МЕТОДИКА ОЦЕНКИ УРОВНЯ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА С ПОМОЩЬЮ SDR ПРИЕМНИКА

Белорусский государственный университет информатики и радиоэлектроники, Минск, Республика Беларусь

Маласай В. А.

Борботько Т. В. - доктор техн. наук, профессор

В настоящее время известно достаточное количество сценариев похищения данных с персонального компьютера. Канал утечки информации за счет побочных электромагнитных излучений (ПЭМИ) является далеко не новым. Однако в силу особенностей, связанных со значительной дальностью перехвата, возможностью бесконтактного съёма информации, а также из-за развития и доступности технических средств разведки, он остаётся достаточно опасным.

Средства вычислительной техники (СВТ), обрабатывающие защищаемую информацию, можно рассматривать как совокупность элементарных электрических и магнитных излучателей. При обработке, хранении и передаче информации СВТ возникает изменение электрических токов, проходящих по токопроводящим элементам и образование разности потенциалов между различными точками цепи, которые в свою очередь порождают электрические и магнитные поля.

Узлы и элементы СВТ, в которых возникают большие перепады напряжения и достаточно малые токи, формируют в ближней зоне электромагнитное поле с преобладанием электрической составляющей. Узлы и элементы СВТ, в которых протекают большие токи, и возникают относительно малые перепады напряжения, создают в ближней зоне электромагнитное поле с преобладанием магнитной составляющей. Именно поэтому при измерении ПЭМИ важно рассматривать обе составляющие электромагнитного поля.

Восстановление информации при перехвате излучений цепей, по которым передается видеосигнал, — это один из тех случаев, когда при использовании многоразрядного (как минимум три разряда для цветного монитора) параллельного кода формат представления информации позволяет восстанавливать большую ее часть (теряется цвет, но может быть восстановлено смысловое содержание), не восстанавливая при этом последовательности значений каждого разряда кода.

К безопасным информативным излучениям ПК можно отнести из лучения цепей, формирующих шину данных системной шины и внутреннюю шину данных микропроцессора, а также излучения других цепей, служащих для передач информации, представленной в виде многоразрядного параллельного кода.

С помощью resistor-transistor logic Software defined radio (RTL-SDR) приёмников (программно-определяемое радио) можно принимать сигналы, декодировать их, а также раскладывать на составляющие. Одной из задач исследования является определение эффективности применения приёмника на практике для определения наличия ПЭМИ технических средств в качестве недорогого аналога сертифицированных комплексов. В настоящее время на рынке существует достаточное количество SDR донглов. Все их можно разделить на два типа: 1. Устройства, позволяющие работать только в качестве приёмной стороны; 2. Устройства, позволяющие работать в качестве как приёмника, так и передатчика (полудуплексный метод).

Экспериментально с помощью RTL-SDR приемника исследованы источники побочных электромагнитных излучений монитора (VGA/DVI интерфейсы). Таким образом, проведены экспериментальные исследования утечек информации за счет ПЭМИ по интерфейсам VGA, DVI монитора, и выполнен сравнительный анализ результатов с результатами, полученными с помощью профессионального измерительного комплекса. По каждому из рассмотренных интерфейсов представлены амплитудно-частотные характеристики [6]. Максимальная разница опасных сигналов по частоте у сравниваемых комплексов не превышает 6 кГц, что свидетельствует о возможности применения RTL SDR приемника в учебных целях. Разницу частот можно объяснить несовершенством самого RTL-SDR приемника и большим количеством внутренних шумов на высоких частотах. По результатам исследований разработан лабораторный стенд по обнаружению ПЭМИ, с помощью которого обучающиеся знакомятся с физическими принципами обнаружения утечек информации за счет ПЭМИ.

Оценка защищённости информации на объекте вычислительной техники (ОВТ) по каналу ПЭМИ является обязательной частью при аттестации соответствующего объекта информатизации.

Список использованных источников:

Алексеенко В.И., Петраков А.В., Лагутин В.С. Техническая защита информации / Алексеенко В.И., Петраков А.В., Лагутин В.С. // Вестник связи – 1994. [Электронный ресурс]. - Режим доступа: https://www.twirpx.com/file/26236/ - Дата доступа: 14.12.2019.

Лысов А.В., Остапенко А.Н. Промышленные шпионаж в России: методы и средства / Лысов А.В., Остапенко А.Н. // СПб.: Лаборатория ППШ – 1994. [Электронный ресурс]. - Режим доступа: http://www.bnti.ru/showart.asp?aid=729&lvl=04. - Дата доступа: 21.12.2019.

Максимов Ю.Н., Сонников В.Г., Петров В.Г. Технические методы и средства защиты информации / Максимов Ю.Н., Сонников В.Г., Петров В.Г. // СПб.: ООО «Издательство Полигон» – 2000. [Электронный ресурс]. - Режим доступа: https://search.rsl.ru/ru/record/01000687101 - Дата доступа: 05.01.2020.

Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации / Хорев А.А. // М.: НПЦ «Аналитика» – 2008. [Электронный ресурс]. - Режим доступа: https://booksee.org/book/597367 - Дата доступа: 14.02.2020.