УДК 501

ОЦЕНКА ВОЗМОЖНОСТИ ПЕРЕХВАТА ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ КЛАВИАТУРЫ КОМПЬЮТЕРА

Т. Ю. Закандаев[1], В. М. Степаненко[1]

[1] *Національний технічний університет України «Київський політехнічний інститут»*

Аннотация

В статье рассмотрены причины возникновения побочных электромагнитных излучений (ПЭМИ) при вводе информации с клавиатуры в компьютер. Проведена оценка возможностей перехвата ПЭМИ клавиатуры компьютера техническими средствами разведки (ТСР). Предложены варианты защиты от перехвата побочных излучений.

Ключевые слова: ТЗИ, ПЭМИ, клавиатура

Вступление

К одной из основных угроз безопасности информации ограниченного доступа относится утечка информации по техническим каналам, под которой наиболее часто понимается неконтролируемое распространение информативного сигнала от его источника через физическую среду до технического средства, осуществляющего перехват информации.

Одним из опасных режимов работы СВТ (с точки зрения утечки информации по каналу ПЭМИ) является ввод данных с клавиатуры.

Клавиши клавиатуры функционально можно разбить на три группы: К первой группе относятся алфавитно-цифровые клавиши, предназначенные для ввода знаковой информации и команд, набираемых по буквам Ко второй группе относятся функциональные клавиши. Этих клавиш двенадцать (от F1 до F12), и размещены они в верхней части клавиатуры. К третьей группе относятся служебные клавиши, располагающиеся рядом с клавишами алфавитно-цифровой группы. К ним относятся клавиши SHIFT и ENTER, и тд.

В качестве датчиков нажатия клавиш применяют механические контакты (открытые или герконовые), кнопки на основе проводящих материалов, а также ёмкостные датчики. В клавиатуре коды символов, изображённых на клавишах, формирует контроллер (специализированный микропроцессор), последовательно опрашивающий все клавиши. Скэн- код (scan code) – это однобайтовое число, младшие 7 бит которого представляют идентификационный номер, присвоенный каждой клавише. Вид информативного сигнала в тракте клавиатуры зависит от её интерфейса. Проводные клавиатуры могут иметь интерфейс USB или PS/2.

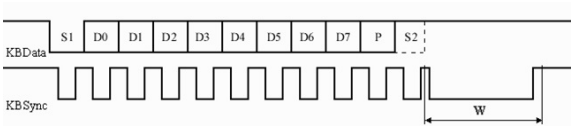

Рис. 1. Общий вид передачи данных от клавиатуры

1. Структура и спектр сигнала побочных электромагнитных излучений клавиатуры PS/2

Обмен данными между клавиатурой PS/2 и контроллером системной платы осуществляется асинхронно по последовательному протоколу. Для обмена данными в клавиатуре PS/2 служат две линии – данных (KBData) и синхронизации (KBSync).

Данные передаются в следующем порядке: один стартовый бит – «0»; восемь бит данных; бит чётности (сумма всех разрядов +1); один стоповый бит – «1». Общий вид передачи данных от клавиатуры представлен на рис. 1 [1].

Синхронизирующий сигнал представляет собой последовательность чередующихся «0» и «1», причём длительность импульса синхронизации в 2 раза меньше, чем длительность импульса данных. Таким образом, вид передаваемого в линию данных сигнала (последовательность нулей и единиц, формирующих пакет данных) будет зависеть от передаваемого скэнкода, а следовательно, будет меняться и частота передачи данных, что подтверждено экспериментально (см. таб. 1).

При прохождении импульсного сигнала от клавиатуры к системной плате по соедини-тельному кабелю, вокруг последнего возникает переменное электромагнитное поле (побочное электромагнитное излучение), спектр которого будет определяться видом импульсного сигнала. Проведённый анализ показал, что последовательность импульсов, близкая к периодической со скважностью $Q = T/\tau = 2$, подается в линию данных клавиатуры PS/2 при нажатии клавиши «=»: при нажатии этой клавиши в линию поступает последовательность импульсов 01010101011. Поэтому такой режим работы клавиатуры наиболее целесообразно использовать в качестве тестового.

На рис. 2 в качестве примера приведён спектр ПЭМИ клавиатуры Genius KB-06X2, работающей в тестовом режиме, нажата клавиша «=» .

Таблица 1. Частоты передачи данных в линию при нажатии некоторых клавиш

Клавиша	Частота синхронизирующей посылки, кГц	Частота передачи данных в линии данных, кГц	Вид передаваемогосигнала
=	12,35	6,25	10101010
1	12,35	3,10	01101000
2	12,35	6,25	01111000
Tab	12,35	6,25	10110000
Left Shift	12,35	4,11	01001000

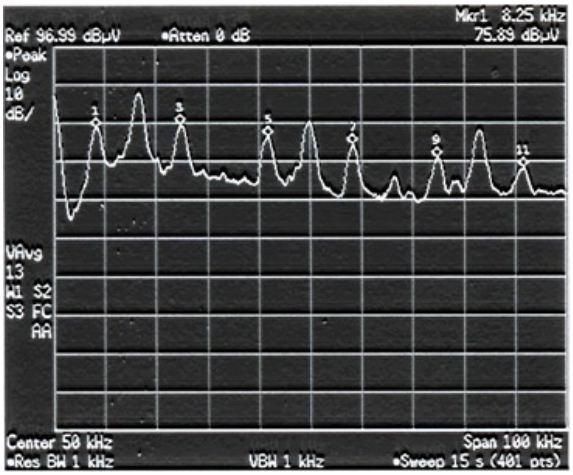

Рис. 2. Спектр ПЭМИ клавиатуры в тестовом режиме, нажата клавиша «=»

Одновременно с данными по тракту клавиатуры передаётся синхронизирующий сигнала, представляющий собой последовательность чередующихся «0» и «1» – 01010101010101010101. Учитывая, что длительность импульса синхронизирующего сигнала в два раза меньше, чем длительность импульса данных, частота передачи синхроимпульсов должна быть в два раза больше, чем частота передачи данных, и составлять $F = 16{,}5$ кГц. На рис. 2 наблюдаются 1, 3 и 5 гармоники сигнала синхронизации: сигналы на частотах 16,5 кГц, 49,5 кГц и 82,5 кГц. С точки зрения перехвата данных, вводимых с клавиатуры, синхронизирующий сигнал не является информативным

2. Методика оценки возможностей перехвата побочных электромагнитных излучений клавиатуры компьютера

Проведённый анализ показал, что для перехвата ПЭМИ клавиатуры диапазон рабочих частот комплекса должен составлять от 3 – 6 кГц до нескольких десятков и даже сотен МГц. Ширина полосы пропускания приёмного устройства должна перестраиваться в диапазоне от 1 кГц до 10 МГц с шагом не более 1 кГц. Уровень шумов приёмного устройства, измеренный при полосе пропускания приёмника $\Delta F = 1$ Гц, не должен превышать – 165 дБм. В комплексе должны использоваться направленные активные широкодиапазонные малошумящие антенны. Блок цифровой обработки сигналов должен обеспечивать обработку перехваченных сигналов в реальном масштабе времени.

При оптимальном приёме импульсного сигнала (каковым является информативный сигнал ПЭМИ клавиатуры) вероятность правильного приёма одиночного импульса с известной фазой (вероятность обнаружения детерминированного сигнала) P_0 рассчитывается по формуле (5):

$$P_0 \approx \Phi(q_c - \Phi^{-1}(1 - P_{fa})) \qquad (1)$$

где $q_c = \sqrt{2E_p/N_o}$ – отношение сигнал шум по напряжению на выходе согласованного фильтра (оптимального приёмника).

Выражение (1) даёт связь между вероятностью правильного обнаружения, вероятностью ложной тревоги и отношением сигнал/шум на выходе согласованного фильтра и определяет семейство кривых (рис. 2), называемых кривыми обнаружения (кривыми Неймана – Пирсона) [2].

Для распознавания нажимаемой клавиши клавиатуры необходимо перехватить её скэн-код, передаваемый контроллером клавиатуры в линию передачи данных. Полагая вероятности правильного обнаружения каждого импульса в сигнале скэн-кода независимыми, вероятность перехвата скэн-кода P можно рассчитать по формуле:

$$P_{sc} = \prod_{i=1}^{m} P_{0i} \approx (P_0)^m \qquad (2)$$

где $P_{o.i}$ – вероятность правильного обнаружения i-го импульса скэнкода; m – количество бит, используемых для передачи скэнкода.

Например, в клавиатуре PS/2 для передачи скэнкода клавиши используется восемь бит. Следовательно, вероятность перехвата скэн-кода будет равна $P_{sc} \approx (F_0)^8$.

Задаваясь пороговым значением вероятности перехвата скэн-кода P_{sci} и вероятности ложной тревоги P_{fa} из формул (1) и (2), легко рассчитать предельно допустимое (пороговое) значение отношения сигнал/шум σ: для детерминированного сигнала:

$$\sigma \approx \Phi^{-1}(\sqrt[m]{P_{sci}}) + \Phi^{-1}(1 - P_{fa}) \qquad (3)$$

Для сигнала со случайной фазой:

$$\sigma \approx \Phi^{-1}(\sqrt[m]{P_{sci}}) + \sqrt{2\ln(\frac{1}{P_{fa}})} \qquad (4)$$

Пороговое значение отношения сигнал/ шум также может быть определено по графикам (кривым Неймана – Пирсона) [2].

Таким образом, для оценки возможностей по перехвату ПЭМИ клавиатуры необходимо рассчитать отношение сигнал/шум по напряжению на выходе согласованного фильтра (оптимального приёмника) q и сравнить его с пороговым значением σ.

Учитывая, что для оптимального приёмника полоса пропускания фильтра $\Delta F = 1/\tau$, и допуская, что форма импульса прямоугольная, отношение сигнал/шум по напряжению на выходе согласованного фильтра (оптимального приёмника) q можно рассчитать по формуле:

$$q_c = \sqrt{\frac{2E_p}{N_0}} \approx \sqrt{\frac{2P_p \cdot \tau}{N_0}} = \sqrt{\frac{2P_p}{N_0 \cdot \Delta F}} \qquad (5)$$

где P_p – мощность одиночного импульса на входе разведывательного приёмника. Полагая, что сопротивление антенны и входа приёмника согласованы, формулу (5) запишем в виде

$$q_c = \frac{U_p}{\sigma_n \cdot \sqrt{\Delta F}}$$

где U_p – напряжение сигнала на входе разведывательного приёмника, σ_n – среднеквадратическое значение напряжения шума, приведённое ко входу разведывательного приёмника и измеренное при полосе пропускания 1 Гц.

Таким образом показана возможность создания приемника в неконтролируемой зоне. Поскольку определены параметры которые влияют на перехват, можем предложить защиту клавиатуры.

Первый способ заключается в экранировании клавиатуры. Пластмассовый корпус обрабатывается металлическим напылением, или заменяется корпусом из тонкого листового железа. Провод тоже заменяется на экранированый.

Второй способ – реализация динамического изменения таблицы скэн-кодов со стороны клавиатуры, и обратное декодирование в стандартную таблицу в PS/2 интерфейсе специальным декодером. Так как основным излучателем является провод клавиатуры, выступающий в роли антены, даже если удастся перехватить сигнал со скэн-кодом, будет сложно сопоставить его с клавишей, которая была им закодирована.

Выводы

В статье рассмотрен принцип работы клавиатуры с точки зрения защиты информации.

- Был исследован спектр излучений PS/2 клавиатуры.
- Проанализировано его составляющие (синхронизирующие и информационные составляющие).
- Определено пороговое отношение сигнал/шум для детерменированого сигнала, и сигнала со случайной фазой, которое показывает возможность перехвата ПЭМИ клавиатуры компьютеров средствами разведки.

С точки зрения защиты информации для уменьшения соотношения сигнал/шум было предложено:

- использование клавиатуры в экранированом корпусе, с экранированим кабелем
- доработка клавиатуры с помошью реализации динамического изменения таблици скэн-кодов.

Перечень использованых источников

1. Статья в электронном портале http://kazus.ru Имитируем работу клавиатуры
2. Исаков В.И Статистическая теория радиотехнических систем: курс лекций Електронный конспект