УДК 004.353 Вестник УрФО № 4(34) / 2019, с. 15–21

Асяев Г. Д., Антясов И. С., Уфимцев М. С.

DOI: 10.14529/secur190402

ИССЛЕДОВАНИЕ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ МОНИТОРА С ПОМОЩЬЮ RTL-SDR ПРИЕМНИКА

Рассмотрены физические принципы образования побочных электромагнитных излучений (ПЭМИ), а также типовые элементы средств вычислительной техники, которые создают ПЭМИ при обработке информации с их использованием. Проведён анализ имеющихся на рынке RTL-SDR приемников, а также комплексов оценки защищённости технических средств от утечки по ПЭМИ. Выполнены экспериментальные исследования утечек информации за счет ПЭМИ по интерфейсам VGA, DVI монитора с помощью RTL-SDR приемника. Сравнительный анализ полученных результатов показал, что технические и функциональные возможности RTL-SDR приемника не уступают современным сертифицированным комплексам по обнаружению ПЭМИ. На основе проведенных исследований разработан лабораторный стенд, который может быть использован в учебном процессе для ознакомления обучающихся с физическими принципами обнаружения утечек информации за счет ПЭМИ.

Ключевые слова: *побочные электромагнитные излучения, средства вычислительной техники, программно-определяемый приемник (RTL-SDR), аналоговый видеоинтерфейс, цифровой видеоинтерфейс, отношение сигнал/шум, амплитудно-частотная характеристика.*

Asyaev G. D., Antyasov I. S., Ufimcev M. S.

INVESTIGATION OF SPURIOUS ELECTROMAGNETIC RADIATION FROM A MONITOR USING AN RTL-SDR RECEIVER

The physical principles of the formation of secondary electromagnetic radiation (TEMPEST), typical elements of computer technology that create TEMPEST when processing information using them are considered. The analysis of RTL-SDR receivers available on the market, as well as complexes for assessing the protection of technical equipment from leakage by TEMPEST, is carried out. Experimental studies of information leaks due to TEMPEST on the VGA, DVI monitor

interface using the RTL-SDR receiver were performed. A comparative analysis of the results showed that the technical and functional capabilities of the RTL-SDR receiver are not inferior to modern certified complexes for detecting TEMPEST. Based on the research, a laboratory stand was developed that can be used in the educational process to familiarize students with the physical principles of detecting information leaks due to TEMPEST.

Keywords: *spurious electromagnetic radiation, computer facilities, resistor-transistor logic software-defined radio (RTL-SDR) receiver, video graphic array (VGA), digital visual interface (DVI), signal-to-noise ratio, frequency response.*

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.

Оценка защищённости информации на объекте вычислительной техники (ОВТ) по каналу ПЭМИ является обязательной частью при аттестации соответствующего объекта информатизации. Разработанный в рамках приведённого исследования стенд с минимальными затратами позволяет продемонстрировать все вышеуказанные особенности исследуемого канала.

Целью работы является исследование утечек информации за счет ПЭМИ цифровых и аналоговых интерфейсов монитора с помощью RTL-SDR приемника.

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 [1].

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.

Стоит отметить, что на персональной электронно-вычислительной машине (ПЭВМ), ведущей обработку защищаемой информации, т.е. являющейся основным техническим средством приема, обработки и передачи информации (ОТСС), не разрешается использование беспроводных устройств [2]. Поэтому в типовой состав автоматизированного рабочего места (АРМ) не входят беспроводные клавиатура и мышь, а также не используются протоколы Bluetooth, Wi-Fi и т.д. В состав типового АРМ могут входить: монитор, клавиатура, мышь, принтер и системный блок, включая материнскую плату, видеокарту, звуковую карту, накопитель на жёстком диске, оптический привод.

Специальные исследования (СИ) – комплекс мероприятий, направленных на выявление технических каналов утечки информации. Проанализировав рынок технической защиты информации, можно выделить следующие сертифицированные системы по проведению оценки защищённости технических средств по каналу ПЭМИ:

1. Сигурд (производитель «Маском»). Основное назначение – проведение измерений электромагнитного излучения и наводок при проведении СИ. Выделяют модификации: «М3», «М5», «М7», «М8», «М19». Имеет свидетельство об утверждении типа средств измерений. Цена от 2 000 000 руб.

2. Навигатор (производитель «НЕЛК»). Основное назначение: оценка защищённости средств вычислительной техники от утечки информации по каналу ПЭМИ. Выделяют модификации: «П3М», «П4М», «П5М», «П6М». Имеет свидетельство об утверждении типа средств измерений. Цена от 2 500 000 руб.

3. Легенда (производитель «Гамма»). Основное назначение: оценка защищённости средств вычислительной техники от утечки информации по каналу ПЭМИ. Выделяют модификации: «11», «05М». Имеет свидетельство

об утверждении типа средств измерений. Цена от 1 800 000 руб.

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. Например, устройство фирмы Kebudu (рис. 1). Основными недостатками этого SDR приёмника является малая частота дискретизации и ограниченный частотный диапазон. Основным преимуществом является невысокая стоимость данного устройства.

2. Устройства, позволяющие работать в качестве как приёмника, так и передатчика

Рис. 1. Внешний вид RTL-SDR приёмника

Рис. 2. Внешний вид устройства HackRF One.

(полудуплексный метод). Например, HackRF One, обладающий достаточно большим спектром возможностей (рис. 2). Это устройство может принимать сигналы на частотах 10 МГц – 6 ГГц и передавать их. С помощью платы расширения можно организовать полнодуплексную связь. Цена: 10 000 руб.

Поскольку в рамках исследования возможности передачи сигнала не требовались, для проведения эксперимента использовано устройство RTL-SDR с чипсетом RTL2832U, относящееся к устройствам первого типа (рис. 1) [3]. Приёмник представляет собой широкополосный радиосканер и имеет характеристики, представленные в табл. 1.

Экспериментально с помощью RTL-SDR приемника исследованы источники побочных электромагнитных излучений монитора (VGA/DVI интерфейсы).

Исследование интерфейса VGA на наличие ПЭМИ. В качестве исследуемого устройства использован монитор Acer V226HQL. Антенна расположена на максимально возможном удалении от исследуемого порта. В качестве тестового сигнала использован режим

Таблица 1

Характеристики RTL-SDR приёмника

Характеристика	Значение
Частотный диапазон	0,001 – 1864 МГц
Полоса пропускания	3,2 МГц
Частота дискретизации	3,2 миллиона семплов в секунду
Разрешение АЦП	8 бит квадратурное семплирование
Чипсет	Realtek RTL2832U
Совместимость	Windows XP, Windows7/8/10, Linux
Поддержка программ	SDRSharp, GNURadio
Разъёмы	Входной: SMA
	Выходной: USB 2.0
Входной импеданс	50 Ом

Рис. 3. АЧХ опасного сигнала VGA (74.22 МГц).

«пиксель через пиксель» [4]. На рис. 3 изображён сигнал на частоте 74,22 МГц, который можно отнести к категории опасных, поскольку его можно перехватить. Наличие боковых составляющих сигнала и центральной частоты при включенном тестовом сигнале свидетельствует об уверенном обнаружении ПЭМИ.

На рис. 4 представлена АЧХ интерфейса VGA, которую удалось обнаружить с помощью поверенной антенны АИ 5-0 и анализатора спектра LIG NEX 1. АЧХ, представленная на рис. 4, по своим энергетическим составляющим подобна АЧХ (рис. 3).

выбрано в связи с особенностями работы самого интерфейса [5]. На рис. 5 изображен участок АЧХ монитора при выключенном тестовом сигнале. Следует заметить, что уровень опасного сигнала выходит за пределы шумов.

Отличительной особенностью интерфейса DVI является наличие энергетической составляющей даже при работающем экране, но при выключенном тестовом сигнале как на рис. 6.

На рис. 7 показан участок АЧХ интерфейса при выключенном мониторе. Никаких «опасных всплесков» не обнаружено.

При выключенном тестовом сигнале на

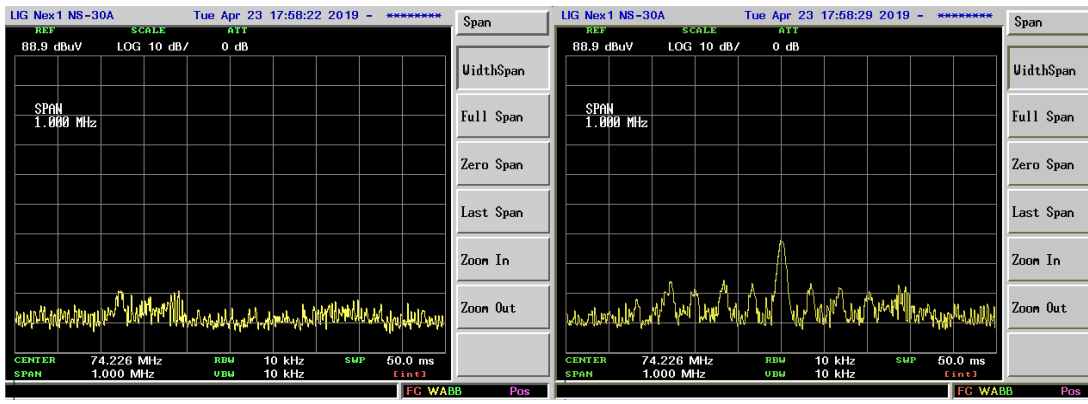

Рис. 4. АЧХ опасного сигнала VGA (74.226 МГц).

При исследовании DVI интерфейса использовался тестовый сигнал, имеющий цветовую расцветку RGB 63-63-63. Это значение частоте 148,5 МГц также наблюдаются статичные энергетические составляющие (рис. 8).

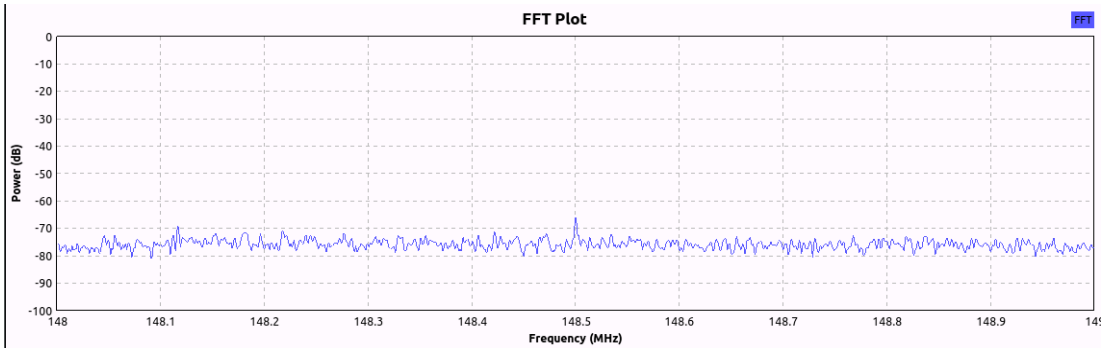

Рис. 5. АЧХ опасного сигнала DVI при выключенном мониторе (148,5 МГц).

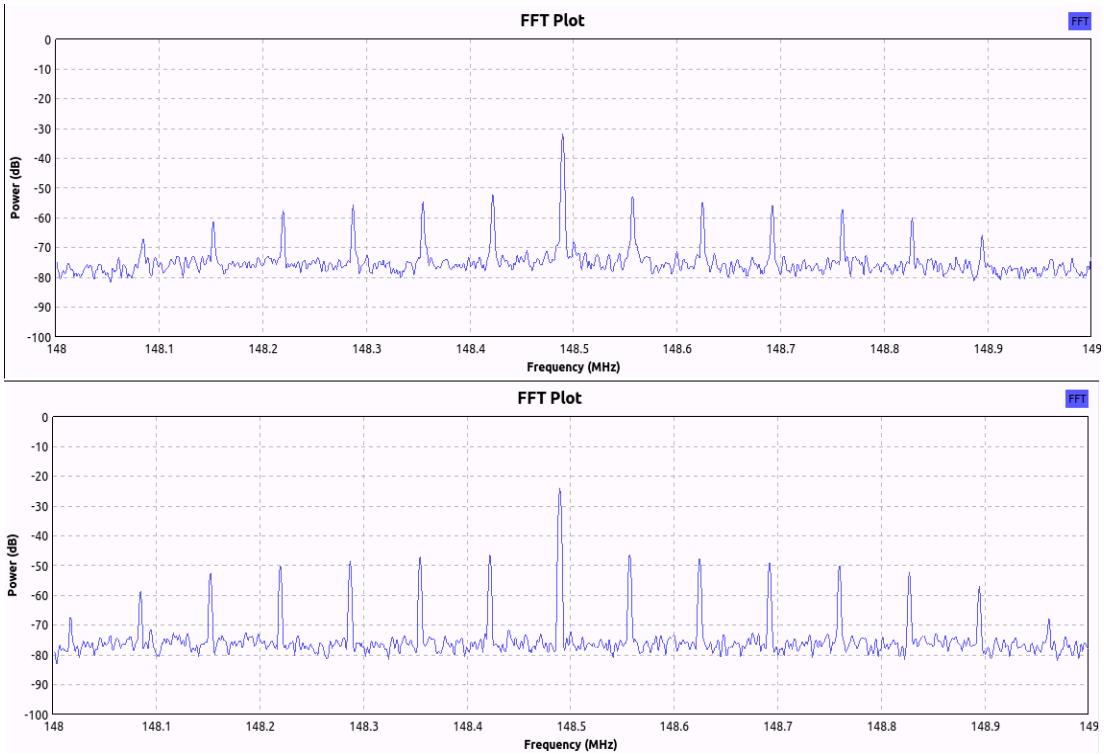

Рис. 6. АЧХ опасного сигнала DVI (148.495 МГц).

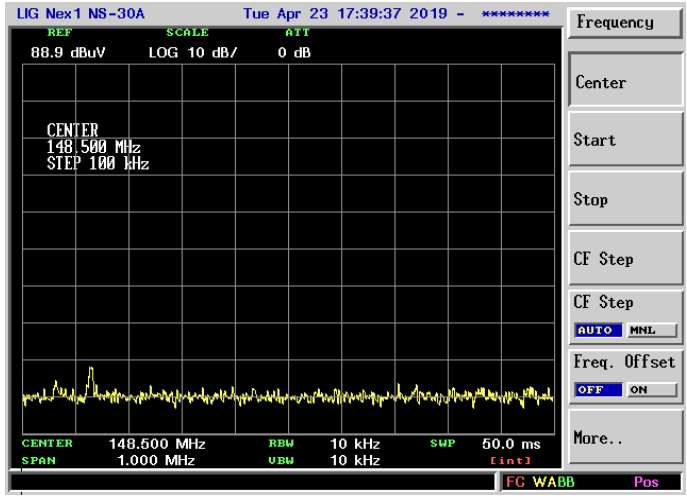

Рис. 7. АЧХ сигнала DVI при выключенном мониторе

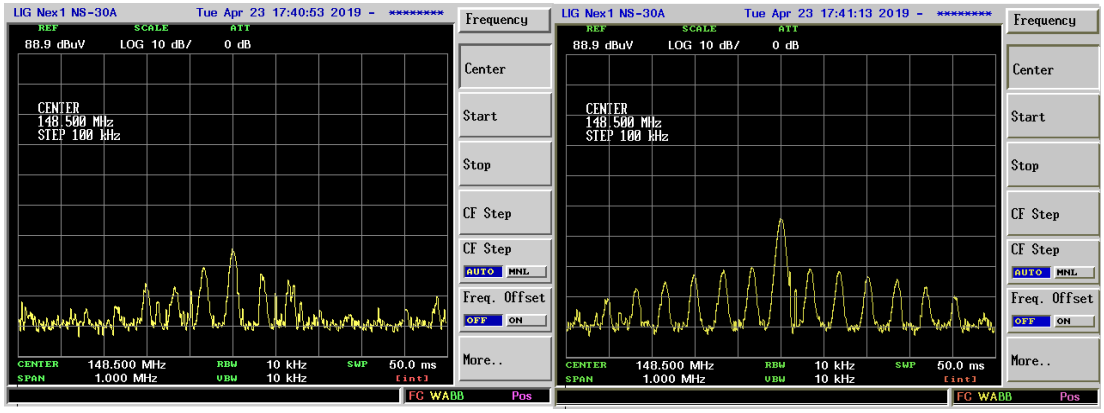

Рис. 8. АЧХ опасного сигнала DVI (148,500 МГц).

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.

Статья выполнена при поддержке Правительства РФ (Постановление №211 от 16.03.2013 г.), соглашение № 02.A03.21.0011.

Литература

1. Алексеенко В.И., Петраков А.В., Лагутин В.С. Техническая защита информации // Вестник связи. – 1994. – № 12. – С. 27 – 34.

2. Вартанесян В. А. Радиоэлектронная разведка. – М.: Воениздат, 1991. – 254 с.

3. Лысов А. В., Остапенко А. Н. Промышленный шпионаж в России: методы и средства. – СПб.: Лаборатория ППШ, 1994. –71 с.

4. Петровский В.И., Седельников Ю.Е. Электромагнитная совместимость радиоэлектронных средств: Учебное пособие для вузов. – М.: Радио и связь, 1986. – 216 с.

5. Технические методы и средства защиты информации/Ю. Н. Максимов, В. Г. Сонников, В. Г. Петров и др. – СПб.: ООО «Издательство Полигон», 2000. – 320 с.

6. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. – М.: НПЦ «Аналитика», 2008. – 436 с.

References

1. Alekseenko V.I., Petrakov A.V., Lagutin V.S. Tekhnicheskaya zashchita informatsii // Vestnik svyazi. – 1994. – № 12. – S. 27 – 34.

2. Vartanesyan V. A. Radioelektronnaya razvedka. – M.: Voenizdat, 1991. – 254 s.

3. Lysov A. V., Ostapenko A. N. Promyshlennyy shpionazh v Rossii: metody i sredstva. – SPb.: Laboratoriya PPSh, 1994. –71 s.

4. Petrovskiy V.I., Sedel'nikov Yu.E. Elektromagnitnaya sovmestimost' radioelektronnykh sredstv: Uchebnoe posobie dlya vuzov. – M.: Radio i svyaz', 1986. – 216 s.

5. Tekhnicheskie metody i sredstva zashchity informatsii/Yu. N. Maksimov, V. G. Sonnikov, V. G. Petrov i dr. – SPb.: OOO «Izdatel'stvo Poligon», 2000. – 320 s.

6. Khorev A. A. Tekhnicheskaya zashchita informatsii: ucheb. posobie dlya studentov vuzov. V 3 t. T. 1. Tekhnicheskie kanaly utechki informatsii. – M.: NPTs «Analitika», 2008. – 436 s.

АНТЯСОВ Иван Сергеевич, старший преподаватель кафедры защиты информации, Южно-Уральский государственный университет (национальный исследовательский университет). 454080, г. Челябинск, проспект им. В.И. Ленина, 76. E-mail: antiasovis@susu.ru

АСЯЕВ Григорий Дмитриевич, аспирант кафедры защиты информации, Южно-Уральский государственный университет (национальный исследовательский университет). 454080, г. Челябинск, проспект им. В.И. Ленина, 76. E-mail: asiaevgd@susu.ru

УФИМЦЕВ Максим Сергеевич, аспирант кафедры защиты информации, Южно-Уральский государственный университет (национальный исследовательский университет). 454080, г. Челябинск, проспект им. В.И. Ленина, 76. E-mail: ufimtcevms@susu.ru

ANTYASOV Ivan Sergeevich, Senior Lecturer, Information Security Department, South Ural State University (National Research University). 454080, Chelyabinsk, etc. them. IN AND. Lenin, 76. E-mail: antiasovis@susu.ru

ASYAEV Grigorii Dmitrievich, Postgraduate Student, Department of Information Security, South Ural State University (National Research University). 454080, Chelyabinsk, etc. them. IN AND. Lenin, 76. E-mail: asiaevgd@susu.ru

UFIMTSEV Maxim Sergeevich, Postgraduate Student, Information Security Department, South Ural State University (National Research University). 454080, Chelyabinsk, etc. them. IN AND. Lenin, 76. E-mail: ufimtcevms@susu.ru