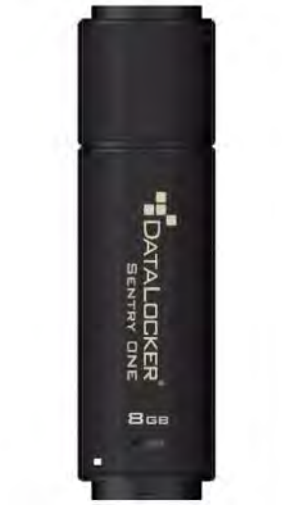
# Sentry ONE Руководство пользователя

*DataLocker Inc.*

Апрель, *2018*




## Sentry ONE
## "Стандартная" и "Управляемая" версии

# Содержание



## Про данное руководство

Устройство безопасного хранения данных DataLocker® Sentry ONE доступно в двух версиях: "стандартной" и "управляемой". Стандартная версия устройства не требует наличия платформы управления. Управляемая версия требует наличия лицензии на устройство и управляется с помощью платформ SafeConsole либо Ironkey EMS.™ SafeConle и Ironkey EMS являются безопасными облачными/стационарными платформами управления, позволяющими вашей организации централизовано управлять USB-совместимы ми устройствами хранения данных с легкостью и высокой эффективностью.

В данном руководстве содержатся инструкции по установке и инициализации обеих версий устройства.

## Быстрый запуск

Установка на Windows (7, 8.1, 10) и macOS (v.10.9.x - 10.13.x)

1. Подключите устройство к компьютеру через USB порт.
2. Следуйте инструкциям на экране в открывшемся диалоговом окне "Установка устройства" Если диалоговое окно не открылось, откройте его вручную:
   - Windows: Пуск > Компьютер > Unlocker > Unlocker.exe
   - macOS: Finder > Unlocker > Unlocker
3. После завершения процесса установки устройства, вы можете записать важные для вас файлы на устойство PRIVATE_USB и они автоматически будут зашифрованы.

Некоторые версии ОС Windows предлагают выполнить перезагрузку после первого подключения устройства. Вы можете смело отказаться от перезагрузки, потому что никакие новые драйверы или приложения не были установлены.

## Об устройстве

DataLocker® Sentry ONE - это совместимый с USB 3.0 портативный flash-носитель со встроенной системой защиты с помощью пароля и шифрования данных. Целью его разработки было создание наиболее защищенного USB носителя в мире. Располагая таким устройством вы можете безопасно переносить с собой свои данные и файлы куда бы вы ни направлялись.


**Рис.1:** DataLocker Sentry ONE

## В чем отличие от обычного жесткого диска?

**Сертифицировано FIPS 140-2 Уровень 3.** Sentry ONE - это FIPS-сертифицированное устройство, поэтому вы можете не беспокоиться о соответствии требованиям нормативных документов.

**Аппаратное шифрование данных.** Специальный "крипточип" внутри устройства защищает ваши данные с уровнем безопасности, соответствующим требованиям к хранению информации, которая представляет собой государственную тайну. Эта технология защиты данных работает на постоянной основе и не может быть отключена.
**Защита паролем.** Доступ к устройству защищен паролем. Не сообщайте свой пароль никому и в случае, если устройство будет утеряно или украдено, никто не сможет получить доступ к вашим данным.
**Сброс настроек устройства.** Если крипточип выявляет попытку физического взлома или количество неудачных попыток ввода пароля превышает 10, устройство инициирует процесс сброса настроек. **Важно:** При сбросе настроек все данные, хранящиеся на устройстве стираются и устройство совершает откат к заводским настройкам, поэтому крайне важно помнить свой пароль.

**Защита от автозапуска вредоносного ПО (только в управляемой версии).** Устройство обладает способностью защищать себя от актуальных угроз, распространяемых через вредоносное ПО, выявляя и предотвращая автозапуск и выполнение неодобренных програм. Защита также может быть включена в режиме "Только чтение", если вы подозреваете, что хост-комппьютер заражен вирусами.

**Простота управления.** Устройство DataLocker оснащено панелью управления, программой для доступа к вашим файлам, управления устройством и редактирования настроек, изменения пароля и безопасной блокировки устройства.

## В каких операционных системах может использоваться устройство?

- Windows® 10
- Windows® 8.1
- Windows® 7
- macOS® (10.9 - 10.13)
- Linux (2.6 или выше) **Примечание:** Разблокировщик Linux CLI не поддерживает функции требующие доступ к сети. Например, установка устройства или изменение пароля.

**Некоторые приложения работают только на определенных операционных системах:**

**Только для Windows**

- Виртуальная клавиатура (английская раскладка)
- Обновления для устройства

## Совместимость с Citrix

Устройство модели Sentry ONE совместимо с:

- XenApp 7.14
- XenApp 7.15 LTSR
- XenApp 7.16
- XenApp 7.17
- XenDesktop 7.14
- XenDesktop 7.15 LTSR

- XenDesktop 7.16
- XenDesktop 7.17

## Технические характеристики

Для получения более подробной информации об устройстве, откройте страницу **Информация об устройстве на панели управления** DataLocker.

| Спецификация | Подробности |
|---|---|
| Объем* | 4Гб, 8Гб, 16Гб, 32Гб, 64Гб, 128Гб |
| **Скорость**** | USB 3.0:<br>- 4**Гб**: 80**Мб/с чтение**, 12**Мб/с запись**<br>- 8**Гб и** 16**Гб**: 165**Мб/с чтение**, 22**Мб/с запись**<br>-32**Гб**: 250**Мб/с чтение**, 40**Мб/с запись**<br>- 64GB & 128**Гб**: 250**Мб/с чтение**, 85**Мб/с запись**<br><br>USB 2.0:<br>- 4**Гб**: 30**Мб/с чтение**, 12**Мб/с запись**-<br>8**Гб**-128**Гб**: 30**Мб/с чтение**, 20**Мб/с запись** |
| Габариты | **77**.**9**мм x **22**.**2**мм x **12**.**05**мм |
| **Влагоустойчивость** | **до** 1.2**м**<br>**Соответствует** IEC 60529 IPX8<br>**При использовании устройство должно быть сухим и чистым** |
| Температура | Рабочая: от 0°C до 60°C<br>Хранения: от -20°C до 85°C |
| Аппаратное шифрование | 256-bit AES (режим XTS) |
| Совместимость с EMI/EMC | TAA Compliant, FCC, CE, VCCI & KC,<br>RoHS & WEEE |
| Сертификация | FIPS 140-2 Уровень 3<br>Совместимо с USB 3.0 иUSB 2.0<br>Требует 2 свободные буквы раздела |
| Совместимость с ОС | Windows 10, Windows 8.1, Windows 7 (SP1)<br>macOS v.10.9.x-10.13.x Linux 2.6.x*** |
| Общедоступность | Панель управления DataLocker разрабатывалась в соответствии с требованиями Раздела 508. Для пользователей с ограниченными возможностями имеется специальная навигация и поддержка скрин-ридера |
| Гарантия | до 2-х лет |

Разработано и собрано в США. Устройство модели Sentry ONE не требуют установки дополнительного ПО или драйверов.
* Заявленный объем является приблизительным. Некоторое количество дискового пространства отведено под встроенное ПО.
** Скорость может варьироваться в зависимости от аппаратных средств и ПО хост-компьютера.
*** Ограниченный набор функций. Отсутствуют функции с онлайн управлением.

### Рекомендации по эксплуатации

1. Блокируйте устройство:

- когда не используете его
- перед отключением от компьютера
- перед переходом системы в спящий режим

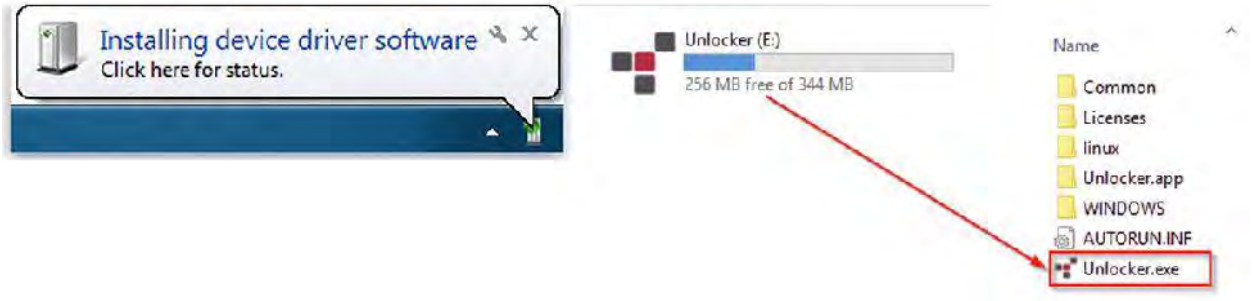
2. Никогда не отсоединяйте устройство при горящем LED-индикаторе.
3. Никому не сообщайте свой пароль.
4. Сканируйте операционную систему компьютера на вирусы перед подключением к нему устройства.

## Настройка устройства

Чтобы убедиться, что устройство получает достаточное электропитание,подключите его прямо к порту USB 2.0/3.0 ноутбука или стационарного компьютера. Не подключайте его к перифирийным устройствам, оснащенным USB портом, таким как USB-клавиатура или USB-концентратор. Первоначальная установка устройства должна производиться на компьютер с операционной системой Windows или mac OS.

### Доступ к устройству (среда Windows)

1. Подключите зашифрованный носитель Sentry ONE к свободному USB порту ноутбука или стационарного компьютера и дождитесь, когда система определит устройство.
   - Пользователи Windows 7/8.1/10 получат оповещение о драйвере устройства.
   - Как только процесс обнаружения устройства завершится, Windows инициирует процесс инициализации.
2. Выберите опцию **Unlocker.exe в разделе** Разблокировщик, к которому можно получить доступ через Проводник. Обратите внимание, что буква раздела может отличаться, так как она зависит от буквы соседнего свободного раздела. Буква привода может изменяться в зависимости от количества подключенных к компьютеру устройств. На иллюстрации ниже буква устройства - E:.



## Доступ к устройству (среда macOS)

1. Подключите зашифрованный носитель Sentry ONE к свободному USB порту ноутбука или стационарного компьютера и дождитесь, когда система определит устройство.

2. Дважды кликните на разделе **Unlocker**, который появится на рабочем столе, чтобы запустить процесс инициализации.

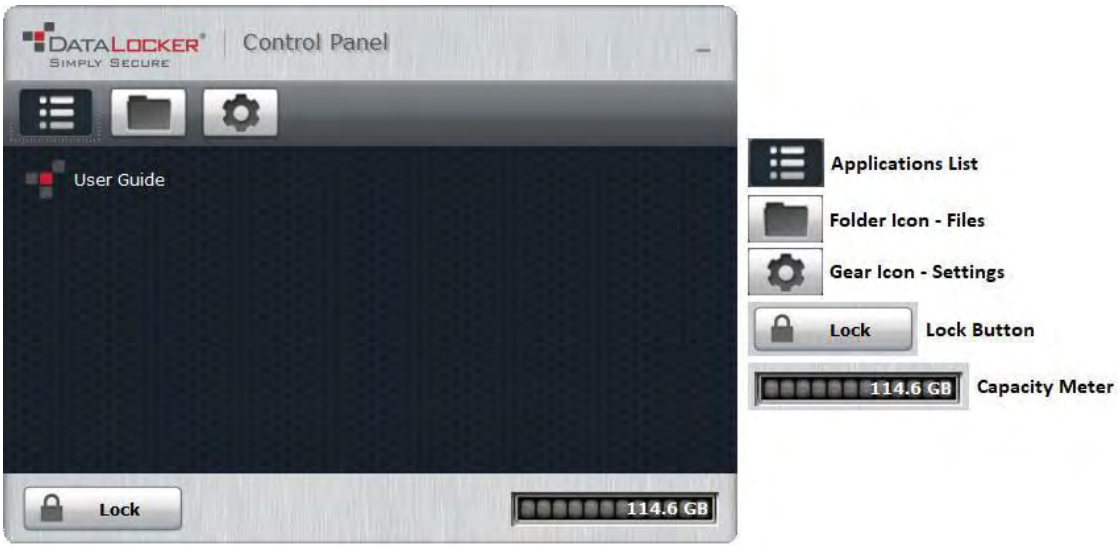
- Если раздел Unlocker не появляется на рабочем столе, откройте Finder и расположите ярлык Unlocker в левой стороне окна Finder (под блоком "Устройства") Выделите раздел и дважды кликните на иконке приложения Unlocker в окне Finder. Данное действие запустит процесс инициализации.

## Базовая инициализация устройства

Процесс инициализации носителя данных Sentry ONE зависит от того, какую версию устройства вы приобрели: **Стандартную** (опциональное управление) или **Управляемую** (принудительное). При инициализации устройства Sentry ONE управляемой версии потребуется ввести код активации или токен связи от Ironkey EMS или SafeConsole. Ironkey EMS и SafeConsole требуют лицензию устройства для активации. Лицензия приобретается отдельно. Для получения более подробной информации по инициализации Sentry ONE управляемой версии смотрите: Установка управляемой версии устройства.

1. Выберите нужный язык из списка. По умолчанию ПО устройства использует активный язык вашей операционной системы (если есть возможность).
2. Ознакомьтесь с лицензионным соглашением, примите его условия и нажмите **Продолжить.**
3. Введите пароль устройства в текстовое поле "Пароль", затем повторно введите пароль в текстовое поле "Подтвердить". Этот пароль защищает данные, хранящиеся на носителе. Пароли чувствительны к регистру и должны состоять как минимум из 4 символов (включая пробелы).
4. При инициализации на платформе Windows, вам будет доступен выбор файловой системы при форматировании носителя PRIVATE_USB: FAT32, NTFS или exFAT. Для получения более подробной информации смотрите Форматирование устройства.
5. Нажмите **Продолжить**. Устройство завершит процесс инициализации. После его завершения откроется панель управления DataLocker. Теперь ваше устройство готово хранить и защищать ваши данные.

## Панель управления DataLocker



### Апгрейд устройства от стандартной до управляемой версии (только для Windows и macOS)

По просьбе вашего системного администратора можно выполнить апгрейд устройства DataLocker Sentry ONE стандартной версии до управляемой версии. Управляемые устройства совместимы с SafeConsole и IronKey EMS. При выполнении апгрейда устройства вам потребуется активировать его с помощью токена связи или кода активации, предоставляемого вашим администратором. Для завершения этого процесса потребуется соединение с Интернет.

**Важно:** Выполняйте апгрейд только в том случае, если системный администратор просит вас активировать устройство с помощью SafeConsole или IronKey EMS. Процесс апгрейда необратим. Ваше устройство останется управляемым даже после сброса всех настроек.

Чтобы выполнить апгрейд со стандартной версии устройства до управляемой, выполните следующие действия:

1. Получив токен связи или код активации от вашего системного администратора запустите панель управления DataLocker и выберите **Настройки (иконка с шестеренкой)**. Для получения более подробной информации смотрите Панель управления DataLocker
2. В левой боковой панели нажмите **Инструменты**, затем **Управление устройством**.
3. Вставьте токен связи или код активации в текстовое поле "Активация".
4. Следуйте инструкциям на экране.
5. На устройство могут быть установлены дополнительные приложения, основываясь на политике управления носителем, установленной вашим администратором От вас также может потребоваться изменить пароль для того, чтобы он соответствовал политике безопасности паролей, принятой в вашей организации.

## Установка устройства управляемой версии с помощью SafeConsole

Процесс инициализации начинается с подготовки устройства к соединению с сервером SafeConsole. Количество шагов при регистрации носителя Sentry ONE корпоративной версии в SafeConsole зависит от политики, установленной вашим администатором. Не все диалоговые окна выводятся на экран.

Потребуется ввести токен связи. Данный токен получает системный администратор, используя руководство по быстрому соединению в пользовательском интерфейсе SafeConsole.

Пользователям, не имеющим доступ к Серверу Управления следует связаться с нашим отделом продаж по эл. почте или по телефону: sales@datalocker.com /(913)310-9088

1. Введите токен связи SafeConsole, алгоритм получения которого описан выше. Ознакомьтесь с лицензионным соглашением, примите его, и нажмите кнопку **Активировать** в левом нижнем углу.
   - **Опционально применяемые политики.** Применение данных политик зависит от решения системного администратора. Если политика применяется, диалоговое окно, связанное с ней появится в процессе регистрации.
     - Подтвердить право собственности на устройство. Введите логин и пароль от системы Windows, установленной на компьютере, к которому подключено устройство хранения данных.
     - Дополнительная информация об устройстве. Обязательная информация о вас и вашем устройстве. Набор обязательных полей может отличаться.
     - Уникальный токен пользователя: Этот токен напрямую ассоциирован с аккаунтом конечного пользователя и предоставляется системным администратором.
     - Подтверждение регистрации администратором. Системный администратор может установить необходимость подтверждения регистрации устройства с его стороны.

2. Введите безопасный пароль и подтвердите его. Если созданный пароль отвечает требованиям, отображаемым справа от текстовых полей, нажмите **Продолжить**. Требования к паролям зависят от политики, установленной администратором.
3. Выберите безопасную файловую систему для носителя (см. Форматирование устройства) и нажмите **Продолжить**.
4. Устройство завершит процесс установки и будет готовым к использованию. Получить доступ к данным на зашифрованном носителе можно нажав на **иконку папки** в верхнем меню. Чтобы открыть панель настроек устройства кликните на **иконку с шестеренкой**. Для получения более подробной информации см. Панель управления DataLocker.

### Установка устройства управляемой версии с помощью Ironkey EMS

Процесс инициализации начинается с подготовки устройства к соединению с сервером Ironkey EMS.

Потребуется код активации Ironkey EMS. Код активации Ironkey EMS получает системный администратор через консоль Ironkey EMS Console. Данный код может быть отправлен конечному пользователю по электронной почте.

Пользователям, не имеющим доступ к Серверу Управления следует связаться с нашим отделом продаж по эл. почте или по телефону: sales@datalocker.com / (913)310-9088

1. Введите код активации Ironkey EMS, алгоритм получения которого описан выше. Ознакомьтесь с лицензионным соглашением, примите его, и нажмите кнопку **Активировать** в левом нижнем углу.
2. Введите безопасный пароль и подтвердите его. Если созданный пароль отвечает требованиям, отображаемым справа от текстовых полей, нажмите **Продолжить**.
3. В зависимости от политики, установленной вашим системным администратором вам может потребоваться создать онлайн аккаунт. На адрес электронной почты конечного пользователя будет выслано письмо с инструкциями, описывающими процесс создания онлайн аккаунта . После того, как аккаунт был верифицирован, нажмите **OK**.
    - Пользователь получит оповещение об ошибке, если аккаунт не был создан или возникла проблема при его верификации.
4. Выберите безопасную файловую систему для носителя (см. Форматирование устройства) и нажмите **Продолжить**.
5. Устройство завершит процесс установки и будет готово к использованию. Получить доступ к данным на зашифрованном носителе можно нажав на **иконку папки** в верхнем меню. Чтобы открыть панель настроек устройства кликните на **иконку с шестеренкой**. Для получения более подробной информации см. Панель управления DataLocker.

## Эксплуатация устройства - функции, доступные в "стандартной" и "управляемой" версиях

### Получение доступа к файлам

После разблокировки устройства вы можете получить доступ к хранящимся на нем файлам. Файлы автоматически шифруются и дешифруются, когда вы сохраняете или открываете их на устройстве. Данная технология обеспечивает такое же удобство при работе, как и при использовании обычных носителей, но система "постоянной безопасности" не прекращает свою работу ни на секунду.

Чтобы получить доступ к файлма:

1. Нажмите **Файлы** в меню панели управления DataLocker.
    - Windows: Откроется проводник с корневой директорией носителя PRIVATE_USB.

- macOS: откроется Finder с корневой директорией носителя PRIVATE_USB.

2. Выполните одно из следующих действий:
   - Чтобы открыть файл, дважды кликните на иконке файла на носителе PRIVATE_USB. • Чтобы сохранить файл, перетащите его со своего компьютера в директорию PRIVATE_USB.

**Совет:** Вы также можете получить доступ к файлам кликнув правой кнопкой мыши на **иконку DataLocker** на панели задач Windows и выбрать **Безопасные файлы.**

## Разблокировка в режиме "Только чтение"

Вы имеете возможность разблокировать устройство в режиме "только чтение", чтобы запретить модификацию файлов на носителе. Например, при использовании на чужом компьютере, установка режима "Только чтение" предотвратит возможное заражения файлов на вашем устройстве вредоносным ПО или их несанкционированную модификацию. Устройства корпоративной версии могут принудительно разблокироваться в состоянии "только чтение", если администратор активировал данную функцию.
При работе в данном режиме, панель управления DataLocker отобразит текст "Режим Только чтение".В данном режиме запрещено выполнять любые операции, предусматривающие модификацию файлов на носителе. Например, вы не сможете отформатировать устройство, восстановить приложения, отредактировать список приложений, а также редактировать файлы на носителе.

Чтобы разблокировать устройство в режиме "Только чтение":

1. Подключите устройство к USB порту хост-компьютера и запустите файл **Unlocker.exe**.
2. Отметьте флажок **"Только чтение"** под полем ввода пароля.
3. Введите пароль вашего устройства и нажмите **Разблокировать**. Откроется панель управления DataLocker с сообщением "Режим Только чтение" внизу.

## Изменение сообщения разблокировки

Сообщение разблокировки - это произвольный текст, который всегда выводится в окне разблокировщика, когда вы разблокируете устройство. Данная функция позволяет вам изменять данное сообщение. Например, если вы указали свои контактные данные, в случае утери устройства, тому, кто его найдет будет проще вам его вернуть. В корпоративной версии данная функция может быть отключена системным администратором.

Чтобы изменить сообщение разблокировки:

1. В меню панели управления DataLocker нажмите **Настройки**.
2. Нажмите **Свойства** в левой боковой панели.
3. Введите текст сообщения в поле "Сообщение разблокировки". Длина сообщения ограничена длиной поля ввода. (приблизительно 7 строк и 200 символов).

## Блокировка устройства

Всегда блокируйте ваш носитель, когда вы не работаете с ним, чтобы предотвратить любой несанкционированный доступ к данным. Вы можете заблокировать устройство вручную, либо задать время, по истечении которого устройство будет заблокировано автоматически при бездействии. В корпоративной версии данная функция может быть отключена администратором.

**Предупреждение:** По умолчанию, если во время автоблокировки устройства открыто какое-либо приложение или файл, система не будет закрывать их принудительно. Однако вы можете задать настройку автоблокировки, которая вызовет принудительно закрытие открытых приложений и файлов на устройстве при его автоблокировке, что может привести к потере несохраненных данных.

Если ваши файлы были повреждены в результате принудительной автоблокировки при отключении устройства от компьютера до его блокировки, у вас будет возможность восстановить эти файлы запустив CHKDSK и использовав специализированное ПО для восстановления данных (только Windows).

Чтобы заблокировать устройство вручную:

1. Нажмите **Блокировать** в нижнем левом углу панели управления DataLocker чтобы безопасно заблокировать устройство.
    - Также заблокировать можно сочетанием "горячих клавиш": **CTRL + L** (только Windows) или кликом правой кнопкой мыши на **иконке DataLocker** в системном трее и выбрать **Блокировать устройство**.

**Примечание:** Устройство корпоративной версии автоматически блокируется если администратор отключает его в удаленном режиме. Вы не сможете разблокировать устройство до тех пор, пока системный администратор не включит его снова.

Чтобы настроить таймер автоблокировки:

1. Разблокируйте устройство и нажмите **Настройки** в меню панели управления DataLocker.
2. Выберите **Свойства** в левой боковой панели.
3. Отметье **флажок** автоблокировки устройства и установите один из следующих временных интервалов: 5, 15, 30, 60, 120, или 180 минут.

Чтобы запустить CHKDSK (только Windows):

1. Разблокируйте устройство.
2. Нажмите кнопку с логотипом WINDOWS + R, чтобы открыть командную строку.
3. Введите CMD и нажмите ENTER.
4. В командной строке введите CHKDSK, букву раздела PRIVATE_USB, затем "/F /R". К примеру, если буква раздела PRIVATE_USB - G, вам нужно ввести: CHKDSK G: /F /R
5. Используйте программное обеспечение для восстановления данных для того, чтобы восстановить ваши файлы.

## Ввод паролей с помощью виртуальной клавиатуры

Если вы разблокируете устройство на незнакомом компьютере или беспокоитесь по поводу возможного использования хакерских приложений, считывающих данные с клавиатуры или дисплея, используйте виртуальную клавиатуру. Она обеспечивает защиту вашего пароля, позволяя вводить буквы и цифры. Базовые механизмы защиты виртуальной клавитуры позволяют обойти множество троянов, а также вредоносного ПО, считывающего данные с клавиатуры и экрана копмьютера.
**Примечание:** Данная функция использует стандартную раскладку QWERTY. Она доступна только в среде Windows, а в языковых настройках обязательно должен быть выбран английский язык.

Чтобы ввести пароль с помощью виртуальной клавиатуры (только Windows):

1. Откройте ее, выполнив одно из следующих действий:
    - В поле ввода пароля нажмите на **иконку виртуальной клавиатуры**.
    - Когда курсор находится в поле ввода пароля нажмите **CTRL+ALT+ V**.
2. Введите свой пароль, используя клавиши виртуальной клавиатуры и нажмете **Enter**.

Вы также можете использовать виртуальную клавиатуру в сочетании с обычной клавиатурой вводя символы вашего пароля как на одной, так и на другой.

**Совет:** Нажмите **Расположить случайным образом**, чтобы изменить порядок введенных символов случайным образом. Это обеспечивает дополнительную защиту от атак хакерского ПО.

**Примечение:** Если вы набираете пароль на виртуальной клавитуре, нажаитые клавиши быстро исчезают. Это делается для того, чтобы не позволить хакерскому ПО считать символы, которые вы ввели. Чтобы отключить данную функцию кликните на иконке (рядом с кнопкой Выход) и выберите **Выключить защиту от хакерского ПО**.

## Управление паролями

Вы имеете возможность изменить пароль вашего устройства во вкладке "Пароль" панели управления DataLocker.

В устройствах корпоративной версии настройки политики паролей определяются системным администратором. В некоторых случаях вам может потребоваться изменить свой пароль, чтобы обеспечить его соответствие с действующей политикой паролей. Когда от вас требуется изменить свой пароль, окно "Изменение пароля" автоматически откроется при следующей разблокировке устройства. Если в этот момент устройство используется, оно заблокируется и вам потребуется изменить свой пароль, перед тем, как разблокировать его снова.

**Примечание:** Когда требуется ввод пароля, например, если вы хотите получить доступ к устройству или в процессе изменения пароля, вы можете использовать виртуальную клавиатуру вместо обычной для ручного ввода пароля.

Для того, чтобы изменить свой пароль:

1. Разблокируйте устройство и нажмите **Настройки** в панели меню.
2. Выберите **Пароль** в левой боковой панели.
3. Введите ваш текущий пароль в соответствующее поле.
4. Введите ваш новый пароль и подтвердите его в соответствующих полях.
5. Нажмите **Изменить пароль**.

## Форматирование устройства

Устройство должно быть отформатировано в процессе инициализации перед тем, как вы сможете использовать его для хранения своих данных.

При инициализации устройства на платформе Windows, вам будет предоставлен выбор файловой системы для форматирования PRIVATE_USB: FAT32, NTFS или exFAT.

**Данные опции доступны только на платформе Windows, на macOS форматирование автоматически происходит в файловой системе FAT32.**

- **FAT32**
  - Плюсы: кроссплатформенная совместимость (Windows, macOS и Linux)
  - Минусы: ограничение максимального размера файла - 4Гб
- **NTFS**
  - Плюсы: нет ограничений по размеру файла
  - Минусы: ограниченная сместимость - Windows и macOS (только чтение)
- **exFAT**
  - Плюсы: нет ограничений по размеру
  - Минусы: Microsoft ограничивает использование по условиям лицензии

После инициализации и форматирования PRIVATE_USB, на устройстве будут стерты все файл, а также ваш Список приложений, но пароль устройства и его настройки сохранятся.

**Важно:** Перед форматированием устройства, сделайте резервную копию файлов с PRIVATE_USB на какой-либо сторонний носитель, например, облачное хранилище или жесткий диск вашего ПК.

Чтобы отформатировать устройство:

1. Разблокируйте устройство и нажмите **Настройки** в меню панели управления DataLocker.
2. Выберите **Инструменты** в левой боковой панели.
3. Под блоком "Состояние устройства", выберите формат файла и нажмите **Переформатировать раздел.**

## Поиск информации об устройстве

Используйте индикатор объема, расположенный в правом нижнем углу панели управления DataLocker, чтобы узнать какое количество свободного места доступно на вашем носителе. Зеленая полоса индикатора отображает занятое пространство устройства. То есть, индикатор будет полностью зеленым, если на носителе не осталось свободного места. Белый текст на индикаторе объема показывает, сколько свободного места на нем осталось.

Для получения общей информации об устройстве, см. страницу Информация об устройстве.

Чтобы вывести на экран информацию об устройстве:

1. Разблокируйте устройство и нажмите **Настройки** в меню панели управления DataLocker.
2. Выберите **Информация об устройстве** в левой боковой панели.

Раздел "О данном устройстве" включает в себя следующие данные об устройстве:

- Номер модели
- Серийный номер
- Версия аппаратного средства и ПО
- Дата выпуска
- Консоль управления
- Буква раздела
- Буква раздела Разблокировщика
- Операционная система и привилегии администратора

**Примечание:** Чтобы посетить официальный сайт производителя или получить более подробную информацию о документации и сертификатах продукции DataLocker, нажмите одну из информационных кнопок на странице Информация об устройстве.

**Совет:** Нажмите **Копировать**, чтобы скопировать информацию об устройстве в буфер обмена для ее дальнешей отправки по эл. почте или составления запроса в службу тех. поддержки.

## Редактирование Списка приложений

Список приложений, расположенный в панели управления DataLocker, это область, с помощью которой вы можете осуществлять быстрый запуск встроенных приложений и файлов. В ней находятся ярлыки соответствующих файлов. Операции по управлению данным списком не затрагивают сами файлы.

Чтобы отредактировать Список приложений:

1. Разблокируйте устройство. Панель управления DataLocker откроется вместе со списком приложений по умолчанию.
2. Если панель управления DataLocker уже открыта, нажмите **иконку Приложения** в меню, чтобы просмотреть список приложений. Выполните одно из следующих действий:
    - Чтобы добавить файл или ярлык: Перетащите файл с рабочего стола в область Списка приложений и он будет добавлен в список. Вы также можете кликнуть правой кнопкой мыши на область Список приложений и выбрать **Добавить приложение**.
    - Чтобы удалить или переименовать элементы: Кликните правой кнопкой мыши на файле и выберите нужное действие из контекстного меню.

- Чтобы отсортировать или изменить тип отображения иконок в списке: Кликните правой кнопкой мыши в области Список приложений и выберите: Большие иконки, Список, Плитка или Сортировать в алфавитном порядке.

Функционал Списка приложений:

- В этот список вы можете добавлять любые файлы, включая документы, изображения и исполняемые файлы.
- Файлы, не являющиеся исполняемыми, операционная система откроет в приложении ассоциированном с файлами данного типа.
- Исполняемые файлы Windows будут невидимым на macOS. Аналогичным образом, исполняемые файлы macOS application не будут отображаться на компьютерах с ОС Windows.

### Сброс настроек устройства

Вы имеете возможность осуществить откат устройства к заводским настройкам. Это действие приведет к удалению всех файлов на носителе и созданию нового ключа безопасности.

Администратор может отключить данную опцию на устройствах корпоративной версии. Если вам нужно выполнить сброс настроек устройства, свяжитесь с вашим системным администратором.

Чтобы осуществить сброс настроек:

1. Разблокируйте устройство.
2. Кликните правой кнопкой мыши на **иконке DataLocker** в системном трее.
3. Выберите **Сбросить настройки**.

Ваше устройство выполнит откат к заводским настройкам.

## Эксплуатация устройства - Функции, доступные только в "управляемой" версии

### Доступ к устройству при забытом пароле

Если вы забыли свой пароль и администратор дал вам права на его собственноручное изменение, вы можете создать новый пароль. Если администратор не предоставил вам таких прав, свяжитесь с ним, чтобы он помог вам с изменением пароля.

Чтобы изменить свой пароль:

1. Подключите устройство и запустите Разблокировщик.
2. Нажмите **Помощь с паролем**.
3. В окне "Помощь с паролем", выберите **Изменить пароль**. Следуйте инструкциям на экране чтобы завершить процесс создания нового пароля.
4. В зависимости от платформы управления, вы можете либо получить сообщение по эл. почте с инструкциями, как получить код восстановления, либо вам будет нужно связаться со своим администратором, чтобы получить этот код. От вас может потребоваться код запроса и серийный номер устройства.
   - Скопируйте и вставьте код восстановления точно в таком же виде, в котором он был вам прислан. Вам дается 10 попыток ввести правильный код восстановления перед тем, как будет произведен сброс настроек устройства.
5. Введите ваш новый пароль (можно использовать виртуальную клавиатуру) и подтвердите его в соотвующих полях, затем нажмите **Изменить пароль**.

## Сканирование устройства для выявления вредоносного ПО

Malware Scanner - это технология самоочищения, которая выявляет и удаляет вредоносное ПО на вашем носителе, проникшее из зараженного файла или компьютера. Сканер вредоносного ПО может включаться/отключаться администратором. Он работает на базе сигнатур баз данных антивирусной программы McAfee®, которые постоянно обновляются, чтобы противостоять актуальным угрозам. Сканер проверяет наличие обновлений, сканирует ваше устройство, затем формирует отчет и устраняет выявленные угрозы.

**Примечание:** Сканер вредоносного ПО поставляется в версии сборки 4.8.30+ под Windows и 6.1.2+ под macOS .

Что важно знать про сканирование вашего устройства:

- Сканер запускается автоматически при разблокировке устройства.
- Он сканирует все выполняющиеся процессы и файлы на носителе (сжатые и несжатые).
- Он формирует отчет и очищает найденное вредоносное ПО.
- Сканер автоматически обновляется перед каждым сканированием, чтобы противостоять самым последним программным угрозам.
- Для обновления требуется Интернет-соединение.
- Оставьте135 Мб свободного места на носителе для загруженных файлов сигнатур вредоносного программного обеспечения.
- Загрузка файлов при первом обновлении может выполняться достаточно долго, особенно при плохом качестве Интернет-соединения.
- Дата последнего обновления показана на экране.
- Если сканер не обновлялся долгое время, вам будет нужно загрузить файл обновлений большого объема, чтобы вернуть его в актуальное состояние.

## Восстановление встроенных приложений

У вас есть возможность восстановить встроенные приложения, установленные Ironkey EMS если они были стерты или повреждены (только Windows).

1. Разблокируйте устройство и нажмите **Настройки** в меню панели управления DataLocker.
2. Выберите **Инструменты** в левой боковой панели. Под блоком "Состояние устройства" нажмите **Восстановить встроенные приложения.**

## Использование ZoneBuilder в SafeConsole

Если данная функция включена вашим системным администратором, вы можете использовать ZoneBuilder. Это инструмент SafeConsole, который позволяет создавать TrustedZone ("Доверительную зону") компьютеров. Такую зону можно использовать для ограничения доступа к устройству с компьютеров не входящих в эту зону, либо, если функция включена, автоматически разблокировать устройство на этих компьютерах.

Если системный администратор включил данную политику, вам может потребоваться сделать ваш аккаунт доверительным. Для этого:

1. Разблокируйте устройство и нажмите **Настройки** в панели управления DataLocker.
2. Выберите **Zone Builder** в левой боковой панели.
3. Нажмите **Сделать данный аккаунт доверительным**. Ваш аккаунт теперь отображается в блоке "Доверительные аккаунты".

Ваш аккаунт теперь входит в Доверительную зону компьютеров. В зависимости от политики, установленной вашим системным администратором, вы можете ограничить доступ к устройству для компьютеров, не входящих в Доверительную зону либо в оффлайн-режиме. Ваше устройство также может автоматически разблокироваться на компьютерах, входящих в Доверительную зону.

Чтобы удалить доверительный аккаунт просто выделите нужный аккаунт в списке и нажмите **Удалить**.

# Использование устройства на платформе Linux

Вы можете использовать данное устройство на комппьютерах с ОС Linux нескольких сборок. В папке linux находится два исполнительных файла: Unlocker_32.exe и Unlocker_64.exe. Замените исполнительный файл Unlocker_xx.exe исполнительным файлом, соответствующим версии вашей операционной системы.

Для использования в среде Linux, устройство должно быть предварительно установлено на компьютере с ОС Windows или macOS. Для получения более подробной информации см. Настройка устройства. Некоторые политики устройств корпоративной сборки, устанавливаемые системным адмнистратором, могут ограничивать доступ к устройству для компьютеров, управляемых операционной системой, отличной от Windows и macOS.

## Использование разблокировщика

Используйте исполнительный файл Unlocker_xx.exe для доступа к файлам в среде Linux. В зависимости от установленной на вашем ПК версии Linux, вам могут потребоваться корневые привилегии для запуска файла Unlocker_xx.exe в папке Linux публичного носителя. По умолчанию, большинство версий ОС Linux добавляют расширение .exe к исполнительным файлам в разделах fat32. В противном случае вам придется добавить нужное расширение вручную, выполнив следующие команды:

- chmod +x Unlocker_32.exe
- chmod +x Unlocker_64.exe

Если к системе подключено только одно устройство, запустите программу из командной оболочки без аргументов (например, Unlocker_xx.exe). Система запросит у вас ввести пароль, чтобы разблокировать устройство. Если подключено несколько устройств, вам потребуется указать, какое именно устройство вы хотите разблокировать.
**Примечание:** Unlocker_xx.exe разблокирует только PRIVATE_USB; в таком случае он должен быть установлен. Большинство современных сборок Linux distributions выполняют установку автоматически. Если ваша сборка этого не предусматривает, запустите программу установки из командной строки, используя название устройства, указанное рядом с файлом Unlocker_xx.exe.

Однако, деинсталлирующие приложения не выполняют блокировку PRIVATE_USB. Чтобы заблокировать устройство, вы должны физически отключить его от компьютера или запустить файл:

- Unlocker_xx.exe -l

Используя устройство в среде Linux учитывайте следующее:

1. Версия ядра должна быть 2.6 или выше
2. Установка
    - Убедитесь, что у вас есть разрешение устанавливать внешние SCSI и USB устройства
    - Некоторые сборки не выполняют автоустановку, в таком случае, следует выполнить команду: mount /dev/(name of the device) /media/(mounted device name)
    - Название установленного устройства зависит от версии сборки.

3. Разрешения
    - У вас должно быть разрешение устанавливать внешние /usb/устройства.
    - У вас также должны быть разрешения запускать исполняемые файлы с публичных носителей чтобы запустить Unlocker.
    - У вас должны быть корневые разрешения пользователя.
4. Разблокировщик для Linux поддерживает версии ОС x86 и x86_64.
5. Политики, блокирующие устройство
    - Если устройство отключено настройками политики в SafeConsole или Ironkey EMS у вас не будет возможности его разблокировать.

## Ссылки на источники справочной информации

Указанные ниже ресурсы позволят вам получить более подробную информацию о продукции DataLocker. Если у вас остались вопросы, свяжитесь с вашей службой или системным администратором.

- support.datalocker.com: Информация, статьи и видео уроки
- support@datalocker.com: Обратная связь и запросы пользователей
- datalocker.com: Общая информация
- datalocker.com/warranty: Информация по гарантии

**Примечение:** DataLocker не несет ответственности за технические или редакторские ошибки и / или упущения, содержащиеся в данном документе, а также за случайные или косвенные убытки, возникшие в результате предоставления или использования данного материала. Информация, представленная в настоящем документе, может быть изменена без предварительного уведомления. Информация, содержащаяся в данном документе, отражает текущую точку зрения DataLocker по освещаемому вопросу на дату его публикации. DataLocker не может гарантировать точность любой информации, представленной после даты публикации. Данный документ предназначен исключительно для информационных целей. В этом документе DataLocker не дает никаких явных или подразумеваемых гарантий . DataLocker и DataLockerlogo являются товарными знаками DataLocker Inc. и ее дочерних компаний. Все остальные торговые марки являются собственностью их законных владельцев.

Ironkey - это зарегистрированная торговая марка Kingston Technologies, используется с разрешения Kingston Technologies.

**Информации по FCC**

Данное устройство соответствует разделу 15 правил FCC. Его эксплуатация соответствует следующим двум условиям: (1) Это устройство не должно создавать вредных помех, и (2) данное устройство должно принимать любые получаемые помехи, включая помехи, которые могут вызывать сбои в работе. Данное оборудование было проверено и признано соответствующим ограничениям для цифровых устройств класса B в соответствии с разделом 15 правил FCC. Эти ограничения предназначены для обеспечения разумной защиты от вредных помех в жилых помещениях. Это оборудование генерирует, использует и может излучать радиочастотную энергию и, если оно установлено и используется не в соответствии с инструкциями, может создавать вредные помехи для радиосвязи. Тем не менее, не существует никакой гарантии, что такие помехи не возникнут в каждом конкретном случае. Если это оборудование создает вредные помехи для приема радио или телевидения (это можно определить, выключив и включив устройство), пользователю рекомендуется попытаться устранить помехи посредством одной или нескольких приведенных ниже мер:

- Измените ориентацию или местоположение приемной антенны.
- Увеличьте расстояние между устройством и приемником.
- Подключите устройство к розетке в цепи, отличной от той, к которой подключен приемник.
- Обратиться за помощью к дилеру или опытному специалисту по теле- и радиотехнике..

**Примечание:**Изменения или модификации, не одобренные явно стороной, ответственной за соответствие, могут лишить пользователя права на эксплуатацию оборудования.