УДК 537.8

ПОБОЧНЫЕ ЭЛЕКТРОМАГНИТНЫЕ ИЗЛУЧЕНИЯ ОТ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ КАК УГРОЗА УТЕЧКИ ИНФОРМАЦИИ

БУНЕВИЧ М. А., МАЙОРОВ А. И., МАРМУЗЕВИЧ М. А., ВРУБЛЕВСКИЙ И. А.

Белорусский государственный университет информатики и радиоэлектроники
(г. Минск, Республика Беларусь)

E-mail: mike_box@bk.ru, hottab2000@gmail.com, mail.may2991@gmail.com, vrublevsky@bsuir.edu.by

Аннотация. Электронные устройства обработки и передачи информации при своей работе генерируют побочные электромагнитные излучения, которые являются паразитными. В рамках работы произведена оценка возможности перехвата информации, передаваемой по видеотракту ПЭВМ, с помощью *SDR*-приемников таких как *RTL-SDR USB Stick, RTL-SDR v3* и AirSpy. Показано, что с помощью приемника *AirSpy* можно перехватить текстовую информацию с ЭЛТ-монитора только при разрешении 800x600 и частоте кадровой развертки 60 Гц с расстояния не более 2 метров. Полученные результаты свидетельствуют, что имеется реальная угроза перехвата текстовой информации или изображений не только с помощью узкоспециализированного дорого оборудования, но и бытовыми радиоприемниками и недорогими радиотехническими устройствами, которые широко представлены на рынке.

Abstract. Electronic devices for processing and transmitting information during their operation generate side electromagnetic emission, which are parasitic. Within the framework of the work, an assessment was made of the possibility of intercepting information transmitted through the video path of a PC using SDR receivers like as RTL-SDR USB Stick, RTL-SDR v3 and AirSpy. It is shown that using the AirSpy receiver it is possible to intercept text information from a CRT monitor only at a resolution of 800x600 and a vertical scan rate of 60 Hz from a distance of no more than 2 meters. The results obtained indicate that there is a real threat of interception of a text information or images not only with the help of highly specialized expensive equipment, but also with household radios and inexpensive radio devices that are widely represented on the market.

Практически все электронные устройства обработки и передачи информации генерируют электромагнитные излучения, являющиеся паразитными, т.е. побочными. В зависимости от вида излучателя и расстояния от него до точки измерения, соотношение между компонентами побочного электромагнитного поля отличается [1]. Основными распределенными источниками электромагнитного поля являются симметричные и несимметричные кабели.

Поскольку подавляющее большинство персональных электронно-вычислительных машин (далее — ПЭВМ) для передачи информации использует цифровые интерфейсы, задача потенциального злоумышленника по перехвату информации по каналу побочных электромагнитных излучений (далее – ПЭМИ) в общем случае заключается в решении бинарной задачи: определить, что

Развитие перечисленных выше технологий привели к появлению нового типа устройств, так называемых программно-определяемых радиосистем (Software Defined Radio, далее – SDR).

Схема типичного SDR-приемника показана на рисунке 1. Входной сигнал усиливается и делится на компоненты I и Q путем смешивания с сигналом гетеродина (для получения квадратурной компоненты он смещается на 90°). Эта архитектура получила название прямое преобразование. После фильтрации сигналов основной полосы в фильтре нижних частот, они оцифровываются в паре аналогово-цифровых преобразователей. Далее в цифровом преобразователе частота сигнала понижается до рабочего диапазона процессора управляющего компьютера. В настоящее время *SDR*-приемники доступны в свободной продаже.

Обработка сигнала осуществляется программным обеспечением (далее – ПО). Широкое распространение получило открытое ПО такое как: *GNURadio, SDRSharp, LimeSDR, HDSDR, Gqrx* и другие. Данные программы имеют различный интерфейс и отличаются функционалом, но суть у них одна: обработка принятого оцифрованного сигнала в соответствии с параметрами, заданными пользователем. Перечисленное ПО доступно для всех популярных операционных систем.

В рамках работы была произведена оценка возможности перехвата информации, передаваемой по видеотракту ПЭВМ, за счет ПЭМИ с помощью *SDR*-приемников *RTL-SDR USB Stick, RTL-SDR v3* и AirSpy.

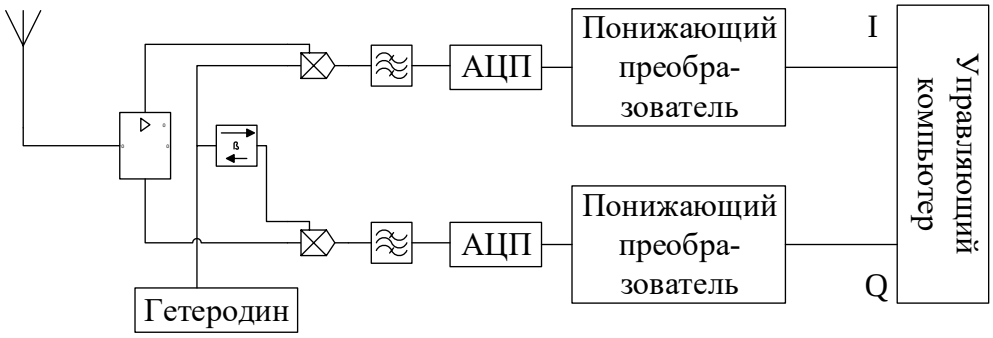

Рис. 1. Структурная схема типичного *SDR*-приемника.

Прием сигналов ПЭМИ велся на штыревые антенны различной длины, дипольную активную антенну АИ 5-0 и другие. В качестве источника сигналов ПЭМИ выступала ПЭВМ соединенная по средствам интерфейса *VGA* с жидкокристаллическим монитором (далее – ЖК-монитор) или монитором с электронной лучевой трубкой (далее – ЭЛТ-монитор).

Эксперимент проводился при нормальном уровне электромагнитных шумов в условиях городской застройки. На мониторы выводилась текстовая большим шрифтом и тест-изображение, представляющее собой чередование черных и белых пикселей.

При использовании приемника *RTL-SDR USB Stick* удалось обнаружить сигнал ПЭМИ на расстоянии до 5 метров при эксплуатации ПЭВМ с ЭЛТ-монитором и на расстоянии 3 метров – с ЖК-монитором, однако восстановить изображение из принятого сигнала не удалось.

При использовании приемника *RTL-SDR v3* удалось обнаружить сигнал ПЭМИ на расстоянии до 7 метров при эксплуатации ПЭВМ с ЭЛТ-монитором и на расстоянии 4 метров – с ЖК-монитором, восстановить изображение из принятого сигнала также не удалось.

С помощью приемника *AirSpy* удалось перехватить текстовую информацию только при разрешении монитора 800x600 и частотой кадровой развертки 60 Гц на расстоянии 2 метра с ЭЛТ-монитором. Результат перехвата показан на рис. 2. Также перехваченное изображение реагировало на вывод тест-изображения на значительно больших расстояниях, чем предыдущие образцы.

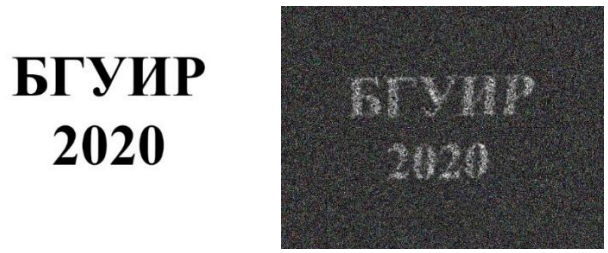

Рис. 2. Исходное и перехваченное изображение.

Неудачные попытки перехвата изображения с помощью приёмников *RTL-SDR USB Stick* и *RTL-SDR* связаны с небольшой пропускной способностью этих приёмников.

Таким образом существует реальная угроза перехвата изображения не специализированным оборудованием, которое стоит на вооружении спецслужб, а, фактически бытовым радиоприемником и оборудованием общей стоимостью около 200$. Такое положение вещей требует пересмотреть модель угроз информационной безопасности, принятую в организации и обеспечить вокруг ПЭВМ, на которых обрабатывается конфиденциальная информация, максимально возможную контролирую зону.

Список использованных источников

1. Гольдштейн Л. Д., Зернов Н. В. Электромагнитные поля и волны // М.: «Советское радио». 1971. 664 с.
2. Крылова С. Л. Исследование побочных электромагнитных излучений видеосистемы ПЭВМ в учебной лаборатории информационной безопасности [Электронный ресурс] — Режим доступа: https://www.sworld.com.ua/konfer35/597.pdf — Дата доступа 11.04.2018
3. Оценка возможности перехвата информации, передаваемой по видеотракту ПЭВМ, с помощью SDR-приемника // Материалы 24 научно-практической конференции «Комплексная защита информации»/ – С. 58-63.