

# IRONKEY BASIC S200



«Мы одни из первых клиентов IronKey и считаем, что это единственный накопитель, который подходит нашей организации»

Кеннет Роджерс, начальник информационного отдела управления науки и техники министерства внутренней безопасности США.

## АППАРАТНОЕ ШИФРОВАНИЕ ПО 256-БИТНОМУ АЛГОРИТМУ AES

## РАБОТА БЕЗ УСТАНОВКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

## ПОДДЕРЖКА РАЗЛИЧНЫХ ПЛАТФОРМ

### ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

#### Объем памяти

1, 2, 4, 8 или 16 гигабайт

#### Скорость работы

Чтение: до 27 МБ/с  
Запись: до 24 МБ/с

#### Габариты

75 x 19 x 9 мм

#### Вес

23 грамма

#### Водонепроницаемость

Стандарт MIL-STD-810F

#### Рабочая температура

От 0°C до 70°C

#### Допустимая температура хранения

От -40°C до 85°C

#### Допустимая перегрузка

16G RMS

#### Интерфейс

USB 2.0 High-Speed

#### Поддерживаемые ОС

Windows 2000 (SP4), XP (SP2+), Vista и 7  
Linux (2.6+, x86)  
Macintosh OS X (10.4+, Intel)

#### Аппаратное шифрование

Данные: режим сцепления блоков шифротекста  
Ключи: AES 256-бит  
PKI: RSA 2048-бит  
Хеширование: SHA 256-бит  
Сертификат FIPS: 140-2 Level 3

#### Соответствие стандартам Статьи 508

### ЕДИНСТВЕННЫЙ В МИРЕ НАКОПИТЕЛЬ, УДОВЛЕТВОРЯЮЩИЙ ТРЕБОВАНИЯМ ТРЕТЬЕГО УРОВНЯ ПО СТАНДАРТУ FIPS 140-2

IronKey Basic S200 – накопитель, созданный для работы в правительственных, военных и корпоративных сетях. Это единственный в мире накопитель, удовлетворяющий требованиям безопасности третьего уровня по стандарту FIPS 140-2. В нем используется аппаратная реализация шифрования пароля, применяемая Министерством Обороны США для защиты информации грифом «Совершенно Секретно». В основе IronKey Basic S200 лежат технологии семейства продуктов IronKey S200: высочайшая безопасность и качественные чипы памяти, что делает его идеальной платформой для запуска виртуальных машин.

### ПОСТОЯННО АКТИВИРОВАННАЯ ЗАЩИТА ДАННЫХ

При сохранении пользовательских данных на накопитель встроенный крипточип автоматически зашифровывает их по 256-битному алгоритму AES, удовлетворяющему требованиям безопасности третьего уровня по стандарту FIPS 140-2. Ключи шифрования данных генерируются по особому алгоритму и также сохраняются во встроенном крипточипе. В отличие от программных средств, аппаратные средства защиты невозможно отключить, а шифрование происходит быстрее и надежнее, чем в любом программном продукте.

### СООТВЕТСТВИЕ ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ТРЕТЬЕГО УРОВНЯ ПО СТАНДАРТУ FIPS 140-2

IronKey Basic S200 – единственный накопитель в мире, удовлетворяющий требованиям безопасности третьего уровня по стандарту FIPS 140-2.

### ЗАЩИТА ОТ ФИЗИЧЕСКОГО ВОЗДЕЙСТВИЯ

IronKey Basic S200 будет служить вам годами. Прочный цельнометаллический корпус защищает внутренние компоненты от повреждений, а сами компоненты заключены в дополнительную герметичную оболочку. Специальный модуль самоуничтожения стирает ключи шифрования и обнуляет сохраненные данные. Накопитель водонепроницаем и превосходит по этому показателю ряд военных стандартов.

Технологии, реализованные в накопителе IronKey Basic S200, соответствуют требованиям безопасности третьего уровня по стандарту FIPS 140-2.

### МЕХАНИЗМЫ ЗАЩИТЫ ДАННЫХ

Данные, сохраненные на накопитель, остаются недоступными, пока не введен правильный пароль доступа к устройству. Шифрование и проверка подлинности пароля осуществляются на аппаратном уровне, поэтому ни пользователь, ни программа не смогут их отключить. В накопителе также реализован ряд аппаратных решений для противостояния вирусам-червям и прочему вредоносному ПО.

### ПРОСТОТА ИСПОЛЬЗОВАНИЯ

Устройства IronKey не требуют установки дополнительного программного обеспечения и драйверов и работают в системах Windows XP и Vista без обязательного предоставления пользователю прав администратора. Они осуществляют шифрование в автоматическом режиме при обычном «перетаскивании» файлов на накопитель, поддерживают технологию «plug-and-play» и технологию упрощенного резервного копирования, снижая общие затраты на эксплуатацию.

### РАБОТА НА РАЗЛИЧНЫХ ПЛАТФОРМАХ

Устройства IronKey S200 работают в системах Windows 2000, Windows XP и Vista без обязательного предоставления пользователю прав администратора и не требуют установки дополнительного программного обеспечения или драйверов. Они также работают на компьютерах под управлением Linux и Mac OS.

# IRONKEY BASIC S200



## ПРЕИМУЩЕСТВА IRONKEY BASIC

- **МАКСИМАЛЬНО ВОЗМОЖНЫЙ ДЛЯ ФЛЭШ-НАКОПИТЕЛЯ УРОВЕНЬ БЕЗОПАСНОСТИ**
- **ВСТРОЕННЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ**
- **ОТСУТСТВИЕ РИСКОВ, СВЯЗАННЫХ С ПОТЕРЕЙ ИЛИ КРАЖЕЙ УСТРОЙСТВА**
- **ВОЗМОЖНОСТЬ ПРИМЕНЕНИЯ В РАЗРАБОТКЕ ПОЛИТИК СООТВЕТСТВИЯ**
- **РАБОТА В СИСТЕМАХ WINDOWS 2000, WINDOWS XP И VISTA БЕЗ ПРЕДОСТАВЛЕНИЯ ПОЛЬЗОВАТЕЛЮ ПРАВ АДМИНИСТРАТОРА**
- **РАБОТА БЕЗ УСТАНОВКИ ДОПОЛНИТЕЛЬНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ДРАЙВЕРОВ**
- **ПРОСТОТА И УДОБСТВО ИСПОЛЬЗОВАНИЯ**

Выберите подходящий IronKey	Enterprise	Personal	Basic
Удаленное отключение потерянных или украденных устройств	✓		
Управление доступом и отключение устройств	✓		
Отслеживание активности пользователя и системных событий	✓		
Удаленное управление устройством через Интернет	✓		
Устанавливаемые политики безопасности	✓		
Автоматическая проверка на вирусы	✓		
Сервисы RSA SecurID®, CRYPTOCARD, генерация разовых паролей	✓		
Безопасное посещение интернет-ресурсов и защита персональных данных (встроенный Интернет-браузер и приложение Identity Manager, сервис VeriSign® Identity Protection (VIP))	✓	✓	
Встроенная защита от вредоносного ПО	✓	✓	✓
Автоматическое аппаратное шифрование данных	✓	✓	✓
Двухканальная производительная архитектура	✓	✓	✓
Прочный водонепроницаемый корпус	✓	✓	✓

## НАКОПИТЕЛЬ IRONKEY BASIC S200

### БЕЗОПАСНОСТЬ, НАДЕЖНОСТЬ И ПРОСТОТА ИСПОЛЬЗОВАНИЯ

IronKey сотрудничали с ведущими технологическими компаниями в различных областях, чтобы создать накопитель, сочетающий в себе абсолютную безопасность, надежность и простоту эксплуатации.

### НАДЕЖНОСТЬ И ВЫСОЧАЙШЕЕ КАЧЕСТВО

Крепкий цельнометаллический водонепроницаемый корпус IronKey рассчитан на долгие годы использования. Высококачественные внутренние компоненты обеспечивают длительный срок службы чипов памяти, в 10-20 раз превышающий таковой у обычных накопителей.

### АППАРАТНАЯ ЗАЩИТА И УПРАВЛЕНИЕ КЛЮЧАМИ ШИФРОВАНИЯ

При подключении накопителя IronKey к компьютеру пользователь должен ввести пароль, чтобы получить доступ к файлам. В отличие от программных продуктов, осуществляющих шифрование данных, IronKey никогда не копирует на компьютер AES-ключи шифрования, и поэтому защищен от вредоносного ПО, а также от взлома методом холодной перезагрузки.

Пароль доступа к IronKey Basic S200 невозможно подобрать, так как счетчик попыток ввода пароля – это аппаратный модуль, расположенный внутри крипточипа. Если пароль введен неправильно 10 раз подряд, запускается запатентованный аппаратный механизм самоуничтожения "flash trash", который полностью и бесследно уничтожает информацию.

### СОВМЕСТИМОСТЬ С СИСТЕМАМИ ЗАЩИТЫ КОНЕЧНЫХ ТОЧЕК СЕТИ

IronKey Basic S200 совместим с большинством ведущих систем защиты конечных точек сети. Каждому устройству в системе присваивается уникальный идентификационный номер, что облегчает применение политик безопасности.



Разработано и



изготовлено в США

©IronKey, Inc. 2009

Все права защищены. Воспроизведение данного документа или его частей допускается только с письменного согласия компании IronKey, Inc. IronKey и логотип IronKey являются зарегистрированными торговыми марками компании IronKey, Inc. Windows и прочие торговые марки являются собственностью их зарегистрированных владельцев. Функциональность и характеристики устройства могут быть изменены без письменного уведомления. Данные о скорости чтения и записи получены в лабораторных условиях. Данные реальной эксплуатации могут отличаться. Заявленный объем памяти накопителя является приблизительным и не будет полностью доступен для сохранения пользовательских данных.

### СОЗДАНИЕ ЭФФЕКТИВНОЙ СИСТЕМЫ БЕЗОПАСНОСТИ

Команда IronKey – это специалисты мирового уровня в области шифрования данных, систем авторизации и сетевой безопасности. Накопитель IronKey и сопутствующие сервисы способны защитить пользовательские данные от самых разнообразных атак: тотального перебора пароля, прослушивания USB-шины, атак по сторонним каналам, а также попыток разобрать устройство или чип.