

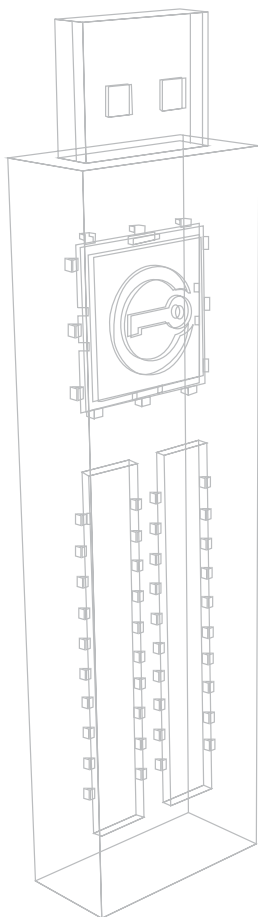
# IronKey Basic

---

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](http://www.humansolutions.ru)

Мы будем рады любым отзывам и предложениям.

Отзывы:

[feedback@humansolutions.ru](mailto:feedback@humansolutions.ru)

# ОГЛАВЛЕНИЕ

<b>ЧТО ТАКОЕ IRONKEY? .....</b>	<b>4</b>
Ключевые особенности .....	5
Изображения устройства .....	7
Средства обеспечения безопасности .....	8
Безопасность устройства .....	8
<b>КАК РАБОТАЕТ IRONKEY? .....</b>	<b>10</b>
Обзор устройства .....	10
Начало работы и инициализация IronKey в среде Windows .....	10
Работа с IronKey Unlocker для Windows .....	11
Начало работы и инициализация IronKey в среде Mac .....	12
Работа с IronKey Unlocker для Mac .....	13
Начало работы и инициализация IronKey в среде Linux .....	14
Работа с IronKey Unlocker для Linux .....	15
Активация IronKey Enterprise для Windows и Mac .....	16
Работа с панелью управления IronKey Control Panel для Windows и Mac .....	17
Работа с Secure Backup для Windows .....	19
Работа с виртуальной клавиатурой IronKey Virtual Keyboard для Windows .....	20
Работа с накопителем в режиме чтения в средах Windows, Mac и Linux .....	21
Технические характеристики .....	22
<b>ЧТО ДАЛЬШЕ? .....</b>	<b>23</b>
Как получить дополнительную информацию? .....	23
Команда IronKey .....	23
Контактная информация .....	24

# Что такое IronKey?

## ПОЗНАКОМЬТЕСЬ С IRONKEY

Флэш-накопитель IronKey Basic – 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 или 16 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.



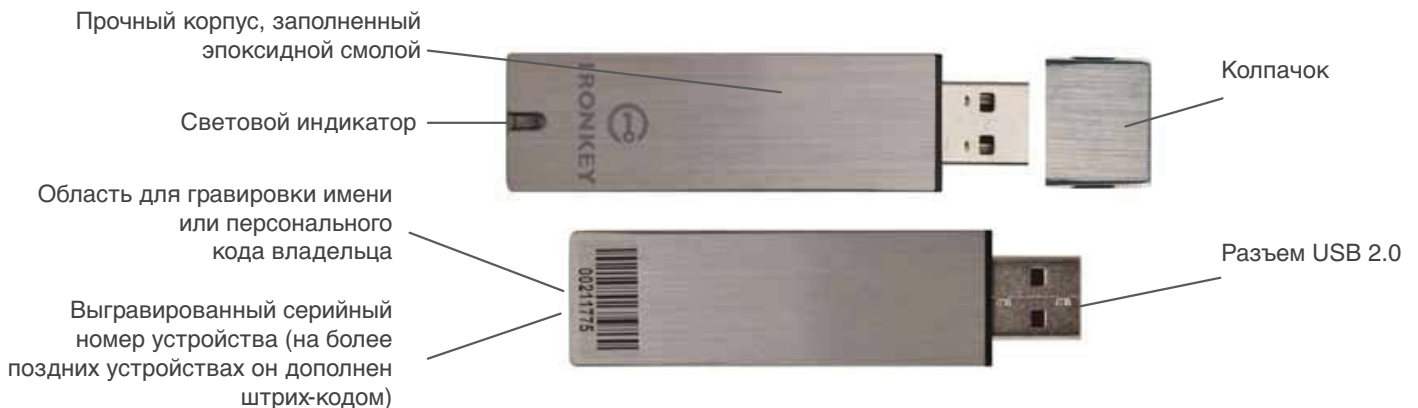
**Водонепроницаемость и защита от внешнего воздействия**  
IronKey способен выдержать любые испытания. Сверхпрочный корпус накопителя заполнен эпоксидной смолой, что не только защищает его от вскрытия, но и обеспечивает водонепроницаемость по военному стандарту США MIL-STD-810F.

**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 накопитель с упором на безопасность. Комбинация самых передовых технологий безопасности обеспечивает защиту данных, а крепкий корпус помогает предотвратить атаки на уровне железа и прямое вскрытие устройства, а также обеспечивает долгий 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

### СКОРОСТЬ

IronKey работает в двухканальном режиме, и поэтому он быстрее обычных флэш-накопителей

### БЕЗОПАСНОСТЬ

Крипточип IronKey осуществляет шифрование на уровне военных стандартов США

### ПРОЧНОСТЬ

Водонепроницаемый металлический корпус защищен от вскрытия

### НАДЕЖНОСТЬ

Самый современный алгоритм снижения износа обеспечивает целостность данных и долгий срок службы устройства

### ИНТЕЛЛЕКТУАЛЬНОСТЬ

Технология "flash-trash" гарантирует полное стирание данных

### ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

Режим чтения и встроенная система защиты от вредоносного ПО



# 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.

### Физическая защита

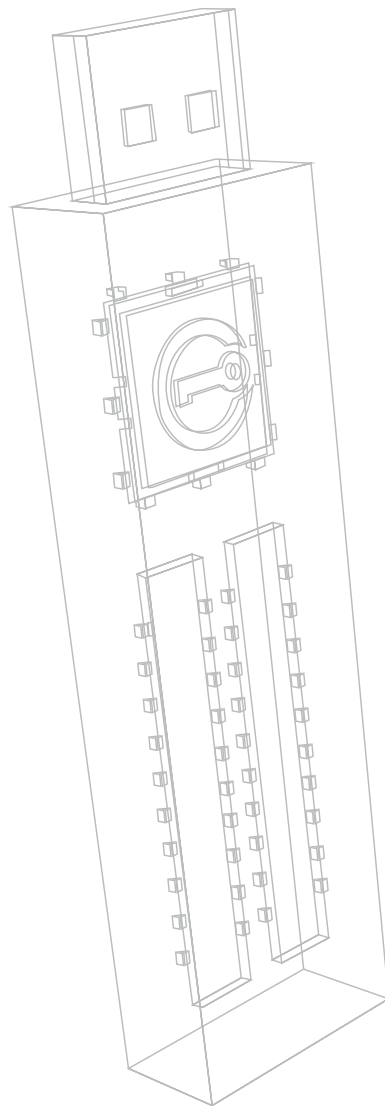
- » Прочный корпус.
- » Ключи шифрования хранятся внутри крипточипа.
- » Компоненты устройства окружены герметичным слоем эпоксидной смолы.
- » Устройство водонепроницаемо по военному стандарту США MIL-STD-810F.

### 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.



# 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)
- » Приложение IronKey Secure Backup (только для Windows)

## 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.

## 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.	<p>Вставьте накопитель в свободный USB порт компьютера</p> 	<p>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.</p>
2.	<p>Появится экран программы «Initialize Your IronKey»</p>	<p>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</p>

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. При необходимости вы можете активировать функцию сброса устройства, отметив флажок «Device Reset». Если эта функция включена, накопитель будет полностью стирать сохраненные данные вместо самоуничтожения, и если вы забыли пароль, вы сможете продолжить пользоваться устройством. Функцию «Device Reset» можно также активировать в меню «Settings» Панели Управления.

4. Начнется процесс инициализации IronKey



Процесс инициализации включает в себя генерацию ключей шифрования AES, создание файловой системы и копирование набора специальных приложений и файлов на защищенный дисковый раздел.

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. Вставьте накопитель в компьютер и введите пароль для разблокирования:	<p>При подключении накопителя появляется экран «Unlock Your IronKey».</p> <ul style="list-style-type: none"><li>• Если экран не появился, вы можете открыть диск IronKey Unlocker двойным щелчком мыши и запустить файл IronKey.exe</li><li>• При правильном вводе пароля произойдет подключение накопителя, и вы получите доступ ко всем файлам. Проверка подлинности пароля осуществляется на аппаратном уровне.</li><li>• Если пароль введен неправильно 10 раз подряд, произойдет полное стирание данных. После каждых трех попыток требуется отключить устройство, а затем подключить его вновь.</li></ul>

<p>2. Выберите желаемое действие после разблокирования.</p>	<p>Отметив соответствующие флажки перед разблокированием, вы можете выполнить следующие действия:</p> <ul style="list-style-type: none"> <li>• просмотреть защищенные файлы</li> <li>• запустить панель управления IronKey Control Panel</li> <li>• разблокировать устройство в режиме чтения, не позволяющем редактировать файлы</li> <li>• подключиться к учетной записи <i>my.ironkey.com</i></li> </ul>
---	---

## 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	<p>IronKey автоматически запускается в режиме виртуального CD-дисковода.</p> <p><b>Примечание</b> Вы можете установить программное обеспечение IronKey Auto-Launch Assistant, автоматически запускающее IronKey Unlocker, как только IronKey подключен к компьютеру. См. раздел «Preferences» в настройках IronKey Control Panel. (только для Mac)</p>
3.	<p>Задайте название устройства и пароль для доступа.</p> 	<p>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> <p>При необходимости вы можете активировать функцию сброса устройства, отметив флажок «Device Reset».</p> <p>Если эта функция включена, накопитель будет полностью стирать сохраненные данные вместо самоуничтожения, и если вы забыли пароль, вы сможете продолжить пользоваться устройством.</p> <p>Функцию «Device Reset» можно также активировать в меню «Settings» Панели Управления.</p>
4.	<p>Появится экран пользовательского соглашения.</p> 	<p>С полным текстом пользовательского соглашения можно ознакомиться на странице <a href="https://www.ironkey.com/terms">https://www.ironkey.com/terms</a></p>

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.

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. Вы можете пользоваться другими приложениями и сервисами IronKey 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».	<b>Примечание</b> Вы можете установить программное обеспечение IronKey Auto-Launch Assistant, автоматически запускающее IronKey Unlocker, как только IronKey подключен к компьютеру. См. раздел “Preferences” в настройках IronKey Control Panel. (только для Mac)	
3.	Введите пароль для разблокирования:		<ul style="list-style-type: none"><li>• При правильном вводе пароля произойдет подключение накопителя, и вы получите доступ ко всем файлам. Проверка подлинности пароля осуществляется на аппаратном уровне.</li><li>• Если пароль введен неправильно 10 раз подряд, произойдет полное стирание данных. После каждого трех попыток требуется отключить устройство, а затем подключить его вновь.</li></ul>
4.	Выберите желаемое действие после разблокирования.	Отметив соответствующие флажки перед разблокированием, вы можете выполнить следующие действия: <ul style="list-style-type: none"><li>• просмотреть защищенные файлы</li><li>• запустить панель управления IronKey Control Panel</li><li>• разблокировать устройство в режиме чтения, не позволяющем редактировать файлы</li><li>• подключиться к учетной записи <i>my.ironkey.com</i></li></ul>	

# 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	Накопитель IronKey может работать на компьютерах семейства x86 под управлением Linux 2.6+. Его также можно настроить и использовать в системах Windows и Mac. Для высокоскоростной передачи данных используйте порт USB 2.0.
2.	Запустите программу ironkey из папки linux накопителя IronKey	IronKey имеет встроенный виртуальный CD-дисковод. Запустите из папки linux программу ironkey.
3.	Примите условия пользовательского соглашения.	Появится экран пользовательского соглашения. Прокрутите соглашение до конца, затем нажмите Q для выхода из режима просмотра. Нажмите Y для принятия соглашения. С полным текстом пользовательского соглашения можно ознакомиться на странице <a href="https://www.ironkey.com/terms">https://www.ironkey.com/terms</a>
4.	Задайте название устройства и пароль для доступа.	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.  При необходимости вы можете активировать функцию сброса устройства, отметив флажок «Device Reset». Если эта функция включена, накопитель будет полностью стирать сохраненные данные вместо самоуничтожения, и если вы забыли пароль, вы сможете продолжить пользоваться устройством. Функцию «Device Reset» можно также активировать в меню «Settings» Панели Управления.
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.

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. Вы можете переносить файлы на устройство и пользоваться другими приложениями и сервисами IronKey в среде Windows. В зависимости от дистрибутива Linux для запуска программы ironkey из папки linux виртуального CD-дисководов 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

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

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

# АКТИВАЦИЯ IRONKEY ENTERPRISE ДЛЯ WINDOWS И MAC

Пользователи устройств IronKey Basic могут активировать функцию IronKey Enterprise, если это продиктовано политикой безопасности организации. Функция IronKey Enterprise позволяет организациям удаленно контролировать устройства IronKey с помощью комплекса приложений и сетевых служб. Для получения подробной информации об IronKey Enterprise, обращайтесь к руководству пользователя IronKey Enterprise.

## ПРИМЕЧАНИЕ

Функция IronKey Enterprise активируется только по требованию системного администратора вашей организации.

» Системный администратор каким-либо образом (например, по электронной почте) предоставит вам код активации.

» Вставьте код активации в поле на экране «Enterprise Activation» в панели управления IronKey (для Windows и Mac). Для активации потребуется соединение с интернетом.



» Следуйте инструкциям на экране для подтверждения того, что вы состоите в организации.

» На накопитель IronKey могут быть установлены дополнительные приложения. Вам может потребоваться сменить пароль доступа к устройству, чтобы он соответствовал требованиям организации.

## РАБОТА С ПАНЕЛЬЮ УПРАВЛЕНИЯ IRONKEY CONTROL PANEL ДЛЯ WINDOWS И MAC





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





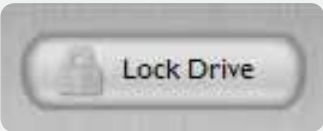
- » Запуск встроенных приложений
- » Доступ к защищенным файлам
- » Запуск приложения Secure Backup для Windows
- » Настройка накопителя
- » Смена пароля для доступа к устройству
- » Форматирование накопителя
- » Безопасная блокировка устройства

Большинство функций панели управления расположены в разделе «Settings».

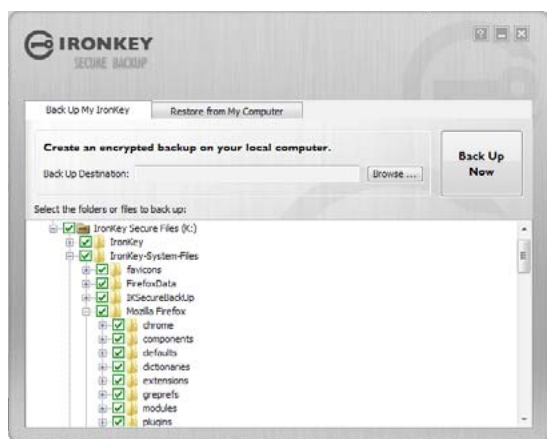
### ПРИМЕЧАНИЕ

На иллюстрациях изображена Windows-версия панели управления.

	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 автоматическая дешифрация. IronKey работает как обычный флэш-накопитель, обеспечивая при этом автоматическую и всегда активизированную защиту данных.</p>
2.	<p>Персональные настройки</p> 	<p>Для редактирования персональных настроек нажмите на кнопку «Preferences» и выполните желаемое действие:</p> <ul style="list-style-type: none"><li>• Включение автоматической блокировки IronKey по истечении времени ожидания</li><li>• Форматирование накопителя</li><li>• Включение режима сброса, в котором устройство не самоуничтожается после десяти неправильных попыток набора пароля. Это позволит вам продолжить пользоваться устройством, если вы забыли пароль.</li><li>• Установка утилиты IronKey Auto-Launch Assistant, автоматически запускающей IronKey Unlocker при подключении IronKey к компьютеру (только для Mac)</li></ul>

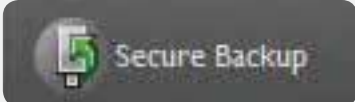
3.	<p>Сообщение Lost and Found</p> 	<p>Функция «Lost and Found» позволяет задать сообщение, выводимое в окне IronKey Unlocker. В случае утери накопителя, вам могут его вернуть, если вы укажете контактную информацию.</p>
4.	<p>Смена пароля доступа к устройству</p> 	<p>Функция «IronKey Password» позволяет сменить пароль доступа к устройству и сохранить его в сетевом хранилище на портале <i>my.ironkey.com</i>. Регулярная смена пароля значительно повышает защищенность данных. Выбирайте только запоминающиеся пароли.</p>
5.	<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. Для перехода на сайт IronKey нажмите CTRL+W. Для просмотра правовых положений нажмите CTRL+N. Для просмотра сертификатов нажмите CTRL+?.</p>
6.	<p>Добавление, переименование и удаление приложений из Списка Приложений</p> 	<p>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. <b>ПРИМЕЧАНИЕ</b></p> <ul style="list-style-type: none"> <li>• Для Mac: приложения, установленные на накопитель, автоматически добавляются в Список Приложений (изначально список пуст).</li> <li>• Элементы списка – это ярлыки приложений. Удаление их из списка не затронет сами приложения.</li> <li>• Список автоматически сортируется по алфавиту.</li> <li>• В список можно добавить любой произвольный элемент: документ, изображение, командный файл и т.д.</li> <li>• В среде Windows файлы, не являющиеся приложениями, открываются в приложениях, сопоставленных типу файла.</li> </ul>
7.	<p>Блокировка и отключение IronKey</p> 	<p>При выборе пункта «Lock Drive» или нажатии CTRL+L (для Windows) или «Lock &amp; Quit» (для Mac) происходит закрытие всех запущенных приложений IronKey, после чего устройство блокируется, и его можно безопасно извлечь из компьютера. Для предотвращения потери данных, закройте все открытые файлы и приложения перед блокировкой устройства.</p>

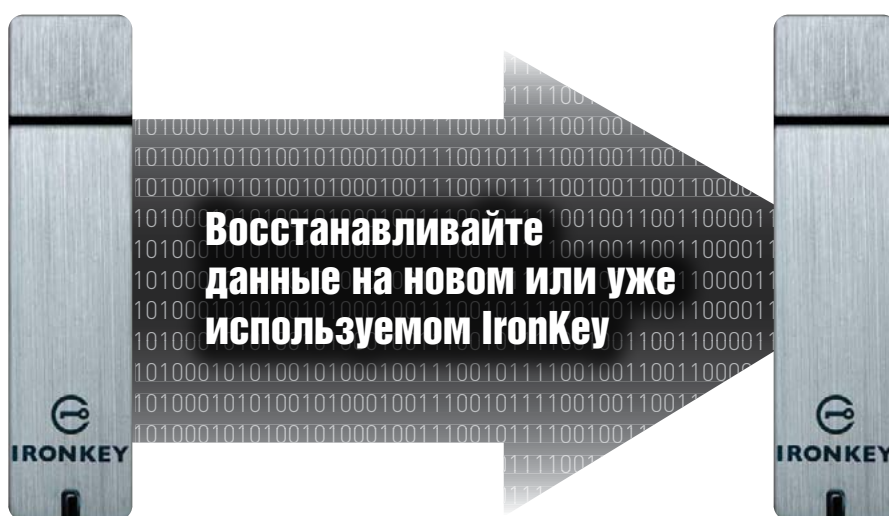
## РАБОТА С SECURE BACKUP ДЛЯ WINDOWS



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.






# 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>	
<p>2. 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>
<p>3. 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 переводе курсора в любое поле ввода пароля.</p>


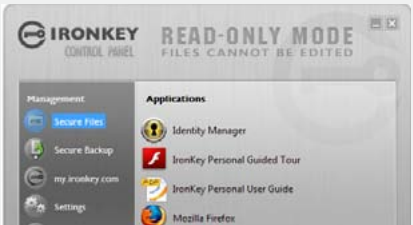
## РАБОТА С НАКОПИТЕЛЕМ В РЕЖИМЕ ЧТЕНИЯ В СРЕДАХ WINDOWS, MAC И LINUX

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](http://forum.ironkey.com)) или оставить отзыв, написав по адресу [feedback@ironkey.com](mailto: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](http://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](http://forum.ironkey.com)) или оставить отзыв, написав по адресу [feedback@ironkey.com](mailto: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](http://forum.ironkey.com)

многотысячное сообщество пользователей IronKey

[www.ironkey.com](http://www.ironkey.com)

общая информация

[support.ironkey.com](http://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](http://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](mailto:feedback@humansolutions.ru)

#### **ИНТЕРНЕТ-САЙТЫ:**

<http://www.humansolutions.ru>

### **НА АНГЛИЙСКОМ ЯЗЫКЕ:**

#### **ОТЗЫВЫ**

[feedback@ironkey.com](mailto:feedback@ironkey.com)

Предложения

[featurerequest@ironkey.com](mailto: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](mailto: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