УДК 537.871

А. А. Персичкин, Н. В. Персичкина, С. Г. Шпилевая

ОСОБЕННОСТИ ОБРАЗОВАНИЯ ПЭМИН В КЛАВИАТУРЕ КОМПЬЮТЕРА С ТОЧКИ ЗРЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Проанализированы возможности образования в компьютерных клавиатурах с интерфейсом ps/2 побочных электромагнитных излучений и наводок, способных приводить к информационным утечкам. Установлены зависимости физических параметров ПЭМИН от конструктивных особенностей используемого оборудования. Проанализированы возможные каналы несанкционированного съема информации посредством использования ПЭМИН. Сформированы рекомендации по безопасному использованию клавиатур ps/2 в информационных системах.

The paper analyzes the possibilities of the formation of spurious electromagnetic radiation and interference in computer keyboards with the ps/2 interface, which can lead to information leaks. The dependences of the physical parameters of the PEMIN on the design features of the equipment used are established. Possible channels of unauthorized information retrieval, through the use of TEMPEST, are analyzed. Recommendations for the safe use of ps/2 keyboards in information systems are formed.

Ключевые слова: клавиатура, интерфейс, ПЭМИН, информационная безопасность, канал утечки

Keywords: keyboard, interface, TEMPEST, Information Security, leak channel

Как известно, клавиатура является неотъемлемой частью персонального компьютера (ПК), обеспечивающей ввод текстовой информации и многие другие операции, к которым в частности относится парольная аутентификация, создание документов, содержащих сведения конфиденциального характера, и т. п. В результате с точки зрения потенциальных угроз по утечке информации данное устройство можно рассматривать как критическое звено ПК, о чем свидетельствует широкое распространение клавиатурных перехватчиков [1].

Доставка перехваченной информации в основном происходит двумя путями: передачей данных через телекоммуникационные каналы связи и через отчуждаемые носители информации (USB-накопители, компакт-диски и т. д.). Несанкционированное функционирование клавиатурных перехватчиков может быть успешно блокировано за счет соблюдения общих требований компьютерной безопасности и некоторых режимных мер. Однако указанные меры защиты не устраняют канал утечки, реализуемый через побочные электромагнитные излучения и наводки (далее — ПЭМИН) [1—3]. В работах [2; 3], в частности, приводятся результаты измерений ПЭМИН клавиатуры ps/2 в широкой полосе частот на расстоянии до нескольких метров. Полноценный

анализ причин возникновения ПЭМИН в упомянутых работах, однако, не выполнялся либо сделаны выводы о наличии высших гармоник в побочном сигнале [4; 5].

В данной статье представлен анализ причин и характерных особенностей образования возможного канала утечки по ПЭМИН для клавиатур с интерфейсом ps/2.

Из данных, приводимых в [2; 3], следует, что ширина спектра ПЭМИН может составлять до десятков МГц. Максимальной для ps/2 можно считать частоту импульсов синхронизации (≈13 кГц) [6]. Таким образом, прием сигнала на сотой и выше гармониках маловероятен, и для объяснения процесса необходимо искать другие физические источники образования ПЭМИН.

Схемотехнически интерфейс ps/2 построен по схеме с открытым коллектором, что является простым и эффективным решением, поскольку в этом случае один провод используется как для приема, так и для передачи информации. Соответственно, в линии связи ps/2 имеются только два информационных провода, обеспечивающих синхронизацию (clock) и передачу данных (data) (рис. 1). В случае прохождения сигналов от клавиатуры к компьютеру они транслируются по линии с волновым сопротивлением ≈120 Ом на приемник с входным сопротивлением в десятки кОм.

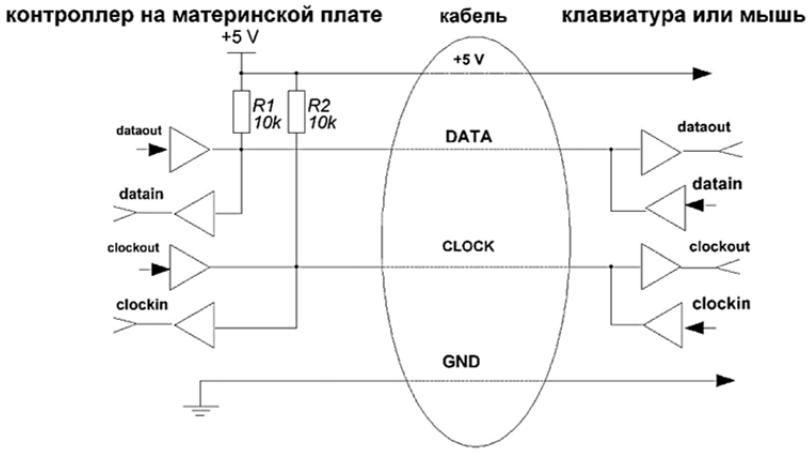

Рис. 1. Принципиальная схема интерфейса ps/2

Известно, что при передаче импульсного сигнала по линии связи с нагрузкой, превосходящей по величине эквивалентное волновое сопротивление, может наблюдаться переходной процесс в виде высокочастотного затухающего периодического колебания («звона»), в общем случае описываемого выражением

$$S(t) = b(t)e^{(2j\pi f+\alpha)t}, \qquad (1)$$

где f — частота колебаний; α — постоянная затухания.

О возможности появления указанного эффекта, характеризуемого выражением (1) при прохождении импульсного сигнала в линии связи, упоминается в работе [7], где рассмотрен интерфейс RS-232.

Для моделирования переходных процессов, которые могут возникнуть в линии клавиатуры ps/2 (рис. 2), воспользуемся программой схемотехнического моделирования Micro-Cap 8 [8]. В качестве исходных данных используем параметры реального кабеля клавиатуры с интерфейсом ps/2 и материнской платы: волновое сопротивление линии 120 Ом; физическая длина линии 1,3 м; сопротивление нагрузки 10 кОм.

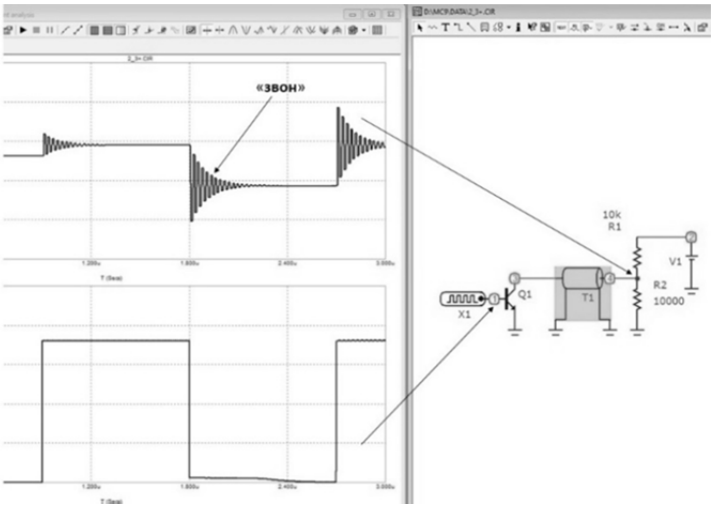

Рис. 2. Результаты компьютерного моделирования переходных процессов в кабеле клавиатуры ps/2

Как показывает модельное представление, частота переходного процесса («звона») в основном зависит от физической длины линии связи, а амплитуда — от сопротивлений потерь линии и внутреннего сопротивления источника, что согласуется с выполненным нами экспериментальными измерениями.

При непосредственных измерениях сигнала с клавиатуры «звон» был выражен значительно слабее либо не фиксировался вовсе. Это связано с наличием блокирующего конденсатора емкостью 300 пФ (рис. 3), расположенного на материнской плате и непосредственно подключенного к линии данных разъема ps/2, а также малыми значениями токов в линии.

Наличие блокирующего конденсатора не является обязательным, поскольку и не входит в спецификацию интерфейса ps/2. Данный элемент представляет собой дополнительную конструктивную опцию, введенную производителем оборудования с целью улучшения электромагнитной совместимости изделия [9].

Помимо сигнала ПЭМИН, вызванного несогласованностью волнового сопротивления линии и нагрузки при передаче информационного сигнала, в линиях связи клавиатур ps/2 постоянно присутствует сигнал в виде всплесков с амплитудой до 50 мВ и частотой следования в десятки кГц (рис. 4).

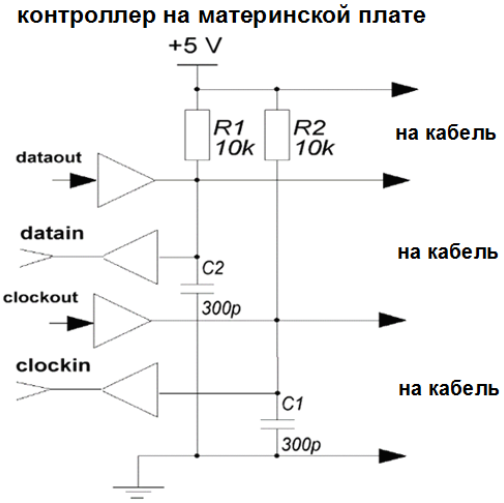

Рис. 3. Схема интерфейса ps/2 со стороны материнской платы

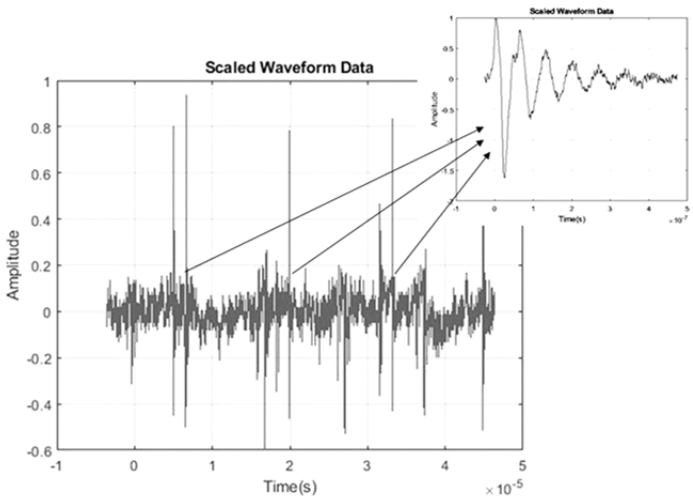

Рис. 4. Всплески сигнала, возникающие в кабеле ps/2

Указанные аномалии представляют собой переходный процесс, образованный за счет емкостной связи между информационным проводом, проводниками питания и экраном кабеля ps/2. Его источником являются неотфильтрованные помехи, просачивающиеся из импульсного блока питания компьютера с частотой преобразования инвертора (50—100 кГц). Результаты моделирования данного процесса представлены на рисунке 5. Сигнал в точке 1 имитирует неотфильтрованные импульсные «всплески» в шине питания, а конденсатор C1 служит аналогом емкостной связи между проводником питания (экраном) и информационным проводом кабеля ps/2.

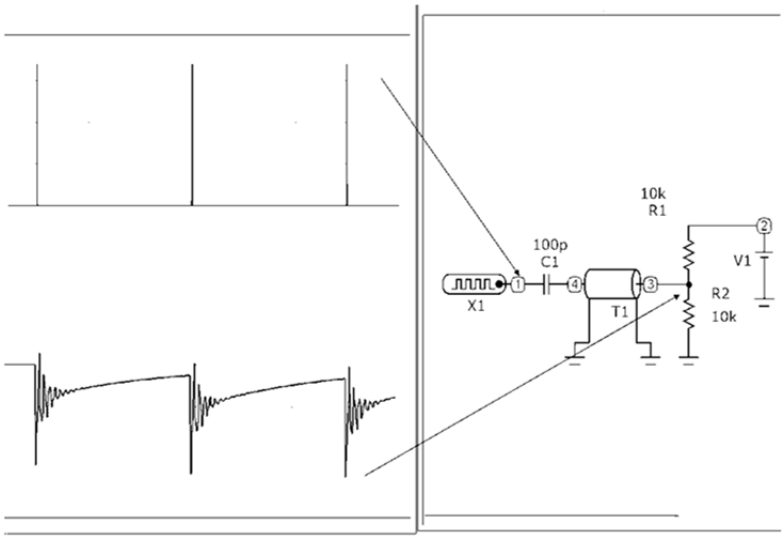

Рис. 5. Результаты моделирования процесса образования наведенных ПЭМИН в линии связи интерфейса ps/2

Как и в предыдущем случае, частота переходных процессов определяется физической длиной линии связи и составляет десятки МГц. Несмотря на то что наведенный сигнал ПЭМИН имеет характер периодических всплесков, он может служить несущей составляющей канала утечки, поскольку формируется кодовой последовательностью с клавиатуры.

Таким образом, можно сделать вывод о потенциальной уязвимости интерфейса ps/2 с точки зрения образования ПЭМИН. Причем в его спецификации не предусмотрены меры по их блокировке. Образование побочного излучения зависит в основном от того, использован ли производителем оборудования блокирующий конденсатор, и от технологии, по которой создан контроллер клавиатуры (ТТЛ или КМОП).

Как правило, в моделях информационных угроз канал утечки по ПЭМИН не считается актуальным, поскольку стоимость оборудования для организации перехвата (широкополосные приемники с преобразованием Фурье) очень велика, что делает его недоступным для потенциального нарушителя. Однако вероятность утечки информации через указанный технический канал является вполне реальной. За последние 10 лет, в особенности с развитием технологии SDR (Software-defined radio), цены на данное оборудование фактически «обвалились» до уровня около 50 долл. за приемник с управляющим и аналитическим программным обеспечением [10; 11]. Причем это соответствует наиболее трудному случая — перехвату по ПЭМИН изображения на мониторе (пример организации указанного канала утечки с использованием SDR-технологии [12]).

На основании вышеизложенного можно заключить, что при формировании моделей угроз вновь создаваемых информационных систем следует уделять существенное внимание детальной проработке раздела технических каналов утечки. В уже функционирующих информационных системах с целью повышения степени их защищенности рекомендуется отказаться от использования в качестве устройств ввода клавиатур с интерфейсом ps/2.

Авторы благодарят государственное автономное учреждение Калининградской области «Калининградский государственный научно-исследовательский центр информационной и технической безопасности» за предоставленную альтернативную измерительную площадку и контрольно-измерительное оборудование.

Список литературы

1. *Базовая* модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. 15.02.2008 г.) // ФСТЭК России. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god (дата обращения: 12.12.2020).

2. *18th USENIX* Security Symposium 2009 in August 2009. URL: https:/www.usenix.org/legacy/event/sec09/tech/full_papers/sec09_attacks.pdf (дата обращения: 18.05.2020).

3. *Meynard O., Guilley S., Flament F.* Characterization of the Electromagnetic Side Channel in Frequency Domain // Information Security and Cryptology : 6th International Conference (Inscrypt 2010, Shanghai, China, October 20—24, 2010). Springer, 2011. P. 471—486.

4. *Закандаев Т.Ю., Степаненко В.М.* Оценка возможности перехвата побочных электромагнитных излучений клавиатуры компьютера. URL: http://ptmip.ipt.kpi.ua/wp-content/uploads/sites/6/2014/06/Zakandaev.pdf (дата обращения: 18.11.2020).

5. *Хорев А.* Оценка возможности перехвата побочных электромагнитных излучений клавиатуры компьютера // Специальная техника. 2011. № 5. С. 24—31.

6. *Гук М.* Аппаратные интерфейсы ПК : энциклопедия. СПб., 2002.

7. *Smulders P.* The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables // Computers & Security. 1990. № 9. P. 53—58.

8. *Амелина М.А., Амелин С.А.* Программа схемотехнического моделирования Micro-Cap 8. М., 2007.

9. *Хоровиц П., Хилл У.* Искусство схемотехники / пер. с англ. 2-е изд. М., 2014.

10. *Аминев А.В., Блохин А.В.* Измерения в телекоммуникационых системах. Екатеринбург, 2015.

11. *Галкин В.А.* Основы программно-конфигурируемого радио. М., 2013.

12. *Перехват* изображения с монитора по радиоканалу с помощью TempestSDR (ПЭМИН). 13.05.2018. URL: https://www.youtube.com/watch?v=PV_v1HgjN3Q (дата обращения: 12.12.2020).

Об авторах

Андрей Андреевич Персичкин — ст. преп., Балтийский федеральный университет им. И. Канта, Россия.

E-mail: a.persichkin@kgnic.ru

Наталья Витальевна Персичкина — ст. преп., Балтийский федеральный университет им. И. Канта, Россия.
E-mail: persichkina@rambler.ru

Светлана Геннадьевна Шпилевая — канд. пед. наук, доц., Балтийский федеральный университет им. И. Канта, Россия.
E-mail: SSHpilevaya@kantiana.ru

The authors

Andrey A. Persichkin, Assistant Professor, Immanuel Kant Baltic Federal University, Russia.
E-mail: a.persichkin@kgnic.ru

Natalia V. Persichkina, Assistant Professor, Immanuel Kant Baltic Federal University, Russia.
E-mail: persichkina@rambler.ru

Dr Svetlana G. Shpilevaya, Associate Professor, Immanuel Kant Baltic Federal University, Russia.
E-mail: SSHpilevaya@kantiana.ru