УДК 004. 056.5 + 004.35.031.4 + 004.5.056

Кобяков В. Ю., Лучинин А. С.

ОБНАРУЖЕНИЕ ПЭМИ ПРОВОДНИКОВ И КОННЕКТОРОВ ПРИ ПЕРЕДАЧЕ ПО ИНТЕРФЕЙСУ USB

В настоящее время огромное количество устройств обмениваются друг с другом по интерфейсу USB. Возможные утечки информации в литературе освещены недостаточно, чем и обоснован выбор темы для исследования. В статье кратко изложена структура интерфейса USB. Для проведения измерений выбрана проводная клавиатура Rapoo N2400 с низкоскоростным соединением USB. Экспериментальные исследования показали возможность перехвата информации за счет побочных электромагнитных излучений.

Ключевые слова: *информационная безопасность, побочные электромагнитные излучения, перехват информации, USB, клавиатура, защита информации.*

Kobyakov V. Y, Luchinin A. S.

DETECTION OF TEMPEST CONDUCTORS AND CONNECTORS IN THE PROCESS OF TRANSMISSION THROUGH USB INTERFACE

Currently a great number of devices are intercommunicating with each other through the USB interface. Data leakages are not properly highlighted which justifies the topic of the research. The article dwells on concise structure of the USB interface with the Rapoo N2400 keyboard with slow connection chosen for execution of measurements. The experiments have shown the possibility of information capturing by means of side electromagnetic radiation.

Keywords: *information security, side electromagnetic radiation, information capturing, USB, keyboard, information security.*

Выделение информативного сигнала из передаваемых данных было невозможно без изучения протокола USB, описанного в соответствующей спецификации [1]. Первоначально (в версиях 1.0 и 1.1) шина обеспечивала две скорости передачи информации: полная скорость FS (FullSpeed) — 12 Мбит/с и низкая скорость LS (LowSpeed) — 1,5 Мбит/с. В версии 2.0 и 3.0 определены ещё высокая скорость HS (HighSpeed) – 480 Мбит/с и супервысокая скорость SS (SuperSpeed) – 5 Гбит/с.

Все обмены информацией, далее транзакции, инициируются хостом. Транзакция состоит из двух-трех пакетов. При обмене данными используются пакеты четырех типов:

1) Маркерные пакеты – пакеты управления, передаются только хостом (рис. 1);
2) Пакеты данных – применяются для передачи полезной нагрузки, используются хостом и устройством (рис. 2);
3) Пакеты квитирования – подтверждение принятого пакета данных, используются хостом и устройством (рис. 3);
4) Пакеты начала кадра (SOF) – выдаются хостом с номинальной скоростью один каждую 1,00 мс±0.05 в полноскоростном соединении. Используется при передаче сообщений, размер которых больше максимальной полезной нагрузки пакета данных (рис. 4).

Практическое наблюдение сигнала производилось с помощью осциллографа, подключенного к дифференциальным парам. Экспериментально установлено, что информация передается младшим битом вперед в кодировке NRZI с добавлением нуля при шести подряд передаваемых единицах. Хост опрашивает устройство через каждые 8 мс пакетом со следующими данными:

[1 0 1 0 1 0 1 1] SYNC
[1 0 1 1]PID IN 10012
[0 0 0 1]Check PID 01102
[1 0 1 0 1 0 1] ADDR 00000012
[1 0 1 0] ENDP 00012
[0 0 1 1 0] CRC
[0 0] EOP

Поля SYNC и EOP не несут смысловой нагрузки, они необходимы для синхронизации и инициализации обмена данными. При передаче EOP (End of packet) обе дифференциальные пары на два такта переходят в нулевое состояние, это означает конец передачи пакета. Поле PID определяет тип пакета, поле Check – инверсионное представление поля PID, необходимо для контроля ошибок.ADDR – поле адреса функции (устройства), назначается хостом. На нулевой адрес должны откликаться все устройства. Поле ENDP – номер конечной точки функции, обеспечивает более гибкую адресацию. CRC – контрольная

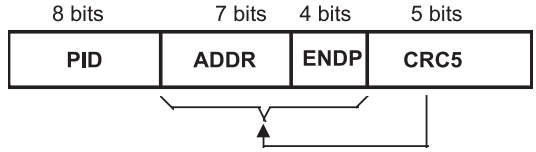

Рис. 1. Формат маркерного пакета

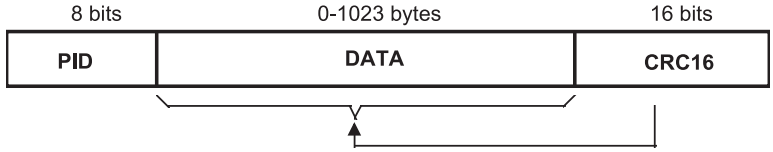

Рис. 2. Формат пакета данных

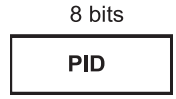

Рис. 3. Формат пакета квитирования

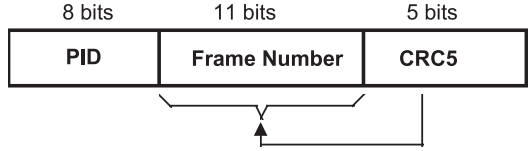

Рис. 4. Формат пакета начала кадра

сумма над полями ADDR и ENDP. В дальнейшем полями SYNC и EOP пренебрежём при описании пакетов, так как информации они не несут и присутствуют в пакетах любого типа.

Устройство отвечает через 8 битовых тактов ≈ 5,3 мс. Если у устройства нет ничего к передаче, то оно отправляет пакет квитирования об отсутствии нагрузки.

[0 0 1 1] PID NAK 10102 – устройство не может принимать данные или посылать данные.

[1 0 0 1] Check PID

Только в пакетах квитирования нет контрольной суммы. Контроль ошибок осуществляется полем Check.

Если у устройства есть что-то к передаче, то передается пакет данных. Передача информации о нажатии клавиши «a».

[1 0 1 0 1 0 1 1] SYNC.

[1 1 0 0] PID data1 – нечетный пакет данных

[1 0 0 0] Check PID

[0 1 0 1 0 1 0 1] DATA 0x00

[0 1 0 1 0 1 0 1] DATA 0x00

[0 1 1 0 1 0 1 0] DATA 0x04 код кнопки «a»

[1 0 1 0 1 0 1 0] DATA 0x00

[1 0 1 0 1 0 1 0] DATA 0x00

[1 0 1 0 1 0 1 0] DATA 0x00

[1 0 1 0 1 0 1 0] DATA 0x00

[1 0 1 0 1 0 1 0] DATA 0x00

[1 1 1 1 1 1 0 0] CRC 0xCE

[1 0 1 0 0 0 0 1] CRC 0x78

Под поле данных в низкоскоростном соединении выделяется максимум 8 байт. Размер поля может быть меньше, но исследуемая клавиатура сконфигурирована следующим образом: первые 2 байта нулевые, следующий байт HID-кода клавиши [2], остальные 5 байт нулевые. Контрольная сумма вычисляется над полем данных. Информация о нажатии клавиши передается один раз. Продолжительность нажатия, регистр, раскладку, комбинации клавиш – всё вычисляет драйвер клавиатуры и определяет, что делать.

В случае если данные приняты без ошибок, то хост отправляет пакет квитирования о подтверждении приема.

[0 0 1 0] PID ACK 0010_2 – приемник принимает пакет данных, свободный от ошибок.

[0 1 1 1] Check

При одновременном нажатии коды клавиш будут передаваться последовательно во время опроса устройства. При отпускании одной из зажатых клавиш будут переданы HID коды клавиш, которые ещё зажаты в по-

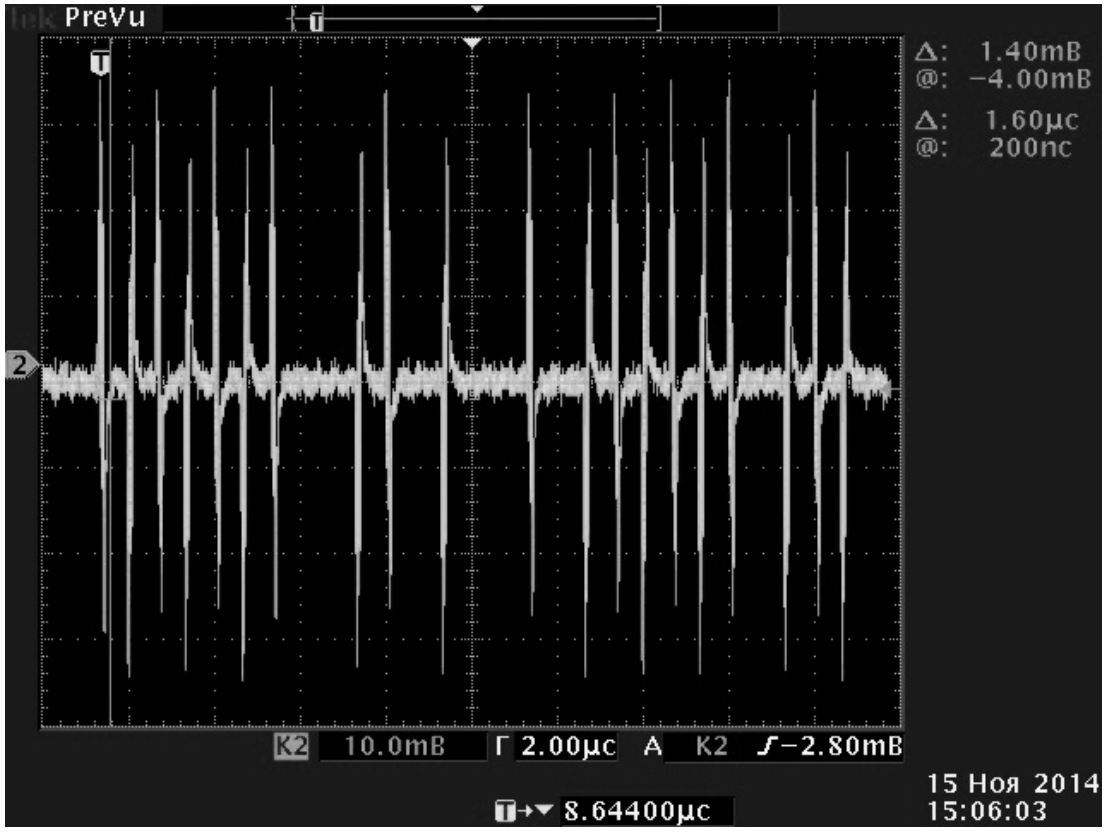

Рис. 5. Обнаруженный пакет данных, передаваемый по D+

рядке их нажатия. Максимальное число одновременно зажатых клавиш семь [3]. Нажатие восьмой клавиши будет проигнорировано. При отжатии последней клавиши передаются 8 нулевых байтов данных.

Для оценки возможности перехвата информации по каналу ПЭМИ, передаваемой по проводному низкоскоростному соединению, были проведены следующие эксперименты.

С помощью токосъемника ТИ2-3 и осциллографа Tektronix TDS 3054C делалась попытка пронаблюдать сигналы, циркулирующие по кабелю USB клавиатуры. Эксперимент не дал результата из-за недостаточной чувствительности осциллографа и хорошего качества кабеля (выполненного в виде витой пары).

Для повышения уровня сигнала была нарушена экранировка кабеля и токосъемник был подключен к одному из проводов сигнальной пары кабеля. В таком виде сигналы побочного излучения обнаруживаются успешно (рис. 5).

Уровень максимального импульсного скачка, образованного фронтом передаваемого импульсного сигнала, около 34 мВ. Уровень ниспадающего импульсного скачка 25–28 мВ. Данный разброс по амплитуде обусловлен разной длительностью переднего и заднего фронта информационных импульсов.

Есть две причины, по которым наблюдаемые импульсные скачки можно относить к побочным сигналам, излучаемым интерфейсом USB:

1. Длительность наблюдаемых возрастающих и ниспадающих импульсных скачков около 120–140 нс. Время нарастания/спадания импульсного сигнала в интерфейсе USB 110–140 нс.
2. Период повторения импульсных скачков около 650 нс – длительность импульса в интерфейсе 660 нс.

Для подавления побочного электромагнитного излучения в интерфейсе USB используется дифференциальная пара для передачи сигналов и экранирования кабеля. Подавление, обусловленное применением экранирования, было оценено экспериментально.

Экранированный кабель Belsis “Multimedia” Hi-Grade USB 2.0 High Speed Cable, со второго кабеля полностью сняты защитная оболочка и экранировка. Нагрузка 100 Ом, генератор N5181A (Agilent Technologies) излучал в линию синусоидальный сигнал амплитудой 1В. Прием вёлся с помощью анализатора спектра ESPI 3 (Rohde & Swartz). Зависимость мощности принятого сигнала от частоты изображена на рис. 6 и рис. 7.

Экранирование подавляет сигнал на 10–15 дБ. На частотах ниже 6 МГц уровень излучения меньше -115 дБм, для наблюдения излучения необходима более чувствительная аппаратура.

Экранированные кабели с применением витых пар позволили обнаружить излучение лишь на небольшом расстоянии. Амплитуды импульсных сигналов рис. 5, около 34 мВ лишь немного превышают порог чувствительности осциллографа. Дальность обнаружения можно увеличить, если применить более чувствительную аппаратуру.

Рассчитаем теоретически реализуемый порог чувствительности приемника, способного перехватить сигнал, излучаемый за счет побочного излучения кабеля и коннекторов USB интерфейса. Зададим параметры:

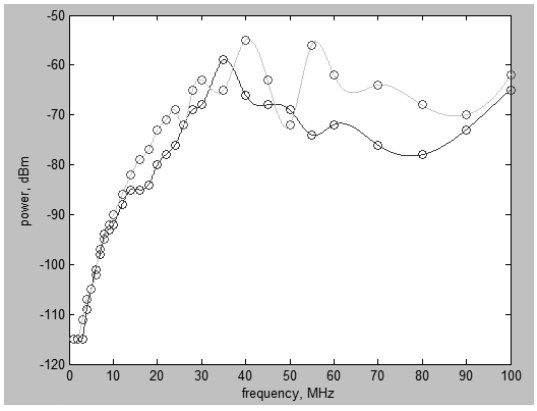

Рис. 6. Уровень ЭМИ при съеме информации токосъёмником ТИ2-3 в экранированном и неэкранированном кабеле

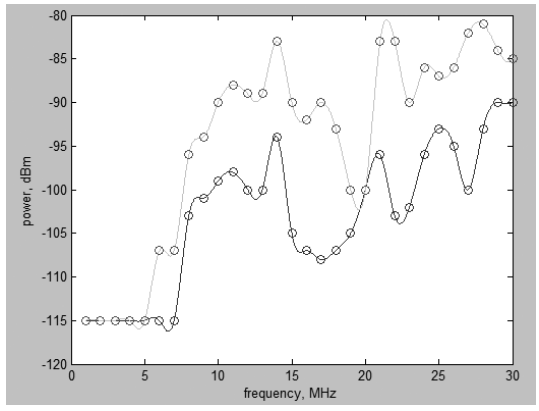

Рис. 7. Уровень ЭМИ в экранированном и неэкранированном кабеле USB на расстоянии 1 м, антенна АИР3-2

- R_a=50 Ом – выходное сопротивление антенны;
- F=10 дБ – коэффициент шума;
- K=10 дБ – требуемое отношение сигнал/шум на входе приемника;
- T=300 К – температура окружающей среды;
- $\tau_и$=120 нс – минимальная длительность ожидаемого импульсного скачка.

Минимальная мощность, необходимая для приема сигнала шумящим приемником (порог чувствительности):

$$P_{min} = F * K * k * T * \Delta f, \quad (1)$$

где $k = 1.38 * 10^{-23}$ Дж/К – постоянная Больцмана,

$$\Delta f = \frac{1}{\tau_и} = \frac{1}{120*10^{-9}} \approx 8.5 * 10^6 \text{Гц} \quad (2)$$

При условии согласования на входе приемника мощность собственных шумов и Э.Д.С. связаны соотношением

$$P_{min} = \frac{e_ш^2}{4*R_a}, \quad (3)$$

где, $e_ш$ – Э.Д.С. шумов, приведенных ко входу приемника.

Минимальное входное напряжение связанно с ЭДС шума:

$$U_{вх} = \frac{\sqrt{e_ш^2}}{2}. \quad (4)$$

Подставив числовые значения, найдем $e_ш^2$:

$$e_ш^2 = 4 * R_a * F * K * k * T * \Delta f \approx \approx 7.04 * 10^{-10} \text{ В}^2 \quad (5)$$

Подставив полученный результат в формулу 4, получим:

$$U_{вх} = \frac{\sqrt{e_ш^2}}{2} = \frac{\sqrt{7.04 * 10^{-10}}}{2} \approx \approx \frac{26.54 * 10^{-6}}{2} \approx 13.3 \text{ мкВ}$$

Полученной чувствительности хватит для того, чтобы перехватить передаваемую информацию по интерфейсу USB. Заданные исходные параметры приемника являются реальными для современной аппаратуры.

Полученные результаты позволяют уточнить требования к качеству экранировки кабеля и других элементов клавиатуры для исключения возможности перехвата информации в реальных устройствах [4].

Примечания

1. Спецификация по USB1.1 на русском языке // Сайт «Паяльник». URL: http://cxem.net/doc/comp/usb11.rar (дата обращения: 08.12.14)

2. USB Hid Keyboard Scan Codes // STIK elektro. URL: http://www.mindrunway.ru/IgorPlHex/USBKeyScan.pdf (дата обращения: 08.12.14)

3. Исупов. Л. Радиоснифер клавиатуры. Свежий подход к перехвату набираемого на клавиатуре текста // Хакер. 2006. № 08. с. 20 – 23. URL: http://xakep.ru/wp-content/uploads/2014/08/xa_08_2006_low.pdf?2bdec0 (дата обращения: 08.12.14)

4. Martin Vuagnoux, Sylvain Pasini. Compromising Electromagnetic Emanations of Wired and Wireless Keyboards // EPFL, Lausanne, Switzerland. URL: http://www.usenix.org-events-sec09-tech-f ull_papers-vuagnoux.pdf (дата обращения: 08.12.14)

Кобяков Василий Юрьвич, студент УрФУ. E-mail: kobyakov93@mail.ru.

Лучинин Александр Сергеевич, к. т. н., доцент УрФУ.

Vasily Yurievich Kobyakov, student of Ural Federal University. E-mail: kobyakov93@mail.ru.

Aleksandr Sergeevich Luchinin, Cand. Sc. Engineering, Associate Professor of Ural Federal University.