Алгоритм работы диода данных для USB интерфейса

Бройко Антон Петрович

к.т.н., с.н.с., СПбГЭТУ «ЛЭТИ», Россия, Санкт-Петербург

broyko@mail.ru (*)

Кондрашов Кирилл Константинович

м.н.с., СПбГЭТУ «ЛЭТИ», Россия, Санкт-Петербург

kondrashovkk@mail.ru

Data diode algorithm for the USB interface

Broyko Anton Petrovich

Ph.D., senior researcher, St. Petersburg ETU “LETI”,

Russia, St. Petersburg

broyko@mail.ru

Kondrashov Kirill Konstantinovich

Junior researcher, St. Petersburg ETU “LETI”,

Russia, St. Petersburg

kondrashovkk@mail.ru

Аннотация. Проанализированы отечественные решения, реализующие однонаправленную передачу данных. Представлен новый алгоритм работы диода данных для USB интерфейса, позволяющий обеспечить высокую степень защиты процесса приема/передачи цифровой информации.

ABSTRACT. We analyzed Russian solutions that implement unidirectional data transmission. A new algorithm of data diode operation for USB interface is presented, which allows to provide a high degree of protection of the process of receiving/transmitting digital information.

Ключевые слова: диод данных; USB интерфейс; защита информации; однонаправленная передача данных.

Keywords: data diode; USB interface; information security; unidirectional gateway.

Введение

Диод данных предназначен для решения проблемы защиты конфиденциальной информации при подключении внешних устройств к персональному компьютеру (ПК) или портативной технике по USB интерфейсу. Данная проблема очень актуальна, поскольку многие организации используют средства защиты от доступа к служебному оборудованию по USB интерфейсу и от утечки конфиденциальных данных с ПК всё по тому же USB интерфейсу. Для решения этой проблемы применяются программно-аппаратные комплексы однонаправленной передачи данных по USB интерфейсу, принцип работы которых основан на промежуточном анализе проходящего трафика и блокировании передач запрещённых данных в соответствии с настройками фильтра. Для этих программно-аппаратных комплексов характерна узкая направленность (например, только на работу с определёнными типами накопителей данных), а также значительные размеры, влекущие за собой неудобство переноски и сложности использования с портативными устройствами. В связи с этим важной научно-технической задачей является разработка аппаратного модификатора трафика USB интерфейса, обладающего широкими возможностями по блокировке передачи запрещённой информации, имеющего компактные размеры, получающего питание по шине USB и обеспечивающего удобство использования с портативными устройствами.

Современное состояние

В настоящее время известно три отечественных устройства однонаправленной передачи данных (диоды данных) по шине USB: ALTELL КОП-USB, СТРОМ-USB-2 и «Диод-2С». Кроме того, существуют устройства однонаправленной передачи данных через сетевые соединения, но принцип их действия несколько отличается из-за особенностей интерфейса [1]. В связи с

этим целесообразно рассмотреть только устройства, предназначенные для работы с USB интерфейсом.

ALTELL КОП-USB – первый российский комплекс однонаправленной передачи данных через USB интерфейс – имеет компактные размеры и может использоваться как в настольном, так и во встроенном исполнении (для этого используется отсек для 2,5-дюймовых жестких дисков). Аппаратная часть комплекса состоит из корпуса, несъемного USB-кабеля для подключения к защищаемому автоматизированному рабочему месту (АРМ), разъема USB для подключения внешнего USB-носителя, трех световых индикаторов режима работы и печатной платы внутри корпуса.

Этот комплекс позволяет гарантированно решить проблему возможной утечки конфиденциальной информации через USB-порты, одновременно обеспечивая свободное использование обычных USB-накопителей для ввода информации. В качестве АРМ может выступать как стационарный, так и переносной компьютер [2].

СТРОМ-USB-2 предназначен для подключения к АРМ, на котором обрабатывается информация, составляющая государственную тайну с грифом не выше «Совершенно секретно», съемных USB-носителей информации в режиме чтения, без возможности вывода на них данных. Этот комплекс позволяет использовать внешние носители данных с USB интерфейсом для ввода информации в охраняемую систему, не опасаясь возможности утечки конфиденциальных сведений.

В нем нашли развитие хорошо зарекомендовавшие себя технические решения в области систем безопасного ввода данных. Реализация однонаправленной передачи данных с USB-носителей обеспечивается на аппаратном уровне. Комплекс обеспечивает защиту устройства, к которому подключается USB-носитель, от возможности внешнего воздействия. Это реализуется идентификацией подключаемых съемных носителей. Внутри комплекса находятся два микроконтроллера фирмы «ST Microelectronics»: один подключается к внешнему USB-носителю, второй – к ПК. Допускается

подключение только устройств, идентифицированных по классу Mass Storage Device (флеш-накопитель). В случае подключения к изделию USB-устройства другого класса (модема, манипулятора, камеры, принтера, телефона, адаптера и прочих) инициализация подключенного устройства не производится. В комплексе СТРОМ-USB-2 реализован механизм, позволяющий модифицировать код и серийный номер подключаемого USB-носителя информации. Это дает возможность, используя программные средства и системы защиты информации (СЗИ) компьютера, определить факт подключения внешнего USB-устройства напрямую [3].

«Диод-2С» предназначен для однонаправленной передачи данных из информационных систем с низкой степенью конфиденциальности (секретности), в том числе из сети Интернет, в информационные системы с высокой степенью конфиденциальности (секретности). Защита информации обеспечивается технологией однонаправленной передачи данных, исключающей утечку информации по каналам сетевого информационного обмена.

Этот комплекс не создает каналов утечки речевой акустической информации. Безопасность информации обеспечивается на аппаратном уровне. Функционирование комплекса не зависит от используемых на АРМ операционных систем и программного обеспечения (ПО). «ДИОД-2С» позволяет подключать информационные сети, использующие линии связи типа «витая пара» или волоконно-оптические линии связи [4].

Предлагаемый метод

На основе анализа открытых источников информации был сделан вывод о принципиальной возможности создания диода данных, способного принимать USB-трафик и при необходимости производить его модификацию, не обнаруживая себя ни для ведущего (host), ни для ведомого (device) устройства. За основу была взята идея уже существующих устройств – перехватчиков USB-

трафика активного соединения. Данные устройства невидимы для передающей и принимающей сторон канала связи. Главной особенностью предлагаемого устройства является отсутствие аппаратной поддержки USB интерфейса, так как при наличие такой поддержки устройство будет обнаруживаться хостом на аппаратном уровне даже при отсутствии соответствующих управляющих программ (драйверов).

Предложенное устройство должно удовлетворять следующим требованиям:

- наличие дифференциальных входов/выходов общего назначения высокой частоты (желательно до 1 ГГц), конфигурируемых на частоту работы 480 МГц для версии протокола USB 2.0;
- высокая частота работы логической системы устройства (не менее 100 МГц);
- наличие элементов синхронизации высоких частот;
- возможность организации быстродействующего буфера переменного объема (не менее 1 кБ).

Было установлено, что наиболее полно предъявляемым требованиям соответствуют программируемые логические интегральные схемы (ПЛИС), преимущественно фирмы Xilinx, в силу их высокой степени универсальности и гибкости конфигурирования.

Аппаратный модификатор USB-соединения основан на использовании ПЛИС, в которой предполагается реализовать промежуточный буфер для перехвата и обработки пакетов, следующих от хоста к устройству. Изначально максимальный объем буфера обусловлен требованиями спецификации USB 2.0, согласно которой допустимый объём пакета для изохронных передач не превышает 1024 байт (1 кБ). Для остальных типов передач установлены свои ограничения ещё меньшего размера, поэтому объём буфера был выбран именно равным 1 кБ. Следует принять во внимание, что заполнение такого буфера целиком требует существенного времени, что (с учётом последующей пересылки пакета далее к устройству) формирует определённую временную

задержку. Для обеспечения нормального функционирования соединения по протоколу USB 2.0 при разработке аппаратного модификатора необходимо соблюсти требования к допустимым задержкам.

Из официальной документации на стандарт USB 2.0 [5] известно, что для обнаружения отсутствия ответа партнера на пакет каждое устройство имеет счетчик тайм-аута, который прерывает ожидание ответа по истечении некоторого времени. В спецификации имеется ограничение на время оборота по шине (roundtrip time), т. е. время от конца маркера EOP (End-of-Packet) отправленного пакета до получения начала ответного пакета. Для конечного устройства (и хост-контроллера) нормируется максимальная задержка ответа (response time) от конца увиденного EOP до введения им начала пакета. Кроме того, для хабов нормируется задержка трансляции пакетов, для кабелей – задержка распространения сигналов. Счетчик тайм-аута конечных устройств должен учитывать максимальную задержку, возможную для допустимой конфигурации шины: до 5 промежуточных хабов, до 5 метров для каждого соединительного кабеля. Допустимое значение тайм-аута выражается в битовых интервалах (bt). Для режима High Speed (скорость передачи данных 25…480 Мб/с) битовый интервал составит:

$$bt = 1/480000000 = 2{,}083 \times 10^{-9} \text{ с } (\sim 2{,}1 \text{ нс})$$

На столь высокой скорости задержка в кабельном сегменте много больше битового интервала, поэтому в модели расчёта тайм-аутов для USB 2.0 на каждый кабельный сегмент отводится по 26 нс, а на хаб – по 4 нс плюс 36 bt. Таким образом, двукратное прохождение 6 кабельных сегментов (2×6×26 = 312 нс ≈ 150 bt) и пяти хабов (2×5×4 = 40 нс ≈ 19 bt плюс 2×5×36 = 360 bt) занимает до 529 bt. Максимальная задержка ответа устройства составляет 192 bt, а значит полная задержка (с учетом кабелей и хабов) равна 721 bt. Исходя из этого, спецификация предписывает передатчикам в режиме High Speed использовать счетчик тайм-аута на 736…816 bt.

У хост-контроллера с каждой конечной точкой всех устройств связан свой счетчик ошибок, обнуляемый при планировании каждой транзакции. Этот

счетчик считает все протокольные ошибки (включая и ошибки по тайм-ауту), и, если количество ошибок превышает порог (обычно 3 ошибки), то канал с данной конечной точкой останавливается, о чем уведомляется его владелец (драйвер устройства или USB-device). До превышения порога хост отрабатывает ошибки для неизохронных передач попытками повтора транзакций, без уведомления клиентского ПО.

У предлагаемого аппаратного модификатора основной вклад в задержку вносится на стадии передачи пакета из буфера к подключаемому устройству, например к LTE-модему. Если предположить, что каждый пакет сначала полностью загружается в буфер, затем обрабатывается и лишь потом начинается его передача, то очевидно, что для пакетов объемом десятки байт задержка становится уже критичной. Полная загрузка буфера перед выгрузкой в таком случае оказывается абсолютно невозможной: 1024 × 8 = 8192 bt. Исходя из этого, можно сформулировать следующие требования к диоду данных для USB интерфейса:

- длина USB-кабеля между хостом и модификатором должна составлять не более 10 см, при этом допустимая задержка кабеля составит 0,1 × 150/(5 × 6) = 0,5 bt;
- подключение принимающего устройства (LTE-модема) напрямую к плате модификатора должно осуществляться через стандартный USB-порт, размеры платы должны быть выбраны с учётом этого требования;
- объем буфера для полной загрузки передаваемого пакета должен быть составляет (736 – 192 – 32)/8 = 64 байта, при этом предполагается, что время на обработку и внутренние задержки ПЛИС не превысит 32 bt.

При передаче пакета данных через промежуточный буфер ПЛИС необходимо соблюсти временные задержки, оценочное значение которых составляет 544 битовых интервала высокоскоростного USB-соединения (bt). Поскольку допустимый объем пакета налагает ограничение на минимальный объем входного буфера (1 кБ), то для анализа и модификации передаваемых

данных предлагается использовать следующий алгоритм работы диода данных для USB интерфейса (рис. 1):

1. Загрузка передаваемого хостом пакета данных во входной буфер размером 1 кБ.

2. Запуск счётчика принятых байтов сразу после начала загрузки пакета.

3. Если объем пакета меньше или равен 64 байтам (512 bt), то выполняется его сверка с шаблоном: сначала по типу передачи, затем, при необходимости, по другим параметрам.

4. В случае управляющей передачи с запрещённым параметром, этот параметр заменяется на другой и производится пересчет контрольной суммы пакета.

5. Передача модифицированного пакета в выходной буфер объемом 1 кБ и его немедленная выгрузка до опустошения буфера.

6. Если объем пакета больше 64 байт, то его первый условный блок объемом 64 байта передаётся в служебный регистр, где выполняются проверка и модификация этого блока.

7. Передача модифицированного блока в выходной буфер и его немедленная выгрузка до опустошения буфера.

8. Если объем пакета больше 128 байт, то его второй условный блок объемом 64 байта, вероятнее всего, не содержит ни контролируемых параметров, ни контрольной суммы, но для него все равно выполняется процедура, аналогичная первому блоку.

9. Передача второго блока в выходной буфер до его опустошения, при этом выгрузка данных продолжается для обеспечения непрерывности соединения.

10. Выполнение аналогичных действий с третьим и последующими условными блоками пакета до момента обнаружения конца поступающих от хоста данных.

11. Пересчет контрольной суммы для всего сохраненного в буфере пакета сразу после окончания входящей передачи.

12. Модификация значений контрольной суммы (2 байта) в последнем условном блоке пакета, передача его в выходной буфер, откуда все данные полностью выгружаются на принимающее устройство.

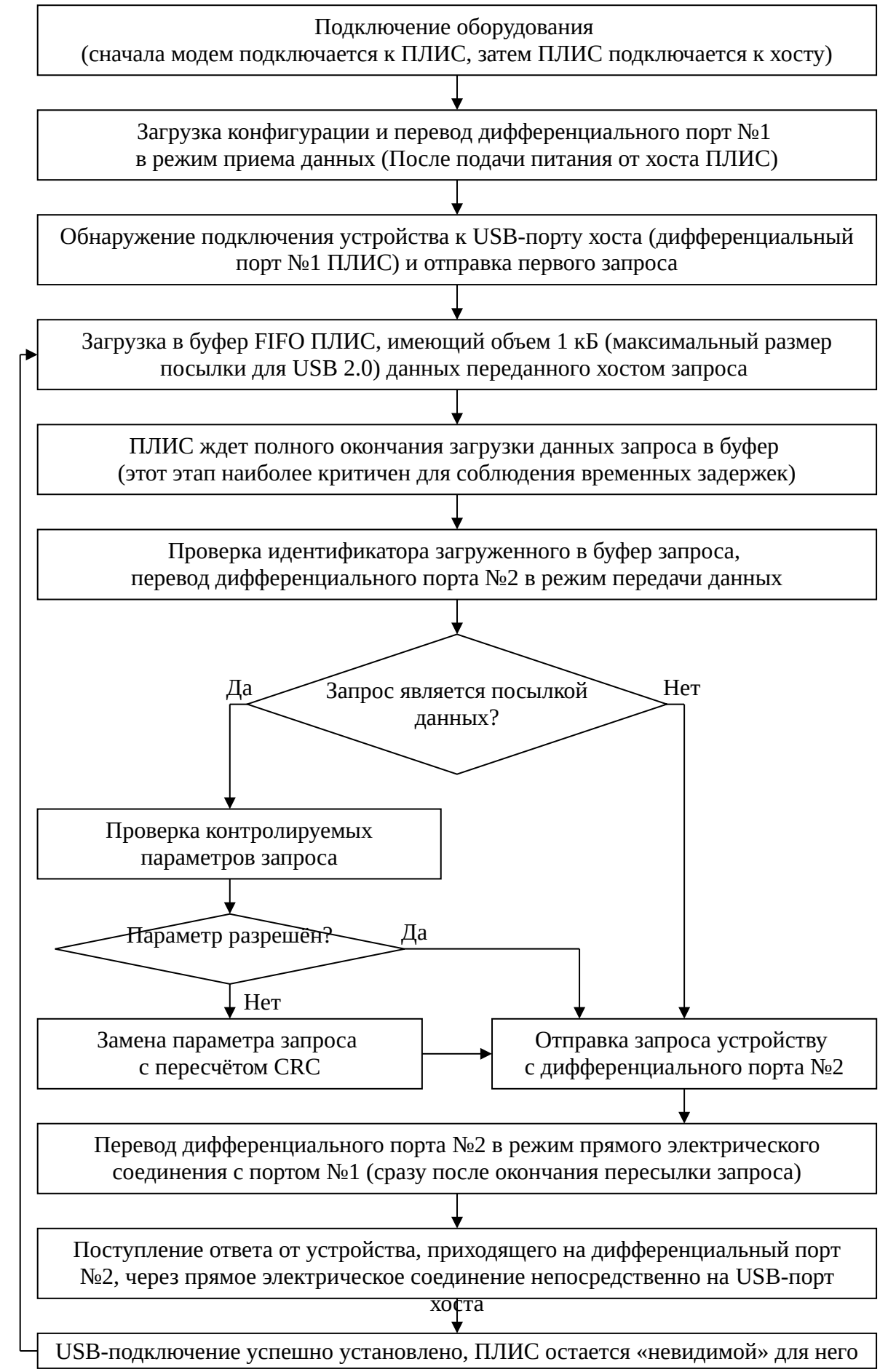

Рис. 1 Алгоритм работы диода данных для USB интерфейса.

Предполагается, что время обработки блока данных объемом не более 64 байт на ПЛИС составит не более 32 bt (~ 66 нс). Результирующая тактовая диаграмма передачи большого пакета через диод данных для USB интерфейса представлена на рис. 2.

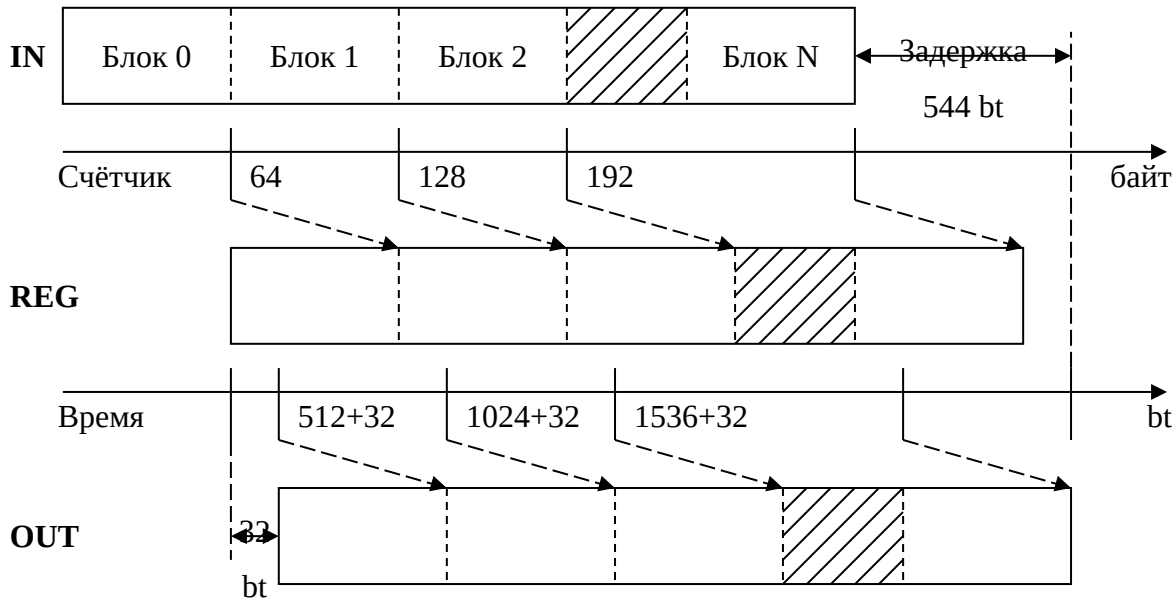

Рис. 2 Тактовая диаграмма передачи пакета через диод данных для USB интерфейса.

Заключение

Предлагаемый алгоритм работы диода данных для USB интерфейса на основе использования ПЛИС позволяет обеспечить полный контроль передачи информации от хоста (ПК или мобильного телефона) к принимающему устройству (флэш-накопителю, LTE-модему или любому другое USB-устройству). Контроль данных по заданным параметрам происходит непосредственно на шине USB, факт подмены не может быть обнаружен ни хостом, ни внешним модемом. Благодаря этому достигается очень высокая степень защиты устройств с особыми требованиями к безопасности, которые работают в условиях подключения к внешним информационным сетям.

Благодарность

Работа выполнена в рамках государственного задания Министерства науки и высшего образования Российской Федерации №075-01024-21-02 от 29.09.2021 (проект FSEE-2021-0015)

Список литературы

1. Бирюков А. Современные средства однонаправленной передачи данных // Каталог «Системы безопасности»-2018. С. 78–80.

2. Комплекс однонаправленной передачи данных ALTELL КОП-USB. Режим доступа: https://www.altell.ru/products/kop-usb.

3. Комплекс однонаправленной передачи данных СТРОМ-USB-2. Режим доступа: https://www.cansec.ru/products/strom-usb-2.

4. Техническое средство однонаправленной передачи данных «Диод-2С». Режим доступа: http://www.cbi-info.ru/groups/page-1180.htm.

5. Universal Serial Bus Specification. Режим доступа: https://www.usb.org/document-library/usb-20-specification.