УДК 004.35
DOI 10.53403/9785951505200_566

ВОПРОСЫ ПРИМЕНЕНИЯ ПРОГРАММНО-ОПРЕДЕЛЯЕМЫХ РАДИОСИСТЕМ ПРИ СОЗДАНИИ МОБИЛЬНОГО КОМПЛЕКСА ИЗМЕРЕНИЯ УРОВНЕЙ ПОБОЧНОГО ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ

Груздев Сергей Владимирович (staff@vniief.ru), Чернышов Сергей Александрович, Лебедева Александра Витальевна[1]

ФГУП «РФЯЦ-ВНИИЭФ», г. Саров Нижегородской обл.
[1]СарФТИ НИЯУ МИФИ, г. Саров Нижегородской обл.

В работе рассматривается возможность применения программно-определяемых радиосистем для приема сигналов побочного электромагнитного излучения. Описываются особенности построения таких систем. Рассматриваются свойства исследуемых сигналов. Дана оценка возможности применения таких систем для выполнения задач измерения.

Ключевые слова: ПЭМИ, программно-определяемая радиосистема, средство вычислительной техники, специальные исследования, измерительный приемник.

QUESTIONS OF THE APPLICATION OF SOFTWARE-DEFINED RADIO SYSTEM WHEN CREATING A MOBILE COMPLEX FOR MEASURING THE LEVELS OF SIDE ELECTROMAGNETIC EMANATION

Gruzdev Sergei Vladimirovich (staff@vniief.ru), Chernyshov Sergei Alexandrovich, Lebedeva Alexandra Vitalievna[1]

FSUE «RFNC-VNIIEF», Sarov Nizhny Novgorod region
[1]SarFTI NRNU MIPHI, Sarov Nizhny Novgorod region

This paper deals with possibility of usage of Software-Depended Radiosystem for receiving compromising electromagnetic emanations. The features of the construction of such systems are described. The properties of the signals under study are considered. An assessment is given of the possibility of using such systems for performing measurement tasks.

Key words: secondary electromagnetic emanation, software-difinied radio system, computer aids, background investigations, measuring receiver.

Угрозы утечки информации

В современном мире трудно представить обработку большого объема данных без применения средств вычислительной техники (СВТ). Компьютерные технологии проникли во все сферы человеческой жизни и без их применения не обходится ни одна современная организация. Однако при использовании СВТ как основного средства обработки и хранения информации возникают вопросы, решение которых требует комплексного подхода. Например, при обработке конфиденциальной информации необходимо обеспечить ее сохранность.

Утечка информации возможна как при утрате физического носителя, так и по техническим каналам. Во втором случае физические поля, возникающие в процессе функционирования СВТ, могут содержать информацию и распространяются в окружающем пространстве. Совокупность источника информации, несанкционированного приемника и среды распространения называют техническим каналом утечки информации (ТКУИ).

Одним из потенциально опасных ТКУИ является побочное электромагнитное излучение (ПЭМИ). Его возникновение обусловлено тем, что обработка информации связана с протеканием по цепям СВТ токов. Протекание изменяющегося во времени тока вызывает возникновение электромагнитного излучения, а поскольку величина тока переносит информацию, излучение так же может быть модулировано ей.

Методы противодействия утечке информации по каналу побочного электромагнитного излучения

Для противодействия утечке информации по каналу ПЭМИ могут применяться активным и пассивные методы защиты. К пассивным методам защиты относятся:

– организация контролируемой зоны, на которой неконтролируемое пребывание посторонних лиц исключено организационными мерами с радиусом не меньшим, чем радиус распространения опасных сигналов;

– использование экранирующих экранов, оплеток, экранированных кабелей в составе СВТ, разработка СВТ с учетом требований по минимизации побочных излучений;

– работа с СВТ в экранированных помещениях с гарантированным уровнем ослабления сигналов.

К активным методам защиты относят применение генераторов шума, которые создают помехи на пути распространения сигналов и не позволяют злоумышленнику восстановить информацию с заданной достоверностью.

Для оценки эффективности применяемых мер противодействия необходимо оценить отношение сигнал/шум на границе контролируемой зоны. Данная задача решается при проведении специальных исследований, однако этот процесс требует использования габаритного и дорогостоящего оборудования. С целью получения достоверных и повторимых результатов условия, при которых проводятся измерения, должны быть регламентированы. На практике это достигается использованием измерительных площадок, чьи геометрические характеристики жестко заданы в руководящих документах регулирующих органов, например, ФСТЭК России. Кроме обязательного использования измерительной площадки так же могут устанавливаться ограничения на климатические условия, параметры питающего напряжения и конфигурацию исследуемой системы. Таким образом, проведение специальных условий формализовано, требует перемещения объекта специальных исследований на измерительную площадку и применения громоздкой и дорогостоящей специальной аппаратуры.

Особенности систем, построенных по модели SDR

На практике возможны случаи, когда объект защиты располагается стационарно и не может быть легко перенесен на измерительную площадку, или необходимо произвести измерения в условиях расположения объекта защиты с учетом всех принимаемых мер [1, 2]. Тогда встает вопрос создания портативного мобильного комплекса, который бы позволил проводить оценку эффективности мер противодействия утечке информации по каналу ПЭМИ. Основой такого комплекса может являться программно-определяемая радиосистема (SDR). В простейшем случае в качестве основного элемента такой системы используется аналого-цифровой преобразователь (АЦП), подключенный непосредственно к приемной антенне. Такой способ организации приемника имеет множество недостатков, поэтому чаще всего приемник выполняют по следующей схеме, представленной на рис. 1.

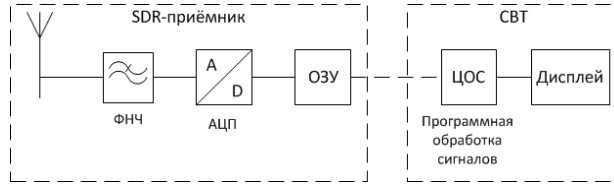

Рис. 1. Схема программно-определяемой радиосистемы: ФНЧ – фильтр низких частот, ОЗУ – оперативное запоминающее устройство, ЦОС – цифровая обработка сигналов, СВТ – средство вычислительной техники

Для сравнения на рис. 2 приведена упрощенная структурная схема супергетеродинного приемника, применяемого при проведении специальных исследований.

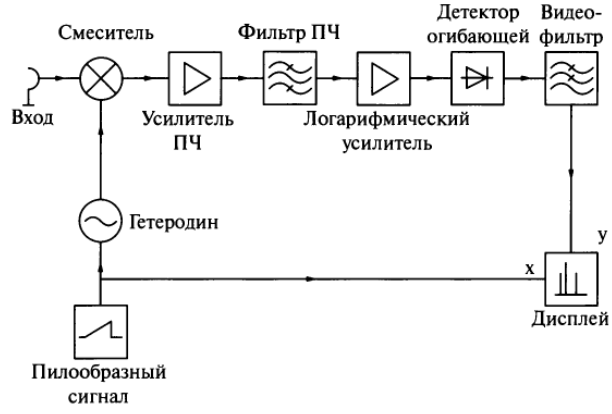

Рис. 2. Схема супергетеродинного приемника

Особенностью супергетеродинного приемника является использование гетеродина для переноса частоты. Данное решение обусловлено сложностью создания перестраиваемого полосового фильтра с допустимыми амплитудно-частотными характеристиками [3]. Приемник, построенный по данной схеме может принимать сигналы в широком частотном диапазоне (на настоящий момент от единиц Гц до ста ГГц с применением внешних смесителей). Разрешение сигналов в таком приемнике осуществляется фильтром промежуточной частоты (ПЧ), построение которого не вызывает затруднений.

Построение приемника по гетеродинной схеме с одной стороны позволяет сделать широкополосное устройство с аналоговыми фильтрами практически достижимой крутизны, реализовать преселектор и предусилитель, однако полоса обзора такого приемника оказывается ограниченной ввиду особенностей операции переноса частоты.

В случае использования схемы, представленной на рис. 1, обработка сигналов осуществляется на СВТ, при этом методы ЦОС позволяют создать фильтр любой требуемой характеристики, в том числе согласованный фильтр и фильтр с прямоугольным окном. Однако, поскольку на вход АЦП поступает широкополосный сигнал, существует вероятность перегрузки входных каскадов в случае наличия мощной помехи на частоте, отличной от частоты исследуемого сигнала. В таком случае восстановление исходного сигнала будет невозможно.

Таким образом, использование SDR-приемника с одной стороны дает возможность использовать методы ЦОС и отложенного анализа, а с другой стороны такой приемник оказывается чувствительным к помеховой обстановке, а его характеристики по уровню шума, согласованию с приемной антенной и точности измерения амплитуды и частоты сигналов оказываются ниже. Кроме ограничений, определяемых аппаратной частью, так же имеются ограничения, связанные с использованием быстрого преобразования Фурье.

Описание используемого SDR-приемника

В качестве измерительного приемника (рис. 3) используется дешевый и доступный RTL-SDR, построенный на основе чипсета RTL2832. Данная микросхема содержит два 8-битных АЦП с частотой дискретизации до 3,2 МГц и интерфейс USB для связи с компьютером. Эта микросхема на входе принимает I- и Q-потоки, источником которых является микросхема R820T. Она реализует радиочастотную часть, а именно буферный усилитель антенны, перестраиваемый широкополосный фильтр и квадратурный демодулятор с синтезатором частоты. Микросхема работает в диапазоне частот 24–1766 МГц. Изначально данный приемник использовался в качестве ТВ-тюнера, однако позже было обнаружено, что его так же можно применять в качестве аппаратной части программно-определяемой радиосистемы.

Рис. 3. Внешний вид приемника

Обзор программного обеспечения для работы с SDR-приемниками

Последнее десятилетие тема применения SDR для приема сигналов активно развивается. Созданы и используются несколько прикладных программ для обработки сигналов. Далее будут рассмотрены некоторые из них.

SDRSharp (рис. 4) – пакет, входящий в программный комплекс AirSpy. В рамках данного комплекса имеются утилиты для приема сигналов GPS, служебной и речевой информации авиадиспетчерских служб, а также для декодирования некоторых открытых протоколов радиосвязи. Так же имеется возможность декодирования открытой служебной информации, передаваемой базовыми станциями сотовой связи. Однако в рамках приема ПЭМИ данные утилиты не представляют интерес.

SDRSharp позволяет регистрировать сигналы, на их основе строить спектр, декодировать некоторые протоколы цифровой связи, демодулировать аналоговые сигналы. Кроме того, в данной утилите реализованы некоторые цифровые фильтры. Данная утилита позволяет просто и быстро начать работу с SDR-приемником, однако не обладает достаточной гибкостью применения. Кроме того, отсутствие возможности выполнения обратного преобразования Фурье не позволяет строить осциллограмму принимаемого сигнала, что затрудняет верификацию принимаемых сигналов. Единственная возможность обнаружить сигнал в данном случае – сравнение спектральной плотности мощности при наличии и отсутствии сигналов ПЭМИ.

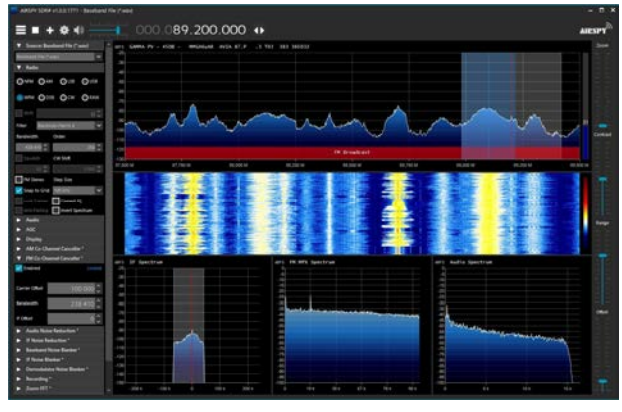

Рис. 4. Внешний вид интерфейса программы SDRSharp

GNURadio (рис.5) - свободно распространяемая среда графической разработки радиоустройств. Она позволяет проводить цифровую обработку сигналов полученных сигналов, при этом программа позволяет изменять характеристики существующих стандартных фильтров, а также создавать свои фильтры с заданной импульсной характеристикой. Данная особенность позволяет создавать оптимальные фильтры на основании априорных знаний об исследуемом сигнале. Кроме фильтрации данный программный продукт позволяет необходимым образом обрабаты-

вать полученный сигнал. Имеется широкий набор демодуляторов, эквалайзеров, аттенюаторов и других модулей для обработки сигналов. Также имеется возможность создания модуля с требуемым алгоритмом обработки сигналов. С этой целью имеется возможность добавления собственной библиотеки. Исполняемый код при этом должен быть написан на языке Python. Данная особенность позволяет автоматизировать процесс регистрации сигналов и реализовать, например, отложенный анализ или восстановление сигналов по нескольким реализациям с использованием их взаимной корреляции.

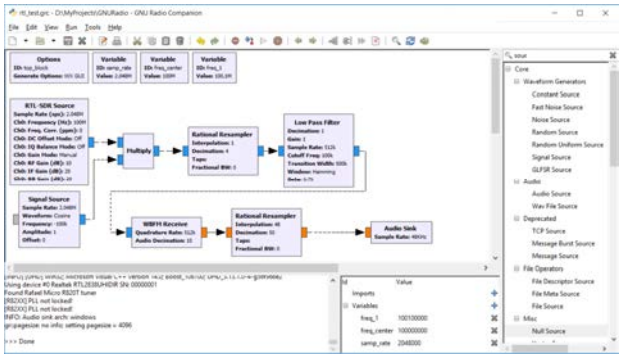

Рис. 5. Внешний вид интерфейса программы GNURadio

Особенности ПЭМИ интерфейсов СВТ

Сигналы ПЭМИ являются побочными, и они не предусмотрены разработчиком на этапе проектирования компонентов СВТ. В свою очередь это приводит к тому, что мощность сигналов ПЭМИ оказывается ниже, чем у сигналов функциональных каналов связи. В отличие от функциональных каналов связи, мощность полезного сигнала распределена в большом частотном диапазоне. Поскольку информативные сигналы СВТ апереодические, а зачастую могут быть даже импульсными, их спектр оказывается бесконечным и не дискретным. В таком случае спектр сигналов ПЭМИ определяется спектральной характеристикой излучающей системы, представленной межблочными кабелями и проводниковыми линиями. Поскольку на этапе разработки задача эффективного излучения сигналов ПЭМИ не ставится. Часто характеристики такой антенны оказываются не согласованными с характеристиками передаваемого сигнала. Таким образом, прием сигналов затруднен, и предварительная оценка ожидаемого спектра сигналов является сложно выполнимой задачей. Поиск сигналов должен осуществляться чувствительной аппаратурой с широким частотным диапазоном и изменяемыми характеристиками фильтров. [4] На рис. 6 представлены спектры сигналов ПЭМИ разных мониторов, полученные Маркусом Куном в его исследованиях [5].

Как видно, спектры сигналов ПЭМИ различаются для различных моделей мониторов, подсоединенных посредством интерфейса VGA значительно различаются даже при одинаковой частоте работы интерфейса.

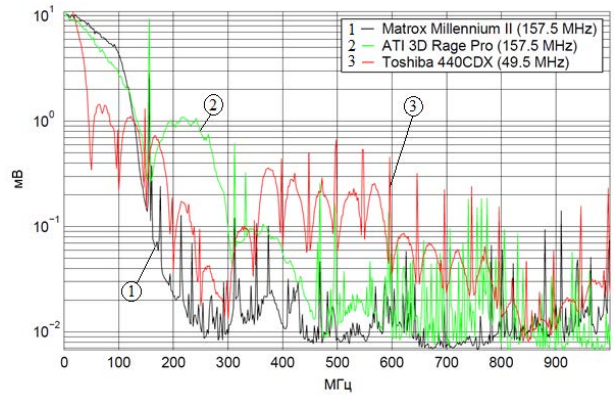

Рис. 6. Сравнение спектров сигналов ПЭМИ различных мониторов

На рис. 7 представлены спектры различных сигналов, а так же спектр сигналов ПЭМИ, полученные в рамках работы [5].

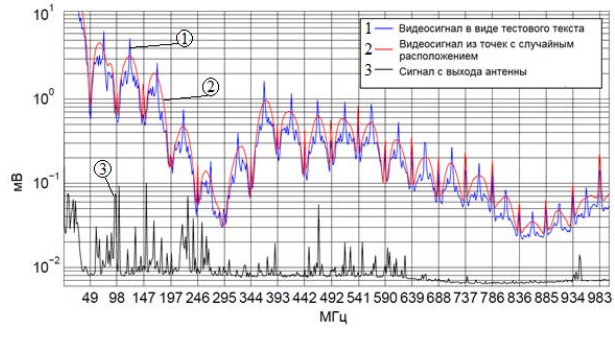

Рис. 7. Сравнение спектров различных сигналов

Как видно из рис. 7, спектр исходного сигнала не совпадает со спектром ПЭМИ. Ранее было сказано, что спектр сигналов ПЭМИ определяется частотной характеристикой излучающей системы. Графики на рис. 7 позволяют оценить величину напряжения на выходе приемной антенны. Данные результаты получены с помощью приемной аппаратуры измерительного приемника, построенного по супергетеродинной схеме, а также с помощью измерительных антенн.

Особенности использования SDR-приемника для регистрации сигналов ПЭМИ

Сигналы ПЭМИ являются широкополосными, а их мощность не велика. Кроме того, зачастую в месте проведения специальных исследований уровень фонового шума оказывается велик. Все это приводит к тому, что измерительная аппаратура должна иметь высокую чувствительность.

В процессе проведения специальных исследований выполняется измерения уровней информативных сигналов. В соответствии с существующей нормативно-методической документацией измерения должны выполняться в соответствии с аттестованной методикой измерений поверенными средствами измерения, включенными в Федеральный информацион-

ный фонд по обеспечению единства измерений (ФИФ). В настоящий момент времени ни один из существующих SDR-приемников не является средством измерений. Для обеспечения возможности их применения для проведения предварительных специальных исследований производители данной аппаратуры должны внести ее в ФИФ. Однако, в рамках данной работы была проведена оценка возможности применения SDR-приемника для приема сигналов ПЭМИ.

Анализ полученных результатов

В рамках данной работы авторы использовали SDR-приемник RTL820T2-SDR для приема сигналов клавиатуры Logitech K120, мыши Logitech M-U0026 и VGA-кабеля, входящих в состав автоматизированного рабочего места. Результаты измерений обрабатывались в программе GNURadio. Результаты исследований показали, что сигнал ПЭМИ не был обнаружен. В то же время, при использовании в качестве измерительной аппаратуры измерительного приемника Rohde&Schwartz ESCI7 и биконической измерительной антенны EMCO3110B данные сигналы были обнаружены. Объект измерений располагался на высоте 1 м над подстилающей поверхностью. Измерения проводились на расстоянии 1 м. Для SDR-приемника измерения проводились также и на расстоянии 10 см. Это объясняется как низкой чувствительностью самого SDR-приемника и уровнем его собственного шума, так и неудовлетворительными характеристиками входящей в комплект антенны. Улучшение характеристик примененного средства измерений возможно за счет применения измерительных антенн, однако это осложняется необходимостью согласования входных каскадов SDR-приемника, антенного кабеля и самой антенны, а также за счет установки разъема для подключения антенны, что выходит за рамки данной работы.

В рамках выполнения работы авторами показано, что использование SDR-приемника для проведения специальных исследований является перспективной задачей, однако требует доработки нормативно-методических документов, улучшения характеристик существующих приемников и включения их в ФИФ.

Список литературы

1. Казаков А. А., Лушкин Д. В., Николаева И. А., Шишков В. Ю. Теоретическая модель распределенной системы средств активной защиты информации / XIV Всероссийская молодежная научно-инновационная школа. Математика и математическое моделирование.// Сборник материалов. Саров, 2020. С. 143–144.

2. Казаков А. А., Ерошев В. И. Исследование вопросов защиты информации от утечки по техническому каналу при использовании средств активной защиты / XIII Всероссийская молодежная научно-инновационная школа. Математика и математическое моделирование // Сборник материалов. Саров, 2019. С. 61-62.

3. Кристоф Раушер. Основы спектрального анализа. М.: Rodhe&Schwarz. Горячая линия-Телеком, 2006. С. 22.

4. Евстифеев А. А., Ерошев В. И., Казаков А. А. Разработка предложений по оценке защищенности информации технических систем от утечки по техническим каналам / XII Всероссийская молодежная научно-инновационная школа. Математика и математическое моделирование. Сборник материалов. Саров, 2018. С. 15–16.

5. Kuhn, Markus G. Compromising emanations: eavesdropping risks of computer displays: Автореф. дис. Ph.D, United Kingdom, Cambridge, 2003.