криптоком

Устройство генерации случайных чисел и хранения ключей «Вьюга»

ИНСТРУКЦИИ И ПРАВИЛА ЭКСПЛУАТАЦИИ

2020

Содержание

1 ИНФОРМАЦИЯ ОБ ИЗГОТОВИТЕЛЕ

Изготовителем устройства является **ООО «КРИПТОКОМ»**, г. Москва, ул.Кедрова, д.14, корп.2, тел. (499) 124-62-26. *http://www.cryptocom.ru, support@cryptocom.ru*

2 ИНСТРУКЦИЯ ПО ЭКСПЛУАТАЦИИ

СЕИУ.467159.002 ИЭ

2.1 Общее описание устройства

Устройство генерации случайных чисел и хранения ключей «Вьюга» представляет собой малогабаритное электронное устройство, предназначенное для использования в составе специализированных компьютерных систем, и функционирует под управлением специального прикладного программного обеспечения.

Устройство включает в себя генератор случайных чисел (ГСЧ) и область памяти 128 байт, которую можно использовать для хранения закрытых ключей.

Устройство снабжено разъёмом для подключения к шине USB компьютера. На противоположной стороне размещен светодиодный индикатор. Других органов управления и регулировки нет.

Свечение индикатора означает исправную работу источника случайной последовательности.

Допускается мерцание индикатора в моменты выполнения процедур обращения к устройству.

При возникновении неисправности в аналоговой части устройства индикатор гаснет.

2.2 Неисправности устройства

Ситуации, связанные с неисправностями устройства «Вьюга», фиксируются процедурами прикладного ПО и сопровождаются выдачей соответствующих сообщений. Неисправное устройство подлежит замене.

Прежде чем предъявлять претензии к исправности устройства, необходимо убедиться в исправности USB-порта.

Для избежания неисправностей следует при эксплуатации и хранении устройства избегать механических повреждений, длительного воздействия повышенной температуры и влажности, а также приближения к источникам сильных электромагнитных полей.

3 РУКОВОДСТВО СИСТЕМНОГО АДМИНИСТРАТОРА ПО УСТАНОВКЕ ДРАЙВЕРОВ

СЕИУ.467159.002 УД

Устройство «Вьюга» подключается к компьютеру через интерфейс USB. Работа с устройством производится через виртуальный COM-порт. В операционной системе необходимо установить драйверы для ГСЧ и виртуального COM-порта.

3.1 Драйверы для ОС Windows

3.1.1 Характеристика драйверов

Необходимые для работы устройства драйверы на ОС Windows 8.1 и Windows 10 можно установить автоматически из базы драйверов Windows. На Windows 8 и Windows 7 автоматическая установка может работать или не работать в зависимости от списка установленных обновлений. В этом случае, а также при отсудствии подключения к Интернету можно воспользоваться комплектом драйверов от фирмы-производителя микросхемы FT232BM, которые записаны на входящем в комплект поставки компакт-диске в каталоге windows.

После установки драйверов в операционной системе формируется дополнительный COM-порт, через который прикладная программа может общаться с устройством. Номер этого COM-порта можно узнать в разделе настроек системы.

3.1.2 Установка драйверов

Установка драйверов устройства «Вьюга» происходит при первом подключении устройства к компьютеру.

Внимание. Первое подключение устройства в ОС Windows обязательно должно производиться пользователем **с правами администратора**.

В случае использования на одном компьютере нескольких экземпляров устройства разными пользователями в ОС Windows после подключения экземпляра устройства «Вьюга», ранее не подключавшегося к данному компьютеру, может потребоваться перезагрузка системы.

Для установки драйвера:

1. Подключите устройство «Вьюга» к компьютеру, система обнаружит подключение нового устройства, после чего будет предложено установить его драйвер;
2. Если компьютер подключён к Интернету, нажмите кнопку «Автоматический поиск обновлённых драйверов», после поиска и скачивания драйверы будут установлены, а в списке устройств появится USB Serial Port;
3. Если автоматическая установка по какой-либо причине не удалась (завершилась с ошибкой) или нет соединения с Интернетом, выполните ручную установку, для этого нажмите кнопку «Указать путь к драйверам» и укажите папку windows на диске с драйверами.

3.2 Драйверы для ОС Linux

3.2.1 Характеристика драйверов

Драйверы для ОС Linux входят в состав операционной системы, это модуль ядра ftdi_sio. Стандартное ядро ОС, устанавливаемое из дистрибутива, содержит этот модуль, при использовании самостоятельно собранного ядра убедитесь, что указанный модуль в него включен.

3.2.2 Вспомогательные скрипты

Для работы прикладного программного обеспечения производства ООО «Криптоком» с устройством «Вьюга» под ОС Linux необходимы скрипты, обеспечивающие взаимодействие между ПО и драйвером. Эти скрипты создают символическую ссылку на соответствующий специальный файл, включающую в себя имя, содержащее серийный номер устройства.

Указанные скрипты поставляются на компакт-диске, входящем в комплект поставки устройства «Вьюга».

3.2.3 Установка скриптов под Linux

Для установки скриптов необходимо:

1. Смонтировать дистрибутивный диск;
2. Перейти на диске в каталог linux;
3. Запустить с правами суперпользователя скрипт install.sh, находящийся в этом каталоге. Этот скрипт автоматически определит используемый пакетный менеджер и установит соответствующий пакет.

4 ПРАВИЛА ЭКСПЛУАТАЦИИ

СЕИУ.467159.002 ПЭ

1. Все устройства «Вьюга» подлежат строгому поэкземплярному учету.
2. Режим создания ключей с записью их на устройство «Вьюга», а также режим хранения устройства «Вьюга» должен исключать доступ к устройству кого-либо, кроме владельца ключей.
3. Для хранения устройств «Вьюга», содержащих закрытые ключи, должны использоваться металлические шкафы (хранилища, сейфы), исключающие несанкционированный доступ.
4. В случае отсутствия у пользователя индивидуального хранилища, соответствующего п. 3, устройства «Вьюга», содержащие закрытые ключи, по окончании рабочего дня должны сдаваться пользователем лицу, ответственному за их хранение.
5. Должно быть запрещено оставлять без контроля вычислительные средства, к которым подключено устройство «Вьюга», содержащее закрытые ключи.
6. Нарушение режима хранения и использования аппаратного компонента «Вьюга», повлекшее доступ к устройству, содержащему закрытые ключи, посторонних лиц, либо возникновение условий, при которых такой доступ был возможен (даже если сам факт доступа не выявлен), называется компрометацией ключей. В случае компрометации ключей необходимо немедленно

принять меры по минимизации последствий компрометации.

7. Смена ключей подписи и шифрования должна производиться не реже раза в год.

8. В случае повреждения или уничтожения устройства «Вьюга», содержащего закрытые ключи, возможность выполнять криптографические операции будет потеряна. Для возможности максимально быстрого и полного восстановления нормального режима работы в подобных ситуациях рекомендуется заблаговременно создавать резервные копии закрытых ключей на резервном устройстве «Вьюга». При этом режим создания и хранения резервных устройств должен исключать доступ к этим копиям кого-либо, кроме владельца ключей. Резервные копии закрытых ключей рекомендуется создавать сразу по завершении процедуры создания новых ключей.

9. Если ключи, содержавшиеся в устройстве «Вьюга», по какой-то причине больше не нужны, сразу же необходимо записать в это устройство другие ключи, или очистить хранилище ключей с помощью программы **WIPEVJUGA**, или уничтожить устройство.

10. При создании новых резервных копий закрытых ключей предыдущие (ставшие неактуальными) резервные копии должны быть уничтожены.

    Устаревшие резервные копии ключевых файлов должны уничтожаться с использованием программы **WIPEVJUGA**. Устройство «Вьюга», содержащее закрытые ключи пользователя, а также устройства «Вьюга», используемые для хранения резервных копий закрытых ключей, после удаления с них ключевых фай-

лов должны использоваться в том же качестве (для хранения новых ключей) либо уничтожаться.