый центр оборудован камерами наблюдения, датчиками движения и сложными системами оповещения и находится под

постоянным контролем службы внутренней безопасности, работающей в режиме 24x7.

Сетевая безопасность

Доступ к сети IronKey контролируется многоступенчатой системой защиты на основе межсетевых экранов, маршрутизаторов, системы предотвращения вторжений и системы безопасности приложений. Сетевые службы и серверные приложения IronKey располагаются в отдельных сегментах сети с дифференцированными правилами и политиками безопасности.

Защищенные каналы связи и безопасность данных

Обмен информацией с интернет-сайтом и сетевыми сервисами IronKey проходит по зашифрованному каналу, безопасность которого реализована на базе протокола SSL и сертификатов Verisign Secure Site и Verisign Secure Site Pro. Для дополнительной защиты сервисов используется режим расширенного подтверждения SSL. Перед передачей по сети и сохранением в базе данных вся информация зашифровывается.

Режим Защищенных Сессий и усовершенствованная сеть Tor

Инфраструктура Защищенных Сессий представляет собой сеть высокопроизводительных Tor-серверов, изолированных от общедоступной сети Tor. Использование собственных серверов служит двум целям:

- 1.** Контроль над «точкой выхода» зашифрованной цепочки Tor осуществляется компанией IronKey, что обеспечивает защиту трафика от шпионского и рекламного программного обеспечения. Общедоступные точки выхода Tor не гарантируют такой защиты.
- 2.** Общедоступные точки выхода Tor могут использоваться злоумышленниками для скрытого перенаправления трафика. Точка выхода IronKey имеет защиту DNS, что является дополнительной антифишинговой и антифарминговой мерой безопасности.



Как работает IronKey?

ОБЗОР УСТРОЙСТВА

Персональный USB-накопитель IronKey использует в работе следующие приложения и сервисы:

- » Приложение IronKey Unlocker (для Windows, Mac и Linux)
- » Панель управления IronKey Control Panel (для Windows и Mac)
- » Виртуальная клавиатура IronKey Virtual Keyboard (только для Windows)
- » Интернет-браузер Mozilla Firefox и приложение IronKey Secure Sessions (только для Windows)
- » Приложение IronKey Identity Manager (только для Windows)
- » Приложение IronKey Secure Backup (только для Windows)
- » Портал my.ironkey.com (Windows и Mac)


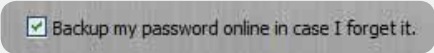

СИСТЕМНЫЕ ТРЕБОВАНИЯ:

- » Компьютер на базе Windows 2000 (SP4), XP (SP2+), Vista, 7, Mac OS X (10.4+) или Linux (2.6+)
- » Порт USB 2.0 для высокоскоростной передачи данных
- » Адрес электронной почты и соединение с сетью Интернет для доступа к сетевым службам.

НАЧАЛО РАБОТЫ И ИНИЦИАЛИЗАЦИЯ IRONKEY В СРЕДЕ WINDOWS

В комплекте поставки IronKey содержатся USB-накопитель IronKey и краткое руководство пользователя. Для инициализации IronKey выполните следующие шаги:

	Шаг	Описание
1.	Вставьте накопитель в свободный USB порт компьютера	Накопитель IronKey может работать на компьютерах под управлением Windows 2000, XP, Vista и 7, а также на компьютерах Mac и в системе Linux. Для высокоскоростной передачи данных используйте порт USB 2.0.
2.	Появится экран программы «Initialize Your IronKey»	IronKey автоматически запускается в режиме виртуального CD-дисковода. Экран может не появиться, если в системе отключен автозапуск USB устройств. В этом случае вы можете открыть диск IronKey Unlocker двойным щелчком мыши и запустить файл IronKey.exe


3.	<p>Задайте название устройства и пароль для доступа:</p> 	<p>К учетной записи IronKey может быть привязано несколько устройств. Вы можете различать их по названиям. Пароль для доступа к устройству чувствителен к регистру; его длина должна составлять не менее четырех символов. Защита от перебора паролей осуществляется с помощью функции самоуничтожения. Не используйте русские символы для пароля (устройство будет невозможно разблокировать).</p>
4.	<p>Сохраните резервную копию пароля:</p> 	<p>IronKey позволяет создать резервную копию пароля в сетевом хранилище my.ironkey.com. Если вы забыли пароль, вы можете зайти на портал https://my.ironkey.com под своим именем и восстановить его.</p>
5.	<p>Появится экран пользовательского соглашения. Примите условия соглашения.</p>	<p>С полным текстом пользовательского соглашения можно ознакомиться на странице https://www.ironkey.com/terms</p>
6.	<p>Начнется процесс инициализации IronKey</p> 	<p>Процесс инициализации включает в себя генерацию ключей шифрования AES, создание файловой системы и копирование набора специальных приложений и файлов на защищенный дисковый раздел.</p>
7.	<p>Активируйте учетную запись на портале my.ironkey.com</p>	<p>Портал my.ironkey.com – это веб-сайт, позволяющий производить настройку учетной записи и подключенных устройств. Доступ на портал требует двухэтапной авторизации (устройство IronKey и пароль).</p>
8.	<p>Произведите настройку учетной записи, следуя инструкциям на экране</p>	<p>Настройка учетной записи включает в себя создание имени пользователя и пароля, подтверждение адреса электронной почты методом внеполосной авторизации, и ввод ответов на секретные вопросы. Помимо этого, вам будет предложено выбрать секретное изображение, демонстрируемое при входе в систему и секретную фразу, служащую антифишинговой защитой электронной переписки.</p>
9.	<p>Электронное письмо с подтверждением регистрации будет содержать код активации учетной записи. Введите его на сайте.</p>	<p>Проверка адреса электронной почты служит нескольким целям: сброс пароля в случае необходимости, разблокирование учетной записи на портале my.ironkey.com и оповещение о возможных угрозах безопасности.</p>

После выполнения этих шагов ваш накопитель IronKey полностью готов к работе.

РАБОТА С IRONKEY UNLOCKER ДЛЯ WINDOWS

Приложение IronKey Unlocker служит для безопасного доступа к файлам на компьютерах под управлением различных операционных систем. Оно запрашивает пароль, производит проверку его подлинности, и только после этого разблокирует и подключает накопитель, предоставляя доступ к файлам.




Для разблокирования накопителя в средах Windows 2000 (SP4), XP (SP2+), Vista и 7 выполните следующие шаги:

	Шаг	Описание
1.	<p>Вставьте накопитель в компьютер и введите пароль для разблокирования:</p> 	<p>При подключении накопителя появляется экран «Unlock Your IronKey».</p> <ul style="list-style-type: none">• Если экран не появился, вы можете открыть диск IronKey Unlocker двойным щелчком мыши и запустить файл IronKey.exe• При правильном вводе пароля произойдет подключение накопителя, и вы получите доступ ко всем файлам. Проверка подлинности пароля осуществляется на аппаратном уровне.• Если пароль введен неправильно 10 раз подряд, произойдет полное стирание данных. После каждых трех попыток требуется отключить устройство, а затем подключить его вновь.
2.	<p>Выберите желаемое действие после разблокирования.</p>	<p>Отметив соответствующие флажки перед разблокированием, вы можете выполнить следующие действия:</p> <ul style="list-style-type: none">• просмотреть защищенные файлы• запустить панель управления IronKey Control Panel• разблокировать устройство в режиме чтения, не позволяющем редактировать файлы• подключиться к учетной записи my.ironkey.com



НАЧАЛО РАБОТЫ И ИНИЦИАЛИЗАЦИЯ IRONKEY В СРЕДЕ MAC

Для инициализации IronKey в среде Mac выполните следующие шаги:

	Шаг	Описание
1.	Вставьте накопитель в свободный USB порт компьютера	Накопитель IronKey может работать на компьютерах под управлением Mac OS X (10.4+, Intel). Его также можно настроить и использовать в системах Windows и Linux. Для высокоскоростной передачи данных используйте порт USB 2.0.
2.	Дважды щелкните на диск IronKey Unlocker на рабочем столе и запустите файл IronKey.exe 	IronKey автоматически запускается в режиме виртуального CD-дисковода. Примечание Вы можете установить программное обеспечение IronKey Auto-Launch Assistant, автоматически запускающее IronKey Unlocker при подключении накопителя к компьютеру. См. раздел “Preferences” в настройках IronKey Control Panel. (только для Mac).
3.	Задайте название устройства и пароль для доступа.	Пароль для доступа к устройству чувствителен к регистру; его длина должна составлять не менее четырех символов. Защита от перебора паролей осуществляется с помощью функции самоуничтожения.
4.	Появится экран пользовательского соглашения. 	С полным текстом пользовательского соглашения можно ознакомиться на странице https://www.ironkey.com/terms
5.	Начнется процесс инициализации IronKey 	Процесс инициализации включает в себя генерацию ключей шифрования AES и создание файловой системы на дисковом разделе. Этот процесс может занять некоторое время.

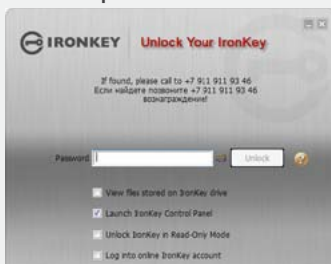
6.	Активируйте учетную запись на портале <i>my.ironkey.com</i>	Портал <i>my.ironkey.com</i> – это веб-сайт, позволяющий производить настройку учетной записи и подключенных устройств. Доступ на портал требует двухэтапной авторизации (устройство IronKey и пароль).
7.	Произведите настройку учетной записи, следуя инструкциям на экране	Настройка учетной записи включает в себя создание имени пользователя и пароля, подтверждение адреса электронной почты методом внеполосной авторизации, и ввод ответов на секретные вопросы. Помимо этого, вам будет предложено выбрать секретное изображение, демонстрируемое при входе в систему и секретную фразу, служащую антифишинговой защитой электронной переписки.
8.	Электронное письмо с подтверждением регистрации будет содержать код активации учетной записи. Введите его на сайте.	Пароль для доступа к устройству чувствителен к регистру; его длина должна составлять не менее четырех символов. Защита от перебора паролей осуществляется с помощью функции самоуничтожения.

После выполнения этих шагов ваш накопитель IronKey полностью готов к работе.

РАБОТА С IRONKEY UNLOCKER ДЛЯ MAC

Приложение IronKey Unlocker для Mac служит для безопасного доступа к файлам и смены пароля устройства на компьютерах Mac. Другими приложениями и сервисами IronKey можно пользоваться только в среде Windows.

	Шаг	Описание
1.	Вставьте накопитель в компьютер.	
2.	Дважды щелкните на диск IronKey Unlocker на рабочем столе и запустите файл IronKey.exe. Появится экран «Unlock Your IronKey».	<p>Примечание</p> <p>Вы можете установить программное обеспечение IronKey Auto-Launch Assistant, автоматически запускающее IronKey Unlocker при подключении накопителя к компьютеру. См. раздел “Preferences” в настройках IronKey Control Panel. (только для Mac)</p>
3.	Введите пароль для разблокирования:	<ul style="list-style-type: none"> • При правильном вводе пароля произойдет подключение накопителя, и вы получите доступ ко всем файлам. Проверка подлинности пароля осуществляется на аппаратном уровне. • Если пароль введен неправильно 10 раз подряд, произойдет полное стирание данных. После каждого трех попыток требуется отключить устройство, а затем подключить его вновь.



4.	Выберите желаемое действие после разблокирования.	<p>Отметив соответствующие флажки перед разблокированием, вы можете выполнить следующие действия:</p> <ul style="list-style-type: none"> • просмотреть защищенные файлы • запустить панель управления IronKey Control Panel • разблокировать устройство в режиме чтения, не позволяющем редактировать файлы • подключиться к учетной записи <i>my.ironkey.com</i>
----	---	---

НАЧАЛО РАБОТЫ И ИНИЦИАЛИЗАЦИЯ IRONKEY В СРЕДЕ LINUX

Для инициализации IronKey в среде Linux выполните следующие шаги:

	Шаг	Описание
1.	Вставьте накопитель в свободный USB порт компьютера	<p>Накопитель IronKey может работать на компьютерах семейства x86 под управлением Linux 2.6+. Его также можно настроить и использовать в системах Windows и Mac.</p> <p>Для высокоскоростной передачи данных используйте порт USB 2.0.</p>
2.	Запустите программу ironkey из папки linux накопителя IronKey	<p>IronKey имеет встроенный виртуальный CD-диск. Запустите из папки linux программу ironkey.</p>
3.	Примите условия пользовательского соглашения.	<p>Появится экран пользовательского соглашения. Прокрутите соглашение до конца, затем нажмите Q для выхода из режима просмотра. Нажмите Y для принятия условий соглашения.</p> <p>С полным текстом пользовательского соглашения можно ознакомиться на странице https://www.ironkey.com/terms</p>
4.	Задайте название устройства и пароль для доступа.	<p>К учетной записи IronKey может быть привязано несколько устройств. Вы можете различать их по названиям. Пароль для доступа к устройству чувствителен к регистру; его длина должна составлять не менее четырех символов. Защита от перебора паролей осуществляется с помощью функции самоуничтожения.</p>
5.	Начнется процесс инициализации IronKey	<p>Процесс инициализации включает в себя генерацию ключей шифрования AES и создание файловой системы на дисковом разделе.</p> <p>Этот процесс может занять некоторое время.</p>

После выполнения этих шагов ваш накопитель IronKey полностью готов к работе.

РАБОТА С IRONKEY UNLOCKER ДЛЯ LINUX

Приложение IronKey Unlocker служит для безопасного доступа к файлам и смены пароля устройства на компьютерах под управлением Linux. Другими приложениями и сервисами IronKey можно пользоваться только в среде Windows.

В зависимости от дистрибутива Linux для запуска программы ironkey из папки linux виртуального CD-дисковода вам могут потребовать права root. Если к компьютеру подключен только один накопитель, программа запускается простой командой без атрибутов («ironkey»). Если накопителей несколько, потребуется дополнительно указать название устройства для разблокирования.

ПРИМЕЧАНИЕ

Команда ironkey только разблокирует накопитель, после разблокирования его необходимо монтировать. Многие дистрибутивы Linux делают это автоматически, но если этого не произошло, монтирование осуществляется из командной строки. Следует использовать название устройства, выведенное командой ironkey.

Для смены пароля к устройству с названием «devicename», используйте следующую команду:

```
ironkey --changepwd [devicename]
```

Для блокирования устройства с названием «devicename», используйте следующую команду:

```
ironkey --lock [devicename]
```

Для разблокирования устройства с названием «devicename» в режиме чтения, используйте следующую команду:

```
ironkey --read-only
```

Для разблокирования устройства паролем «devicepassword», используйте следующую команду:

```
ironkey --password [devicepassword]
```

При демонтаже накопителя не происходит его автоматической блокировки. Для блокирования устройства, его следует либо демонтировать и отключить от компьютера, либо использовать следующую команду:

```
ironkey lock
```

ВАЖНЫЕ ЗАМЕЧАНИЯ ПО ИСПОЛЬЗОВАНИЮ IRONKEY В СРЕДЕ LINUX

1. Версия используемого ядра должна быть не ниже 2.6

При компилировании собственного ядра включите в него следующий код:

```
DeviceDrivers->SCSIDeviceSupport-><*>SCSICDROMSupport
```

```
DeviceDrivers-><*> Support for Host-side USB
```

```
DeviceDrivers-><*> USB device filesystem
```

```
DeviceDrivers-><*> EHCI HCD (USB 2.0) support
```

```
DeviceDrivers-><*> UHCI HCD (most Intel and VIA) support
```

```
DeviceDrivers-><*> USB Mass Storage Support
```

Ядра, включенные в состав большинства распространенных дистрибутивов, имеют поддержку этих драйверов, поэтому при использовании ядра по умолчанию производить дополнительных действий не требуется.

На 64-битных системах для работы программы ironkey требуется проинсталлировать 32-битные библиотеки.

2. Проблемы при монтировании

Для монтирования IronKey вы должны обладать правами доступа на монтирование SCSI и USB устройств.

» Некоторые дистрибутивы Linux не производят монтирования автоматически, поэтому оно должно быть выполнено с помощью следующей команды:

```
mount /dev/<name of the device> /media/<name of the mounted device>
```

» Название устройства, используемое для монтирования, зависит от используемого дистрибутива. Названия устройств IronKey можно получить, выполнив следующую команду:

```
ironkey --show
```

3. Права доступа

» Требуются права доступа на монтирование external, usb, и flash устройств.

» Для запуска IronKey Unlocker требуются права доступа на запуск программ с CD-дисковода IronKey.

» Могут потребоваться права root.

4. Поддерживаемые дистрибутивы

Поддерживаются не все дистрибутивы Linux. С полным списком поддерживаемых дистрибутивов можно ознакомиться на странице <https://support.ironkey.com/linux>.

5. IronKey Unlocker для Linux в настоящий момент доступен только для x86-систем




С более подробной информацией можно ознакомиться на странице <https://support.ironkey.com/linux>.




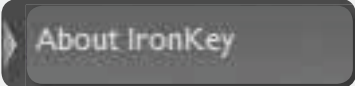
РАБОТА С ПАНЕЛЬЮ УПРАВЛЕНИЯ IRONKEY CONTROL PANEL ДЛЯ WINDOWS И MAC



Панель управления IronKey Control Panel – это приложение, служащее для выполнения следующих задач:

- » Запуск встроенных приложений
- » Вход на портал my.ironkey.com
- » Настройка накопителя
- » Обновление микропрограммы
- » Смена пароля для доступа к устройству
- » Безопасная блокировка устройства
- » Получение справки

	Шаг	Описание
1.	<p>Создание, редактирование и удаление защищенных файлов</p> 	<p>При выборе пункта «Secure Files» содержимое накопителя отображается в браузере. Файлы на накопителе IronKey зашифрованы по алгоритму AES. Шифрование осуществляется автоматически при переносе файлов на накопитель; при перемещении файлов с накопителя на рабочий стол происходит автоматическое расшифровывание. IronKey работает как обычный флэш-накопитель, обеспечивая при этом автоматическую и всегда активированную защиту данных.</p>
2.	<p>Обновление микропрограммы и сопутствующего программного обеспечения</p> 	<p>IronKey производит обновление микропрограммы и сопутствующего программного обеспечения. Обновления передаются по защищенному каналу и проверяются на аппаратном уровне, обеспечивая актуальность состояния устройства и защиту от возможных угроз.</p> <p>Для проверки наличия обновлений, нажмите на кнопку «Check for Updates» (для Windows) или «Check now» (для Mac).</p> <ul style="list-style-type: none"> • Windows: при наличии обновлений, их можно загрузить и установить, нажав кнопку «Download Update» • Mac: вы можете загружать и устанавливать обновления политик безопасности. Обновления программного обеспечения загружаются и устанавливаются только в среде Windows.
3.	<p>Персональные настройки</p> 	<p>Для редактирования персональных настроек нажмите на кнопку «Preferences» и выполните желаемое действие:</p> <ul style="list-style-type: none"> » Включение Identity Manager » Включение режима Безопасных Сессий Выбор интернет-браузера по умолчанию » Включение автоматической блокировки IronKey по истечении времени ожидания » Установка утилиты IronKey Auto-Launch Assistant, автоматически запускающей IronKey Unlocker при подключении IronKey к компьютеру (только для Mac) <p>Доступны также следующие служебные функции:</p> <ul style="list-style-type: none"> » Форматирование накопителя » Восстановление встроенных приложений IronKey, в случае если они повреждены или удалены (только для Windows)

4.	<p>Настройки сети и прокси-сервера</p> 	<p>Для настройки подключения к сети Интернет, нажмите на кнопку «Network Settings» (для Windows) или «Network» (для Mac):</p> <ul style="list-style-type: none"> >> Direct Connection: прямое соединение без использования прокси-сервера >> Use System Settings (по умолчанию): используются системные настройки прокси-сервера: <ul style="list-style-type: none"> • Для Windows: Панель Управления > Свойства Обозревателя • Для Mac: Системные настройки > Сеть > Прокси <p>Примечание Firefox не обращается к «Системным настройкам», поэтому в его настройках прокси-сервера должны быть вручную заданы те же значения, что и в «Системных настройках» и панели управления IronKey.</p> <ul style="list-style-type: none"> >> Configuration Script: введите URL или путь к файлу автоматического определения прокси-сервера >> Manual Proxy: введите адрес и номер порта прокси-сервера <p>Если для подключения к прокси-серверу требуется авторизация, введите имя пользователя и пароль в соответствующих полях.</p>
5.	<p>Сообщение Lost and Found</p> 	<p>Функция «Lost and Found» позволяет задать сообщение, выводимое в окне IronKey Unlocker. В случае утери накопителя, вам могут его вернуть, если вы укажете контактную информацию.</p>
6.	<p>Смена пароля доступа к устройству</p> 	<p>Функция «IronKey Password» позволяет сменить пароль доступа к устройству и сохранить его в сетевом хранилище на портале my.ironkey.com. Регулярная смена пароля значительно повышает защищенность данных. Выбирайте только запоминающиеся пароли.</p>
7.	<p>Просмотр информации об устройстве</p> 	<p>При выборе пункта «Viewing device details» отображается подробная информация об устройстве: номер модели, серийный номер, версии микропрограммы и программного обеспечения, данные о состоянии накопителя и тип операционной системы. Вы можете скопировать эту информацию в буфер обмена, нажав кнопку «Сору» (CTRL+C), для последующей вставки в сообщение форума или запрос технической поддержки.</p> <p>Для перехода на сайт IronKey нажмите CTRL+W. Для просмотра правовых положений нажмите CTRL+N. Для просмотра сертификатов нажмите CTRL+?.</p>

8. Добавление, переименование и удаление приложений из Списка Приложений



Для управления содержимым Списка Приложений, щелкните правой кнопкой мыши в окне Applications List и выберите желаемое действие (добавление, переименование или удаление) из контекстного меню. Вы можете также задать режим представления содержимого в виде иконок или списка.

ПРИМЕЧАНИЕ

- » Для Mac: приложения, установленные на накопитель, автоматически добавляются в Список Приложений (изначально список пуст).
- » Элементы списка – это ярлыки приложений. Удаление их из списка не затронет сами приложения.
- » Список автоматически сортируется по алфавиту.
- » В список можно добавить любой произвольный элемент: документ, изображение, командный файл и т.д.
- » В среде Windows файлы, не являющиеся приложениями, открываются в приложениях, сопоставленных типу файла.

9. Блокировка и отключение IronKey



При выборе пункта «Lock Drive» или нажатии CTRL+L (для Windows) или «Lock & Quit» (для Mac) происходит закрытие всех запущенных приложений IronKey, после чего устройство блокируется, и его можно безопасно извлечь из компьютера. Для предотвращения потери данных, закрывайте все открытые файлы и приложения перед блокировкой устройства.



РАБОТА С ВИРТУАЛЬНОЙ КЛАВИАТУРОЙ IRONKEY VIRTUAL KEYBOARD ДЛЯ WINDOWS

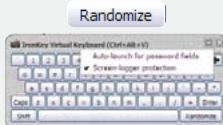
Если безопасность компьютера, на котором вы работаете, вызывает сомнения, вы можете воспользоваться виртуальной клавиатурой IronKey Virtual Keyboard. Виртуальная клавиатура служит для набора цифр и букв и защищает пароль от программ-троянов, а также клавиатурных и экранных шпионов.

Экранную клавиатуру IronKey Virtual Keyboard можно запустить следующими способами:

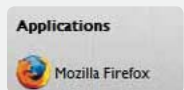

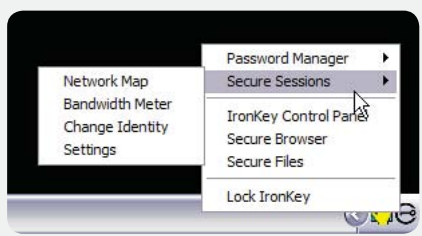
- » В момент ввода пароля доступа к устройству (т.е. при запуске IronKey Unlocker, смене пароля или инициализации накопителя) нажмите на значок виртуальной клавиатуры.
- » Используйте сочетание клавиш CTRL+ALT+V

Виртуальную клавиатуру можно использовать и во всех прочих приложениях (например, для написания электронных писем или документов), если требуются повышенные меры безопасности.

Шаг	Описание
<p>1. Нажмите на значок виртуальной клавиатуры: </p> <p>Появится виртуальная клавиатура. Вы можете также использовать сочетание клавиш CTRL+ALT+V</p>	

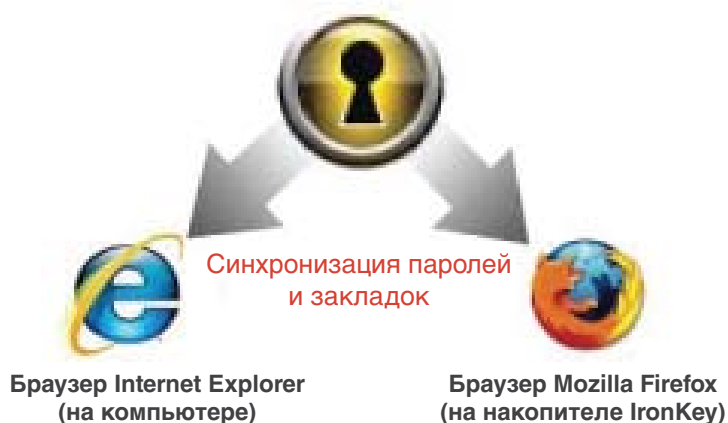
2.	<p>Нажимайте на кнопки виртуальной клавиатуры для ввода пароля. По окончании ввода, нажмите на кнопку «Enter».</p>	<p>Виртуальную клавиатуру можно использовать в паре с обычной клавиатурой – вы можете вводить символы любым удобным способом.</p>
3.	<p>При необходимости вы можете случайным образом изменить расположение символов на клавиатуре, что служит защитой от программ-экранных шпионов. Для этого нажмите на кнопку «Randomize»:</p> 	<p>При нажатии кнопки на виртуальной клавиатуре подписи всех кнопок исчезают. Это не позволяет программам-экранным шпионам определить место нажатия. При необходимости эту функцию можно отключить в выпадающем меню рядом с кнопкой закрытия окна.</p> <p>В меню опций можно выбрать режим виртуальной клавиатуры, в котором она автоматически запускается при перемещении курсора в любое поле ввода пароля.</p>

РАБОТА СО ВСТРОЕННЫМ ИНТЕРНЕТ-БРАУЗЕРОМ FIREFOX И РЕЖИМОМ ЗАЩИЩЕННЫХ СЕССИЙ ДЛЯ WINDOWS

Шаг		Описание
1.	<p>Для пользования интернет-ресурсами с накопителя запустите встроенный браузер Firefox:</p> 	<p>При выборе пункта Mozilla Firefox в Списке Приложений запускается встроенный интернет-браузер Firefox. Параллельная работа браузеров Firefox на накопителе и на компьютере не поддерживается. Если Firefox запущен на компьютере, система предложит закрыть его.</p>
2.	<p>Для запуска режима Защищенных Сессий, обеспечивающего безопасное пребывание в интернете, нажмите на соответствующий значок:</p> 	<p>Нажатие на значок режима Защищенных Сессий в правом нижнем углу окна браузера включает и выключает режим Защищенных Сессий. В этом режиме задействуется прямой зашифрованный канал между накопителем IronKey и защищенным сервером IronKey. Расшифровка данных осуществляется на сервере, откуда они пересылаются на требуемый интернет-сайт. Эти меры безопасности защищают от фишинга и фарминга, так как на серверах IronKey осуществляется проверка DNS. Кроме того, в этом режиме скрываются персональные данные: ваш IP-адрес не будет виден интернет-провайдерам и веб-ресурсам. Вы можете проверить эту функцию, посетив сайты, определяющие IP-адрес посетителя, например <i>whatismyip.com</i> или <i>ipchicken.com</i>.</p>
3.	<p>Работа с режимом Защищенных Сессий: карта сети, информация о подключении и изменение идентификационных данных:</p> 	<p>Для просмотра текущей информации, выберите соответствующий пункт из меню IronKey в области уведомлений.</p> <ul style="list-style-type: none"> • Карта сети «Network Map» отображает доступные «виртуальные цепочки» и показывает, откуда поступает входящий трафик. • Информация о подключении «Bandwidth Meter» отображает данные текущего подключения. • Изменение идентификационных данных «Change Identity» позволяет сменить «виртуальное местоположение». При этом случайным образом создаются новые «виртуальные цепочки» и соответственно меняется путь трафика. Так как сменится также и IP-адрес, интернет-сайты будут идентифицировать вас как нового посетителя.

РАБОТА С IRONKEY IDENTITY MANAGER ДЛЯ WINDOWS

Приложение IronKey Identity Manager предназначено для безопасного хранения персональных данных, например, данных учетных записей в сетевых сервисах и паролей к различным приложениям. По нажатию кнопки оно запускает нужное приложение, автоматически вводит имя пользователя и пароль и производит авторизацию. При необходимости приложение может сгенерировать надежный пароль для защиты особо важных данных.



IronKey Identity Manager позволяет создать резервную копию персональных данных в сетевом хранилище, синхронизировать их на нескольких накопителях IronKey, а также, в случае утраты накопителя, перенести их на новый IronKey.

IronKey Identity Manager не хранит пароли в файле на дисковом разделе, поэтому их нельзя оттуда извлечь. При вводе паролей включается дополнительная защита от программ-клавиатурных шпионов.



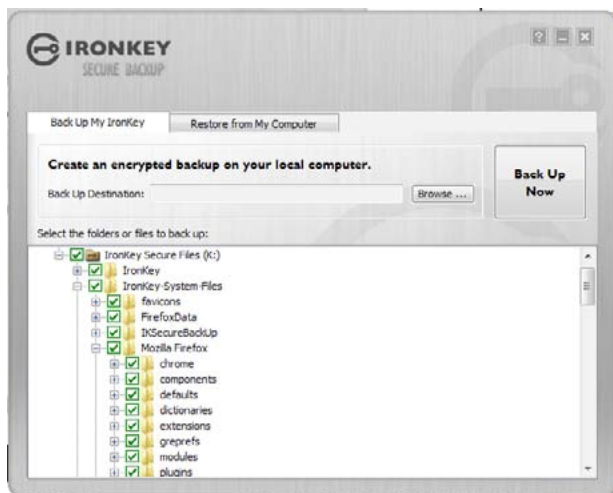
В IronKey Identity Manager применяется технология VeriSign VIP. При работе с важными сетевыми сервисами, например, eBay, PayPal, AOL и Geico, при каждом подключении генерируется новый пароль. Таким образом, сервис привязывается к накопителю IronKey и может использоваться только в паре с ним.

Для получения подробной информации о возможностях IronKey Identity Manager ознакомьтесь со справочными материалами. Для просмотра справки нажмите на кнопку «Help» в правом верхнем углу окна IronKey Identity Manager.

	Шаг	Описание
1.	Добавление учетных записей и паролей	Добавить учетные записи и пароли для использования в IronKey Identity Manager можно следующими способами: <ul style="list-style-type: none">• Восстановив их из сетевого хранилища• Импортировав из Firefox, KeePass, RoboForms или Internet Explorer• Добавив вручную по нажатию кнопки «Add» в окне IronKey Identity Manager• Выбрав пункт «Add Account» в меню заголовка окна при нахождении на желаемом интернет-сайте• Используя встроенный режим самообучения. При входе на интернет-сайт, IronKey Identity Manager перехватывает данные учетной записи и предлагает сохранить их на накопитель.

2.	Автоматический вход	<p>При входе на интернет-сайт или в приложение, учетные данные которого сохранены в IronKey, соответствующие поля заполняются автоматически и, если включена соответствующая опция, автоматически производится вход.</p> <p>Вход также можно осуществить следующими способами:</p> <ul style="list-style-type: none"> • Используя приложение IronKey Launcher (CTRL+ALT+R) • Выбрав соответствующий пункт в меню заголовка окна в правом верхнем углу • Выбрав соответствующий пункт в меню IronKey в области уведомлений • Нажав кнопку «AUTO» в окне IronKey Identity Manager
3.	Редактирование и удаление учетных записей и паролей	<p>Редактирование учетных записей и паролей производится в окне IronKey Identity Manager. Дважды щелкните на желаемой записи или выделите ее и нажмите на кнопку «Edit».</p> <p>По окончании редактирования данные автоматически сохраняются.</p>
4.	Создание резервной копии и восстановление данных	<p>Для создания резервной копии данных нажмите на кнопку «Backup» в окне IronKey Identity Manager. Впоследствии вы можете восстановить эти данные на накопитель, что позволяет синхронизировать накопители и организовывать их в виде иерархии.</p>
5.	Привязка учетных записей с использованием технологии VeriSign VIP	<p>Учетные записи важных сетевых сервисов (например, eBay и PayPal) можно привязать к IronKey, так что их использование без накопителя станет невозможным.</p> <p>Для привязки учетной записи войдите на сетевой сервис под своим именем и выполните шаги, предлагаемые IronKey Identity Manager.</p> <p>Для выполнения привязки вручную, войдите в режим редактирования учетной записи и выберите пункт «VeriSign VIP» из списка «Additional Authentication».</p>
6.	Генерирование надежных паролей	<p>При редактировании учетной записи IronKey Identity Manager позволяет сгенерировать случайный пароль. Этот пароль можно сохранить на накопителе для последующего использования.</p>
7.	Редактирование настроек IronKey Identity Manager	<p>Для редактирования настроек IronKey Identity Manager нажмите на кнопку «Settings» в окне IronKey Identity Manager. Для получения более подробной информации ознакомьтесь со справочными материалами.</p>

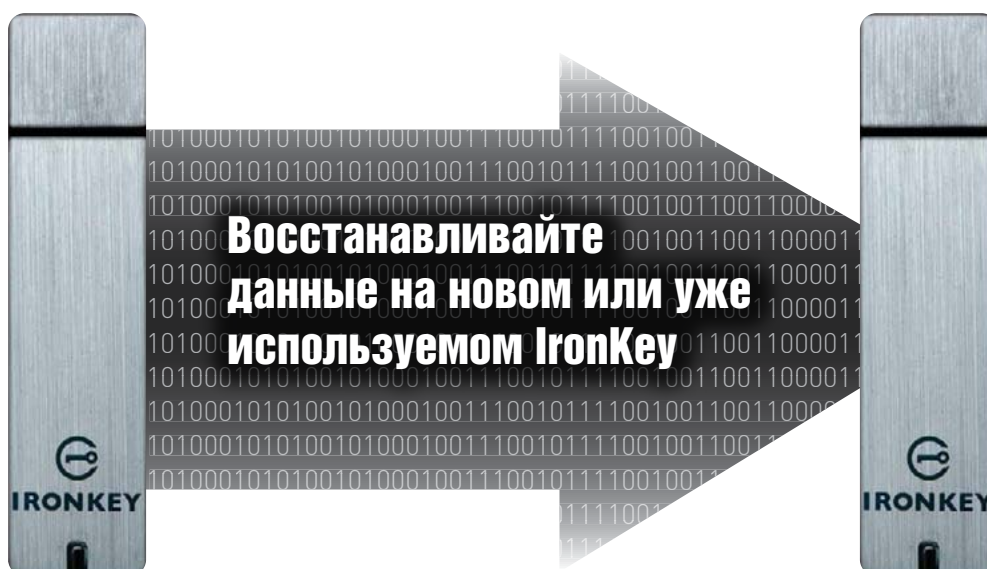
РАБОТА С SECURE BACKUP ДЛЯ WINDOWS



В случае утраты накопителя IronKey вы можете быть уверены, что ваши персональные данные останутся недоступными, а приложение Secure Backup позволит быстро и безопасно восстановить все данные из резервной копии.

Компания IronKey рекомендует регулярно создавать резервную копию данных.


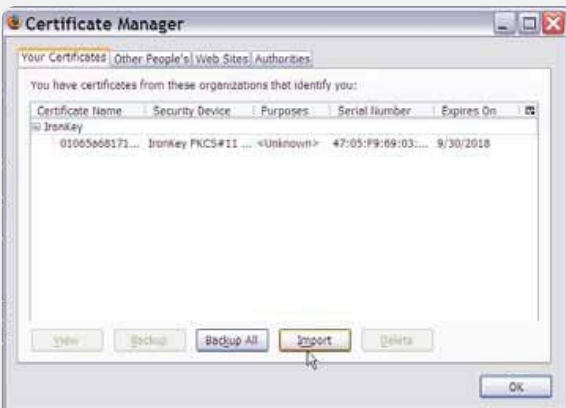
	Шаг	Описание
1.	Создание резервной копии 	Для создания зашифрованной резервной копии на компьютере нажмите на кнопку «Secure Backup» в панели управления IronKey, задайте путь для копирования и выберите необходимые файлы. Можно выбрать как отдельные файлы, так и все содержимое накопителя.
2.	Восстановление данных из зашифрованной резервной копии	В случае утраты накопителя вы можете восстановить данные из резервной копии. Откройте приложение Secure Backup, укажите путь к копии и выберите, какие файлы и папки следует восстановить. При восстановлении данных на другой накопитель, введите пароль доступа к нему.

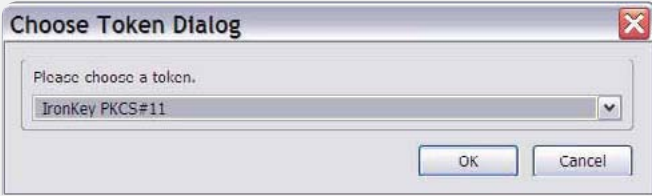




ИМПОРТИРОВАНИЕ ЦИФРОВОГО СЕРТИФИКАТА НА НАКОПИТЕЛЬ IRONKEY В СРЕДЕ WINDOWS

В криптичипе IronKey выделена специальная особо защищенная область для хранения персонального ключа, связанного с цифровым сертификатом. Хранение ключа предоставляет дополнительные возможности безопасной авторизации: к примеру, вы можете сохранить самоподписанный сертификат для подключения к внутренним сетям, и при использовании встроенного браузера Firefox вход будет производиться автоматически.

Импортирование сертификата осуществляется по протоколу PKCS#11 и требует использования Mozilla Firefox. В устройстве выделено место под хранение лишь одного ключа, но тем не менее этот ключ защищен ударопрочным корпусом и механизмами самоуничтожения криптичипа.

	Шаг	Описание
1.	Откройте встроенный браузер Firefox	Нажмите на значок Firefox в Списке Приложений накопителя
2.	Откройте вкладку «Encryption» в опциях Firefox	<ol style="list-style-type: none">1. Выберите «Tools» в меню приложения.2. Выберите «Options»3. Нажмите на значок «Advanced»4. Перейдите на вкладку «Encryption»
3.	Нажмите на кнопку «View Certificates». Появится окно Firefox Certificates Manager.	
4.	В списке доступен сертификат IronKey. Для добавления собственного сертификата, нажмите на кнопку «Import»	




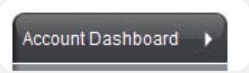
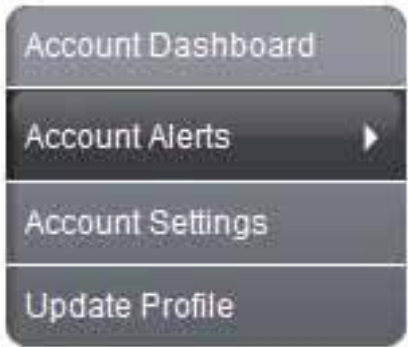
5.	Выберите требуемый файл сертификата в формате PKCS#12.	Укажите расположение файла сертификата в формате PKCS#12. Расширение файла в системах Linux/UNIX – .p12; в системах Windows – .pfx.
6.	Появится окно подтверждения сохранения сертификата. Укажите место сохранения, выбрав «IronKey PKCS#11»	
7.	Введите пароль защиты сертификата. Если пароль не использовался, оставьте поле пустым.	
8.	Сертификат сохранен в крипточипе IronKey, и его можно использовать во встроенном браузере Firefox.	

РАБОТА С MY.IRONKEY.COM ДЛЯ WINDOWS И MAC

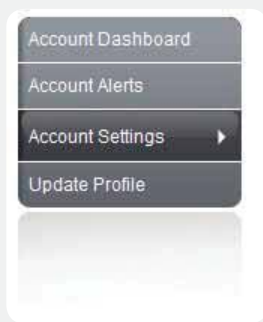
Накопитель IronKey поддерживает надежные механизмы авторизации с использованием ключевых пар PKI, которые генерируются крипточипом. При подключении к portalу my.ironkey.com эти ключи используются в качестве уникальных идентификаторов. Таким образом, для доступа к сервису требуется одновременно наличие накопителя и знание пароля. Это дополнительная мера защиты: даже если накопитель украден или кто-то узнал ваш пароль, только вы имеете доступ к своей учетной записи.



В случае утери накопителя на портал можно войти в безопасном режиме ограниченной функциональности. В этом режиме вы можете указать, что накопитель утрачен, а также восстановить забытый пароль.

	Шаг	Описание
1.	<p>Вход под своей учетной записью</p> 	<p>Для входа на портал my.ironkey.com нажмите на кнопку «my.ironkey.com» в панели управления IronKey. Запустится процесс PKI-аутентификации, после которого произойдет вход.</p> <p>В случае утери накопителя, на портал можно войти в безопасном режиме: для этого зайдите на сайт https://my.ironkey.com и введите данные своей учетной записи. В этом режиме вы можете указать, что накопитель утрачен, а также восстановить забытый пароль.</p>
2.	<p>Указание утраченного накопителя</p> 	<p>В случае утраты накопителя IronKey вы можете быть уверены, что ваши персональные данные останутся недоступными. Вы также можете дополнительно указать, что накопитель утрачен: в этом случае доступ с этого накопителя к вашей учетной записи на портале my.ironkey.com блокируется.</p> <p>В случае обнаружения накопителя доступ можно восстановить.</p>
3.	<p>Восстановления пароля доступа к устройству</p> 	<p>IronKey позволяет создать резервную копию пароля доступа к устройству на портале my.ironkey.com.</p> <p>Если вы забыли пароль, вы можете войти на портал в безопасном режиме (или используя другой накопитель IronKey) и восстановить его.</p>
4.	<p>Информация об активности учетной записи</p> 	<p>IronKey позволяет создать резервную копию пароля доступа к устройству на портале my.ironkey.com.</p> <p>Если вы забыли пароль, вы можете войти на портал в безопасном режиме (или используя другой накопитель IronKey) и восстановить его.</p>
5.	<p>Сообщения учетной записи для наблюдения в реальном времени</p> 	<p>Включение режима «Account Alerts» позволяет вести постоянное наблюдение за учетной записью. При любой активности вы будете получать электронное письмо с информацией о событии, включая время и IP-адрес источника.</p> <p>Для защиты от фишинга, все электронные письма содержат часть секретной фразы в теле письма.</p>

6. Изменение параметров учетной записи



Для того чтобы обезопасить учетную запись, вы можете периодически менять пароль доступа, секретные вопросы, секретное изображение, секретную фразу и адрес электронной почты.

Вы можете задать часовой пояс и изменить настройки отображения даты и времени.

Также рекомендуется указать дополнительный адрес электронной почты, на случай если основной адрес по каким-то причинам окажется недоступным.

В случае утери накопителя, на портал можно войти в безопасном режиме ограниченной функциональности. В этом режиме вы можете указать, что накопитель утрачен, а также восстановить забытый пароль доступа к устройству.

	Шаг	Описание
1.	Зайдите на сайт https://my.ironkey.com	На этом сайте вы можете войти на портал под своей учетной записью в безопасном режиме.
2.	Введите адрес электронной почты (или имя пользователя) и пароль учетной записи	Появится секретное изображение, гарантирующее, что вы действительно на сайте my.ironkey.com . Не вводите пароль доступа к устройству. Если вы забыли пароль учетной записи, нажмите на ссылку «Reset Password»
3.	На ваш адрес электронной почты будет отправлено письмо с кодом подключения.	Скопируйте код подключения и вставьте его в требуемое поле на странице. В зависимости от настроек учетной записи, вам может быть предложено ответить на секретные вопросы.
4.	Вы вошли на портал в безопасном режиме	Если вы забыли пароль доступа к устройству, но сохранили его в сетевом хранилище, вы можете восстановить его.



РАБОТА С НАКОПИТЕЛЕМ В РЕЖИМЕ ЧТЕНИЯ В СРЕДАХ WINDOWS, MAC И LINUX

Накопитель IronKey может быть разблокирован в режиме чтения, при этом файлы на накопителе остаются недоступными для редактирования. Этот режим можно использовать при работе на общедоступном компьютере: вы можете быть уверены что вредоносное или шпионское программное обеспечение не попадет на накопитель и не повредит файлы.

Если IronKey разблокирован в режиме чтения, он остается в этом режиме до момента блокировки.

В режиме чтения некоторые функции, требующие модификации файлов, становятся недоступными. К примеру, недоступен встроенный браузер Firefox, форматирование накопителя, обновление и восстановление приложений, а также пользование Списком Приложений.

НА КОМПЬЮТЕРАХ ПОД УПРАВЛЕНИЕМ WINDOWS И MAC:

	Шаг	Описание
1.	Отметьте флажок «Unlock IronKey in Read-Only Mode» при разблокировании накопителя	
2.	В панели управления появится надпись, подтверждающая, что накопитель разблокирован в режиме чтения.	

НА КОМПЬЮТЕРАХ ПОД УПРАВЛЕНИЕМ LINUX:

	Шаг	Описание
1.	Выполните следующую команду:	<code>ironkey --read-only</code>
2.	Для перехода в стандартный режим, заблокируйте накопитель:	<code>ironkey --lock</code>

Если у вас есть интересные идеи и предложения или вы хотите принять участие в тестировании новой функциональности, сообщите нам. Вы можете создать тему на пользовательском форуме (forum.ironkey.com) или оставить отзыв, написав по адресу feedback@ironkey.com.

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Для получения подробной информации об устройстве выберите пункт «About IronKey» в разделе «Settings» панели управления.

ОБЪЕМ ПАМЯТИ

В зависимости от модели, до 32-х гигабайт

ГАБАРИТЫ

75 x 19 x 9 мм

ВЕС

23 грамма

ВОДОНЕПРОНИЦАЕМОСТЬ

Стандарт MIL-STD-810F

РАБОЧАЯ ТЕМПЕРАТУРА

От 0 C до 70 C

ДОПУСТИМА ПЕРЕГРУЗКА

16G RMS

ШИФРОВАНИЕ

Аппаратное шифрование: AES 256-бит (на моделях S200 и D200), AES 128-бит (на модели S100)

Хеширование: SHA 256-бит

PKI: RSA 2048-бит

СЕРТИФИКАТ FIPS

Подробная информация доступна на сайте www.ironkey.com

ИНТЕРФЕЙС

USB 2.0 High-Speed (рекомендуется), USB 1.1

Поддерживаемые ОС:

Windows 2000 (SP4), XP (SP2+), Vista и 7

IronKey Unlocker для Linux (2.6+, x86)

IronKey Unlocker для Mac (10.4+, Intel)

Устройства IronKey не требуют установки дополнительного программного обеспечения или драйверов.

Разработано и



изготовлено
в США



*Заявленный объем памяти является приблизительным. Часть памяти задействуется для установки сопутствующего программного обеспечения.

Что дальше?

Во многом это зависит от вас. Команда IronKey ставит своей целью не просто разработку самого защищенного накопителя, но технологий, который просто и приятно использовать. Мы рады любым откликам пользователей и тщательно изучаем отзывы о продуктах и предложения о новых возможностях.

Если у вас есть интересные идеи и предложения или вы хотите принять участие в тестировании новой функциональности, сообщите нам. Вы можете создать тему на пользовательском форуме (forum.ironkey.com) или оставить отзыв, написав по адресу feedback@ironkey.com.

КАК ПОЛУЧИТЬ ДОПОЛНИТЕЛЬНУЮ ИНФОРМАЦИЮ?

Мы стремимся как можно подробнее рассказывать о технологиях безопасности и архитектуре устройств IronKey и сопутствующих сетевых служб. С этой информацией можно ознакомиться на наших сайтах:

forum.ironkey.com

многотысячное сообщество пользователей IronKey

www.ironkey.com

общая информация

support.ironkey.com

техническая поддержка и

обучающие видеоматериалы

КОМАНДА IRONKEY

Команда IronKey – это коллектив профессионалов в области информационной безопасности и защиты информации, сотрудничавших с компаниями Visa, RSA Security, PayPal, Authenex, Nokia, Cisco, Lexar, Netscape, Tumbleweed, Valicert, Apple, Министерством Внутренней Безопасности США. Президент компании Дейв Джеванс параллельно является председателем Антифишинговой рабочей группы (www.antiphishing.org).

На разработку IronKey потрачены годы исследований и миллионы долларов. Этот удобный и простой в использовании накопитель защитит ваши данные и сделает пребывание в интернете по-настоящему безопасным.



КОНТАКТНАЯ ИНФОРМАЦИЯ

НА РУССКОМ ЯЗЫКЕ:

ОТЗЫВЫ:

feedback@humansolutions.ru

ИНТЕРНЕТ-САЙТЫ:

<http://www.humansolutions.ru>

НА АНГЛИЙСКОМ ЯЗЫКЕ:

ОТЗЫВЫ

feedback@ironkey.com

Предложения

featurerequest@ironkey.com

ИНТЕРНЕТ-САЙТЫ IRONKEY

<https://my.ironkey.com>

<https://support.ironkey.com>

<https://forum.ironkey.com>

<https://store.ironkey.com>

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

<https://support.ironkey.com>

ООО «ЧЕЛОВЕЧЕСКИЕ РЕШЕНИЯ»

197110, Россия, Санкт-Петербург, ул. Большая Зеленина,
д.24, офис 925

Тел./Факс: +7 (812) 607-68-36

E-mail: info@humansolutions.ru

ПРИМЕЧАНИЕ

Компания IronKey не несет ответственности за возможные ошибки или пропуски в тексте этого документа и не отвечает за случайные или закономерные негативные последствия использования сведений, содержащихся в документе. Представленная информация может измениться без предварительного уведомления.

Информация, представленная в документе, представляет собой видение компании IronKey предмета описания на момент публикации документа. Документ предназначен только для информационных целей. Компания IronKey не предоставляет гарантий, прямо или косвенно обозначенных содержанием текста документа. IronKey и логотип IronKey являются зарегистрированными торговыми марками IronKey Inc. на территории США и других стран. Права на прочие торговые марки принадлежат их зарегистрированным владельцам.
© 2010 IronKey, Inc. Все права защищены. IKPUG20100510