

На правах рукописи

БЕХТИН МАКСИМ АЛЕКСАНДРОВИЧ

**СИСТЕМА ОБНАРУЖЕНИЯ ПОБОЧНЫХ ИНФОРМАЦИОННЫХ
ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ ТЕХНИЧЕСКИХ СРЕДСТВ**

Специальность 05.12.04 – Радиотехника,
в том числе системы и устройства телевидения

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

Москва – 2009

Работа выполнена на кафедре теоретической радиотехники Московского авиационного института (государственного технического университета) «МАИ».

Научный руководитель: доктор технических наук, профессор
Юрий Владимирович Кузнецов

Официальные оппоненты: доктор технических наук, профессор
Куприянов Александр Ильич

кандидат военных наук, доцент
Набока Юрий Иванович

Ведущая организация: Федеральное государственное унитарное
предприятие «Научно-производственное
предприятие «Гамма»

Защита диссертации состоится «29» декабря 2009 г. в 10⁰⁰ часов на заседании диссертационного совета Д 212.125.03 при Московском авиационном институте (государственном техническом университете) по адресу: 125993, г. Москва, А-80, ГСП-3, Волоколамское шоссе, 4.

С диссертацией можно ознакомиться в библиотеке МАИ.

Автореферат разослан « » _____ 2009 года.

Ученый секретарь
диссертационного совета
Д 212.125.03, к.т.н., с.н.с.



М.И. Сычев

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность проблемы. В процессе функционирования технических средств (ТС) обработки, хранения и передачи информации в конструктивных элементах и кабельных соединениях этих устройств циркулируют электрические токи информативных сигналов. Это приводит к формированию и излучению в окружающее пространство электромагнитных полей, уровни которых могут быть достаточными для их приема на расстоянии от технического средства и извлечения из них информации с помощью специальной аппаратуры. Возможность скрытого от владельца технического средства съема информации, обрабатываемой на устройстве, сложность выявления электромагнитного канала утечки информации обусловили высокий интерес к методам и средствам анализа побочного электромагнитного излучения технических средств обработки, хранения и передачи информации.

Под утечкой информации по каналам побочного электромагнитного излучения понимается возможность доступа к информации, обрабатываемой на технических средствах, осуществляемого путем перехвата и соответствующей обработки побочных электромагнитных излучений технических средств передачи, обработки и хранения информации. Канал утечки информации включает в себя техническое средство, среду распространения электромагнитных волн, систему перехвата и обработки побочных излучений.

Каналы утечки информации могут возникать вследствие излучения информативных сигналов при работе технического средства и наведения этих сигналов в линиях связи, цепях питания и заземления, других коммуникациях. ПЭМИ технических средств может распространяться на большие расстояния и регистрироваться современными измерительными средствами. Частоты информационных составляющих побочных излучений зависят от типа технического средства и видов сигналов, обрабатываемых на нем, и могут перекрывать диапазон частот от сотен герц до нескольких десятков гигагерц.

В настоящее время литература по вопросам обеспечения информационной безопасности практически отсутствует. В большинстве книг, посвященных проблеме информационной безопасности, материалы об электромагнитном канале утечки информации носят обзорный характер. Большинство работ в области исследования побочного электромагнитного излучения техниче-

ских средств проводятся в целях обеспечения государственной безопасности, и вся полученная информация является секретной.

Для обеспечения информационной безопасности технических средств необходимо принимать во внимание электромагнитную обстановку и уровень электромагнитных излучений исследуемых технических средств в широком диапазоне частот. В большинстве случаев мероприятия по снижению уязвимости радиотехнического оборудования опираются на совокупность инженерно-технических исследований (ИТИ), в результате которых должны быть получены обоснованные рекомендации для каждого конкретного технического средства. Целью ИТИ является выявление и количественная оценка степени защищенности технического средства. Наиболее часто на практике применяют критерий оценки защищенности в виде отношения уровня информативного сигнала в канале утечки к уровню нормированной помехи. Т.е. задача ИТИ состоит в определении реального отношения сигнал/шум на выходе приемника ПЭМИ в точке его возможного расположения и сравнении полученного значения с нормой. На практике при оценке защищенности каналов ЭМИ используют не реальное отношение сигнал/шум, а расстояние от технического средства, за пределами которого выполняется условие защищенности.

В настоящее время для проведения исследований ПЭМИ технических средств целесообразно использовать такой комплекс аппаратуры, основу которого составляет измерительный приёмник или анализатор спектра с набором соответствующих измерительных антенн. Измерительные приёмники в наибольшей степени отвечают требованиям, предъявляемым к аппаратуре для исследований ПЭМИ. Они обеспечивают высокую точность измерений при относительно больших временных затратах.

Значительная часть измерительных приёмников позволяет наблюдать панораму исследуемого диапазона частот, анализировать сигналы на выходе детекторов различных типов. Однако цена измерительных приёмников весьма высока. Анализаторы спектра по своим функциональным возможностям вполне сопоставимы с измерительными приёмниками. Более того, на стадии обнаружения ПЭМИ они оказываются удобнее приёмников.

Для защиты технических средств от утечки информации применяются организационные и технические мероприятия. Организационные мероприятия направлены на то, чтобы, не изменяя уровня ПЭМИ исследуемого уст-

ройства или уровня электромагнитных шумов путем изменения расположения ТС добиться уменьшения зоны возможного перехвата информации. К техническим мероприятиям защиты информации относятся меры и средства, воздействующие либо на уровень ПЭМИ, либо на уровень электромагнитных шумов. Например, электромагнитное экранирование является эффективным способом защиты информации.

При проведении ИТИ для обеспечения стационарности излучения технического средства и, как следствие, более уверенного обнаружения информационных составляющих в ПЭМИ ТС, на практике используют такой режим работы устройства, при котором в нем циклически выполняется набор одинаковых операций. Этот режим работы ТС называется тестовым режимом. Например, для отдельных блоков персонального компьютера используются следующие тест-режимы: для монитора используется режим отображения «точка через точку»; для жестких магнитных дисков используется чередование записи и чтения «единиц»; для клавиатуры – нажатая клавиша.

Условия, предъявляемые к качеству измерения ПЭМИ ТС, требуют разработки специальных программно-аппаратных комплексов, использующих, наряду с универсальными измерителями, специализированные устройства для обнаружения, обработки и регистрации информационных составляющих ПЭМИ ТС. Это определяет актуальность задачи разработки новых методов и алгоритмов эффективного анализа электромагнитных излучений в широкой полосе частот, учитывающих характеристики тестовых последовательностей и используемых универсальных измерительных устройств.

В связи со всем выше сказанным задача разработки системы обнаружения побочных информационных электромагнитных излучений технических средств с использованием квадратурной обработки является актуальной.

Целью работы является разработка алгоритма поиска и обнаружения информационных составляющих побочного электромагнитного излучения технических средств с использованием квадратурной обработки и реализация радиотехнической системы обнаружения.

Для достижения поставленной цели в работе решены следующие основные задачи:

1. Синтезирована математическая модель информационных сигналов побочных электромагнитных излучений технических средств.

2. Разработан алгоритм обнаружения информационных составляющих ПЭМИ технических средств на основе квадратурной обработки сигналов, учитывающий параметры и режим работы измерительного оборудования.

3. Разработана математическая модель системы обнаружения информационных составляющих побочного электромагнитного излучения технических средств обработки, хранения и передачи информации.

4. Проведено компьютерное моделирование процесса обнаружения информационных составляющих ПЭМИ ТС с использованием синтезированных моделей системы обнаружения и сигналов технического средства.

5. Проведено стохастическое исследование статистических характеристик и параметров сигналов на выходе системы обнаружения.

6. Разработана и реализована система обнаружения и блок цифровой обработки побочных электромагнитных излучений технических средств.

7. Проведено экспериментальное исследование по обнаружению информационных составляющих ПЭМИ отдельных блоков персонального компьютера.

Методы исследований. Для решения поставленных задач использовался аппарат теории вероятностей, математического анализа, цифрового спектрального анализа и его приложения, методы анализа линейных и нелинейных радиоустройств, методы математического и статистического моделирования, а также теоретические основы статистической радиотехники.

Научная новизна:

1. Обоснована и разработана параметрическая частотно-временная модель системы обнаружения информационных составляющих ПЭМИ технических средств, учитывающая режим работы и параметры измерительного оборудования.

2. Синтезирована модель информационных составляющих электромагнитного излучения технических средств, учитывающая особенности сигналов, обрабатываемых в различных технических средствах хранения, обработки и передачи информации.

3. Предложен алгоритм обнаружения информационных составляющих ПЭМИ технических средств на основе квадратурной обработки сигналов.

4. Проведено стохастическое компьютерное моделирование процессов обнаружения информационных составляющих ПЭМИ технических средств для заданных значений полосы частот и времени наблюдения сигналов.

Практическая значимость результатов работы состоит в том, что на основе предложенного алгоритма разработана и реализована радиотехническая система обнаружения информационных составляющих ПЭМИ технических средств, позволяющая анализировать сигналы в диапазоне частот от единиц мегагерц до десятков гигагерц с полосой анализа от 10 кГц до 750 кГц, временем накопления до десятков секунд и динамическим диапазоном до 110 дБ. Также разработан и реализован блок цифровой обработки с частотой дискретизации 200 МГц, осуществляющий дискретизацию радиосигнала промежуточной частоты, синхронное детектирование, выделение квадратурных составляющих, децимацию, цифровую фильтрацию и передачу накопленных данных в компьютер.

Разработанная система обнаружения и блок цифровой обработки могут быть эффективно применены для решения задач электромагнитной совместимости и обеспечения информационной безопасности технических средств. Используемые в работе методы цифровой обработки могут эффективно использоваться в различных областях современной радиотехники, в том числе в учебном процессе как в традиционных дисциплинах кафедры «Теоретическая радиотехника» МАИ, так и в дисциплинах специализации.

Реализация и внедрение результатов работы. Основные результаты диссертационной работы использованы и внедрены в Федеральном государственном унитарном предприятии «НПП «Гамма». Акт о внедрении приведен в приложении к диссертации.

Научные и практические результаты работы использованы в процессе выполнения научно-исследовательских работ и отражены в отчетах по нескольким хоздоговорным НИР.

Достоверность полученных результатов обуславливается корректностью исходных положений и преобразований, использованием апробированного адекватного математического и статистического аппарата, компьютерных программ и логической обоснованностью выводов. Полученные результаты многократно подтверждены физическими и вычислительными экспериментами.

Апробация результатов работы.

Результаты исследования докладывались и обсуждались на:

Международных научно-технических конференциях: 10-я Международная конференция и выставка «Цифровая обработка сигналов и ее применение», Москва, (2008 г.); Международная молодежная научно-техническая конференция студентов, аспирантов и ученых “Молодежь и современные проблемы радиотехники и телекоммуникаций РТ-2006”, Севастополь (2005 г.); Международной научной конференции ИРЭМВ-2005 «Излучение и рассеяние электромагнитных волн», посвященной 110 годовщине Дня радио, Таганрог, (2005 г.); 8 и 9 ежегодные международные научно-технические конференции студентов и аспирантов “Радиоэлектроника, электротехника и энергетика”, Москва, МЭИ (2002, 2003 гг.).

Международном научно-техническом семинаре: «8-й научный обменный семинар. Радиотехнические устройства СВЧ диапазона», г. Мюнхен: MTU (2004 г.).

Российских научно-технических конференциях: Научно-техническая конференция молодых ученых «Информационные технологии и радиоэлектронные системы», посвященная 80-летию профессора П.А. Бакулева, Москва, МАИ (2008 г.); Научно-техническая конференция молодых ученых факультета «Радиоэлектроника летательных аппаратов», Москва, МАИ (2007 г.); Юбилейная научно-техническая конференция молодых ученых «Информационные технологии и радиоэлектронные системы», Москва, МАИ (2006 г.); Юбилейная научно-техническая конференция «Инновации в радиотехнических информационно-телекоммуникационных технологиях», Москва, МАИ, (2006 г.).

Публикации.

По теме диссертации опубликовано 14 печатных работ, из них 4 научные статьи, 6 докладов на международных конференциях, 4 доклада на российских научных конференциях.

Основные положения, выносимые на защиту:

1. Использование квадратурной обработки в алгоритме обнаружения информационных составляющих ПЭМИ технических средств позволяет уменьшить вероятность пропуска при фиксированных вероятности ложной тревоги и отношении сигнал-шум.

2. Повышение разрешающей способности по частоте и увеличение точности оценки параметров информационных ПЭМИ технических средств обеспечивается за счет учета параметров и характеристик измерительной системы при формировании опорных сигналов в системе цифровой обработки.

3. Расширение полосы частот анализируемых сигналов за счет использования высокочастотного АЦП позволило сократить временные затраты на проведение измерений в несколько раз.

Структура и объем работы.

Диссертационная работа изложена на 144 машинописных страницах и состоит из введения, пяти глав, заключения и списка литературы. Иллюстративный материал представлен в виде 78 рисунков и 8 таблиц. Список литературы включает 79 наименований.

СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обоснована актуальность разработки алгоритма поиска и обнаружения информационных составляющих ПЭМИ технических средств и реализации радиотехнической системы обнаружения, сформулированы цель и задачи исследований, показаны научная новизна и практическая значимость работы, представлена структура диссертации.

В **первой главе** выполнен обзор литературы по материалам отечественных и зарубежных источников в области анализа побочных электромагнитных излучений технических средств обработки, хранения и передачи информации с точки зрения информационной безопасности. В главе рассмотрена модель канала утечки информации, состоящая из источника информационного сигнала, среды распространения сигналов, источников мультипликативных и аддитивных помех, а также аппаратуры перехвата и обработки.

При исследовании технических средств на наличие информационных побочных электромагнитных излучений главными задачами являются обнаружение сигналов, несущих в себе информацию, и оценка их параметров. Наиболее часто измерения проводятся в частотной области с помощью анализаторов спектра. Современные анализаторы спектра позволяют измерять сигналы в частотном диапазоне от единиц килогерц до десятков гигагерц. Кроме того, анализаторы спектра могут применяться для измерений во временной области. В работе рассмотрены особенности алгоритмов проведения

исследований ПЭМИ ТС с использованием современного измерительного оборудования.

В первой главе также предложен алгоритм проведения исследований побочных электромагнитных излучений технических средств, позволяющий повысить точность обнаружения информационных сигналов и уменьшить временные затраты на проведение исследований ТС. На первом этапе алгоритма обнаружения информационных составляющих ПЭМИ технических средств обработки, хранения и передачи информации производится выбор и установка параметров системы измерения: диапазон анализируемых частот, полоса анализа, время анализа и другие. Выбор конкретных значений параметров зависит от типа анализируемого технического средства, типов и характеристик информационных сигналов. Процедура выбора параметров системы измерения подробно рассмотрена в последующих главах диссертации. На следующем этапе алгоритма производится оценка электромагнитной обстановки в месте измерения. Это делается для определения порога в системе обнаружения информационных составляющих ПЭМИ технических средств. На основании выбранного режима работы измерительного оборудования и с учетом известного тестового сигнала, используемого в анализируемом техническом средстве, производится формирование опорного сигнала системы обнаружения. Использование априорной информации о форме и параметрах тестовых сигналов при формировании опорного сигнала приводит к значительному улучшению качества обнаружения информационных составляющих ПЭМИН технических средств.

Далее производится измерение и цифровая обработка электромагнитного излучения технического средства, работающего в тестовом режиме. При этом в предложенном алгоритме используется квадратурная обработка измеренных сигналов. Это стало возможно благодаря разработанному и предложенному в данной диссертационной работе цифровому блоку формирования квадратур, включающему в себя аналого-цифровой преобразователь, сигнальный процессор и систему накопления и передачи данных в компьютер. Использование квадратурной обработки при обнаружении информационных составляющих ПЭМИ технических средств позволяет увеличить точность определения частот, на которых излучаются информативные сигналы, и уменьшить время, необходимое для проведения исследований.

По результатам цифровой обработки регистрируются данные о частотах, на которых были обнаружены информационные составляющие электро-

магнитного излучения технического средства. Полученные данные используются для оценки защищенности технического средства по каналу ПЭМИ.

В заключение главы проведен анализ методов измерения ПЭМИ и рассмотрены возможные пути автоматизации процесса измерения электромагнитных излучений технических средств.

Во **второй главе** решена задача математического описания электромагнитного канала утечки информации. Представлена модель электромагнитного излучения технических средств, модель системы измерения на основе анализатора спектра, работающего по гетеродинному принципу, а также модель блока цифровой обработки измеренного сигнала.

При проведении исследований технического средства его необходимо включить в тестовый режим. В зависимости от физических процессов, протекающих при функционировании отдельных блоков технического средства, функциональное преобразование тестового сигнала можно представить в виде линейных и нелинейных операторов. Линейное преобразование сигнала $s_k(t)$ в k -м блоке ТС описывается его импульсной характеристикой $h_k(t)$

$$\Phi_k(t) = s_k(t) * h_k(t) = \int_{-\infty}^{+\infty} s_k(\tau) \cdot h_k(t - \tau) d\tau, \quad (1)$$

где «*» – оператор линейной свёртки. При безынерционном нелинейном преобразовании тестового сигнала его можно представить с помощью полинома M -й степени

$$\psi_k(t) = a_0 + a_1 s_k(t) + a_2 s_k^2(t) + \dots + a_M s_k^M(t). \quad (2)$$

После подстановки выражения (2) в линейный оператор (1) получим тестовый сигнал, преобразованный нелинейным блоком технического средства. Преобразованный тестовый сигнал может также модулировать одно или несколько гармонических колебаний с частотами f_j , излучаемых генераторами технического средства

$$\xi_k(t) = \sum_j \{ \Phi_k(t) * h_k(t) \} \cdot A_j \cos(2\pi f_j t + \theta_j), \quad (3)$$

где A_j, f_j, θ_j – амплитуда, частота и начальная фаза j -го гармонического сигнала. Выражение (3) является наиболее общим математическим описанием преобразования тестового сигнала в отдельном блоке технического средства. Следует отметить, что, несмотря на сложность преобразований, которые могут происходить с тестовым сигналом в техническом средстве, в нём сохраняется информация об исходной тестовой последовательности. Наличие этой

информации в излучаемом сигнале позволяет впоследствии выделить характерные признаки информационных побочных электромагнитных излучений ТС.

Принимаемое измерительной системой побочное электромагнитное излучение анализируемого технического средства представляет собой аддитивную смесь информационного сигнала технического средства, белого шума и помеховых сигналов

$$e_{\text{пр}}(t) = e_{\text{инф}}(t) + e_{\text{ш}}(t) + e_{\text{п}}(t), \quad (4)$$

где $e_{\text{инф}}(t)$ – информационная составляющая побочного излучения ТС, $e_{\text{ш}}(t)$ – нормальный шум в полосе информационного сигнала, $e_{\text{п}}(t)$ – помеховые сигналы.

Предложенный в диссертационной работе метод обнаружения информативных ПЭМИ технических средств основан на анализе взаимнокорреляционной функции (ВКФ) комплексной огибающей измеренного сигнала и комплексного опорного сигнала. Превышение ВКФ в заданном временном интервале порогового значения означает наличие на анализируемой частоте информационной составляющей ПЭМИ. При сканировании всего частотного диапазона осуществляется поиск и регистрация частот, на которых имеется превышение порогового значения сигнала на выходе коррелятора. Пороговое значение определяется на основе анализа электромагнитной обстановки вблизи исследуемого технического средства при выключенном тестовом режиме. Использование комплексных сигналов при формировании опорного сигнала системы обнаружения позволяет повысить вероятность обнаружения по сравнению с алгоритмом, использующим модуль комплексной огибающей измеренного сигнала.

Рассмотрим основные этапы обработки ПЭМИ ТС. Принятый сигнал побочного электромагнитного излучения технического средства после преобразования в анализаторе спектра и переноса на промежуточную частоту поступает на вход аналого-цифрового преобразователя (АЦП). АЦП обеспечивает дискретизацию и квантование сигнала промежуточной частоты. Параметры АЦП выбираются исходя из максимальной частоты сигнала на выходе блока промежуточной частоты измерительного прибора и динамического диапазона полезного сигнала. С выхода АЦП дискретный сигнал $s_N[n]$ поступает на вход блока формирования квадратур, структурная схема, которого показана на рис. 1.

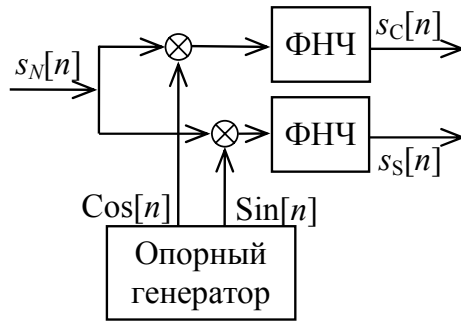


Рис. 1. Структурная схема блока формирования квадратур.

Квадратурные составляющие получаются путем перемножения дискретного сигнала $s_N[n]$ с сигналами опорных генераторов, представляющих собой гармонические колебания на промежуточной частоте $F_{ПЧ}$, сдвинутые по фазе на $\pi/2$ друг относительно друга, и пропускания через фильтры низких частот

$$s_C[n] = (s_N[n] \cdot \cos(2\pi F_{ПЧ} n T_d)) * h_{ФНЧ}[n], \quad (5)$$

$$s_S[n] = (s_N[n] \cdot \sin(2\pi F_{ПЧ} n T_d)) * h_{ФНЧ}[n], \quad (6)$$

где $h_{ФНЧ}[n]$ – импульсная характеристика ФНЧ, T_d – период дискретизации. Комплексная огибающая измеренного сигнала $\dot{s}[n]$ формируется из квадратурных компонент следующим образом:

$$\dot{s}[n] = s_C[n] + j s_S[n], \quad n = 1, \dots, N, \quad (7)$$

где $s_C[n]$, $s_S[n]$ – квадратурные составляющие комплексной огибающей измеренного сигнала, N – количество отсчетов измеренного сигнала.

Комплексная огибающая измеренного сигнала $\dot{s}[n]$ поступает на вход блока цифровой обработки. В диссертации рассмотрены два блока цифровой обработки: амплитудный и квадратурный. В амплитудном блоке, структурная схема которого показана на рис. 2, осуществляется обработка модуля комплексной огибающей анализируемого сигнала, полученного на выходе амплитудного детектора (АД).

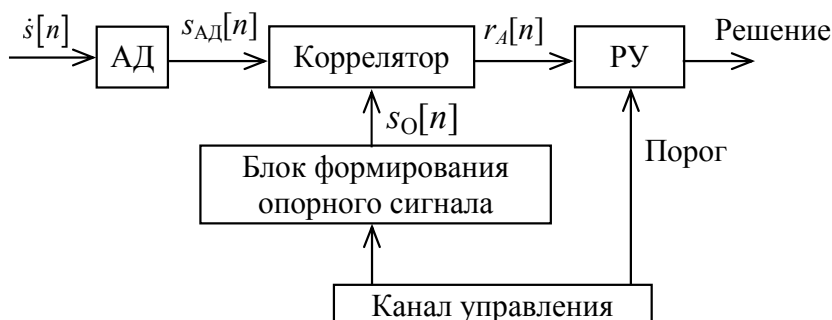


Рис. 2. Амплитудный блок обработки и принятия решения.

Сигнал на выходе детектора определяется по формуле

$$s_{\text{Ад}}[n] = |\dot{s}[n]| = \sqrt{s_C^2[n] + s_S^2[n]}. \quad (8)$$

С выхода детектора действительный сигнал поступает на вход коррелятора, на другой вход которого подается действительный опорный сигнал $s_o[n]$. Взаимно-корреляционная функция двух сигналов определяется по формуле:

$$r_A[n] = \frac{1}{N} \sum_{m=0}^{N-1} s_{\text{Ад}}[m] \cdot s_o[n-m], \quad (9)$$

где $s_{\text{Ад}}[n]$ – сигнал на выходе амплитудного детектора, $s_o[n]$ – опорный сигнал. На выходе коррелятора оценивается максимальное значение корреляционной функции в интервале времени, соответствующему одному периоду опорного сигнала. В решающем устройстве найденное значение максимума сравнивается с порогом и принимается решение о наличии, либо отсутствии информационной составляющей в измеренном сигнале.

Структурная схема предложенного квадратурного блока цифровой обработки показана на рис. 3.

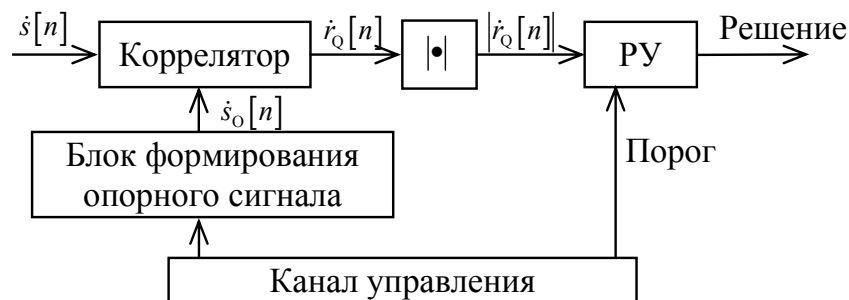


Рис. 3. Квадратурный блок обработки и принятия решения.

В квадратурном блоке комплексная огибающая сигнала $\dot{s}[n]$ поступает непосредственно на вход коррелятора, на второй вход которого подается комплексный опорный сигнал. Взаимно-корреляционная функция двух комплексных сигналов находится как

$$\dot{r}_Q[n] = \frac{1}{N} \sum_{m=0}^{N-1} \dot{s}[m] \dot{s}_o[n-m], \quad (10)$$

где $\dot{s}[n]$ – комплексная огибающая измеренного сигнала, $\dot{s}_o[n]$ – комплексная огибающая опорного сигнала.

В заключение рассмотрена статистическая теория принятия решения о наличии информационных сигналов в измеренном ПЭМИ технического средства.

В третьей главе рассмотрены характерные особенности сигналов технических средств обработки, хранения и передачи информации. На примере излучения от отдельных компонент персонального компьютера показана возможность выделения информационных ПЭМИ технических средств. Произведен синтез компьютерной модели побочного электромагнитного излучения ТС и математической модели обработки измеренного сигнала в системе обнаружения информационных составляющих ПЭМИ технических средств.

Синтезированная компьютерная модель системы обнаружения ПЭМИ ТС учитывает следующие параметры измерительного прибора:

- диапазон перестройки частот;
- полоса пропускания фильтра промежуточной частоты;
- время анализа.

Также в модели имеется возможность управлять частотами и уровнем излучения информационной составляющей ПЭМИ ТС, уровнем помех с амплитудной и частотной модуляцией, а также параметрами белого гауссовского шума. Результаты статистического моделирования для 1000 независимых реализаций модели ПЭМИ ТС с шумом для $\Delta F_{ПЧ} = 100$ кГц и отношения сигнал/шум $Q_{Ш} = 15$ дБ для амплитудного и квадратурного каналов показаны на рис. 4.

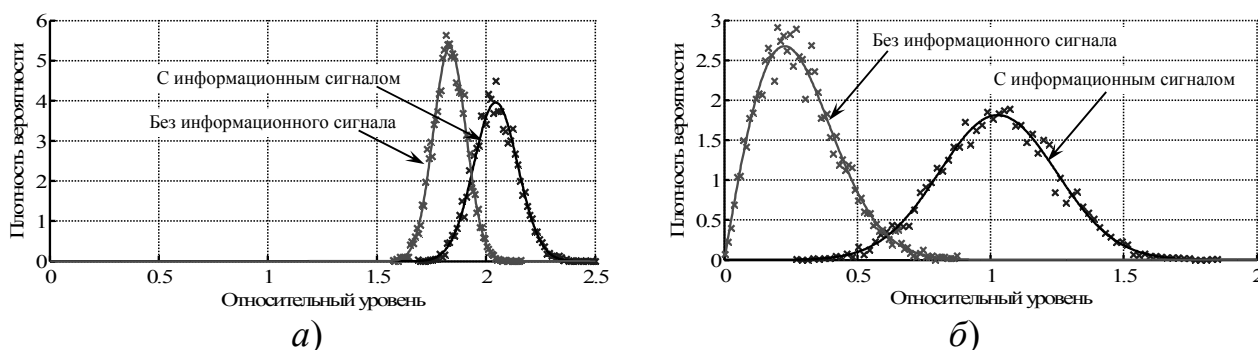


Рис. 4. Гистограммы сигналов на выходе коррелятора амплитудного (а) и квадратурного (б) каналов. $\Delta F_{ПЧ} = 100$ кГц, $Q_{Ш} = 15$ дБ,

“x” – результаты моделирования.

Из рисунков видно, что сигналы на выходе коррелятора амплитудного канала распределены по гауссовскому закону, а в квадратурном канале – по закону Райса. Эксперименты показали, что при увеличении уровня шума математическое ожидание сигналов на выходе коррелятора амплитудного канала увеличивается вместе с увеличением дисперсии случайных величин. В то

же время в сигналах на выходе коррелятора квадратурного канала при увеличении уровня шума дисперсия сигналов растет, а математическое ожидание сигнала с информационной составляющей не изменяется. Результаты компьютерного моделирования показали, что увеличение полосы пропускания фильтра промежуточной частоты анализатора спектра приводит к уменьшению дисперсии случайных величин на выходе коррелятора, а, следовательно, к увеличению вероятности правильного обнаружения и уменьшению вероятности ложной тревоги при фиксированном отношении сигнал/шум.

По результатам статистического моделирования были получены зависимости вероятности правильного обнаружения от вероятности ложной тревоги (рабочие характеристики приемника). Рабочие характеристики приемника для амплитудного и квадратурного каналов для разных значений отношения сигнал/шум для $\Delta F_{ПЧ} = 100$ кГц показаны на рис. 5.

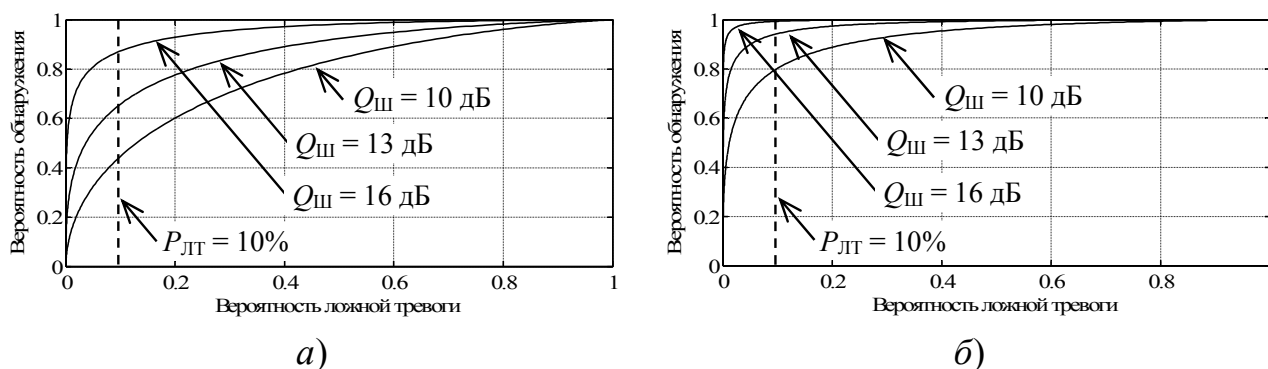


Рис. 5. Рабочие характеристики амплитудного (а) и квадратурного (б) каналов.

По рисункам видно, что для заданного отношения сигнал/шум и фиксированной вероятности ложной тревоги для квадратурного канала вероятность пропуска информационной составляющей ПЭМИ ТС в 2-3 раза меньше чем для амплитудного канала. Аналогично можно показать, что для заданных вероятностей правильного обнаружения и ложной тревоги отношение сигнал шум для квадратурного канала будет ниже. Например, для вероятности правильного обнаружения $P_D = 99\%$ и вероятности ложной тревоги $P_{FA} = 10\%$ выигрыш квадратурного канала в отношении сигнал/шум составляет 6 дБ.

Проведенное моделирование системы обнаружения показало, что использование предложенного алгоритма обнаружения информационных составляющих ПЭМИ ТС позволяет повысить вероятность правильного обнаружения.

ружения, уменьшить пороговое значение отношения сигнал/шум, а также увеличить точность определения частот информационных сигналов.

В четвертой главе представлены результаты экспериментальных исследований побочных электромагнитных излучений технических средств на примере излучения от накопителя на жестких магнитных дисках персонального компьютера. Представлены основные сведения о накопителях на жестких магнитных дисках. Показана структурная схема измерительной установки, использованной для обнаружения побочных электромагнитных излучений технических средств.

Экспериментальные исследования по обнаружению информационных составляющих ПЭМИ технических средств проводились на базе измерительной лаборатории Федерального государственного унитарного предприятия «Научно-производственное предприятие «Гамма». Схема экспериментального стенда показана на рис. 6.



Рис. 6. Схема экспериментального стенда проведения измерений ПЭМИ технических средств

При проведении исследований использовалось следующее контрольно-измерительное оборудование:

- антенна дипольная активная Пб-51, рабочий диапазон частот 9 кГц – 300 МГц;
- анализатор спектра Agilent E4407B;
- модуль аналого-цифрового преобразования;
- персональный компьютер.

Антенна дипольная активная Пб-51 предназначена для измерения электрической составляющей напряжённости электромагнитного поля. Антенны такого типа используются при решении задач электромагнитной совместимости технических средств, а также для определения и контроля предельно допустимых уровней электромагнитных полей технических средств.

Широкополосный анализатор спектра Agilent E4407B представляет собой современный высокотехнологичный прибор, обладающий широкими возможностями измерения спектра сигналов. Для получения анализируемых сигналов большой длительности прибор оснащен опциональной платой выхода промежуточной частоты.

Для получения цифрового сигнала с выхода промежуточной частоты анализатора спектра сигнал подавался на специально разработанный цифровой блок формирования квадратур. Использование этого модуля позволило получать и обрабатывать на компьютере комплексную огибающую принимаемого сигнала. Для управления параметрами работы приборов, накопления измеренных данных и их последующей обработки используется персональный компьютер.

Также в четвертой главе приведены результаты экспериментальных исследований ПЭМИ ТС для разных режимов работы системы обнаружения. Сигналы на выходе корреляторов амплитудного и квадратурного каналов для частоты настройки 17 МГц, диапазона анализируемых частот $\Delta F = 30$ МГц и полосы пропускания ФПЧ $\Delta F_{\text{ПЧ}} = 100$ кГц показаны на рис. 7.

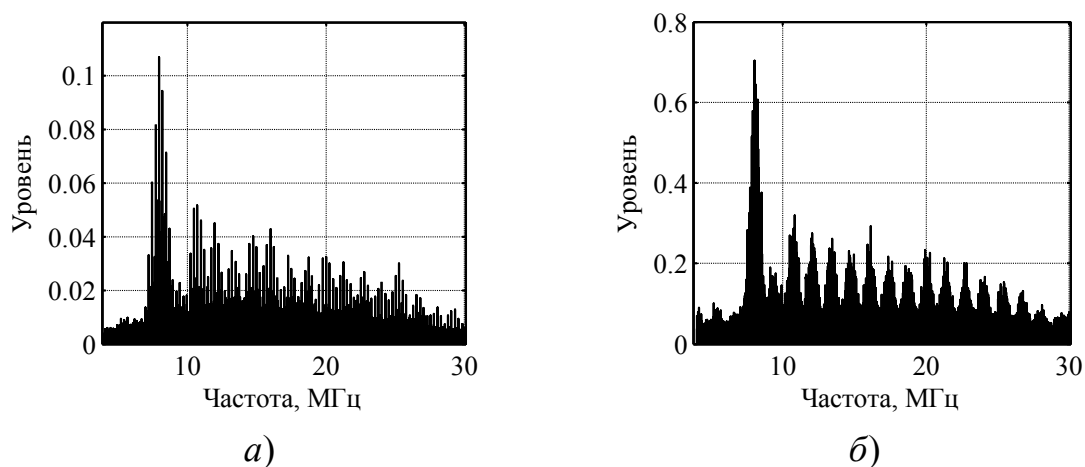


Рис. 7. ВКФ измеренного ПЭМИ ТС с опорным сигналом для амплитудного (а) и квадратурного каналов (б).

$$F = 17 \text{ МГц}, \Delta F = 30 \text{ МГц}, \Delta F_{\text{ПЧ}} = 100 \text{ кГц}.$$

Из рисунков видно, что информационные составляющие ПЭМИ жесткого диска повторяются с частотой, кратной частоте $F_1 = 1,32$ МГц. При этом из-за близкого расположения друг к другу частот информативного сигнала жесткого диска и широкой полосы пропускания фильтра промежуточной частоты на выходе коррелятора амплитудного канала произошло наложение соседних лепестков взаимнокорреляционной функции. Это привело к невозможности оценить

точные значения частот информационных составляющих ПЭМИ ТС. При этом на выходе коррелятора квадратурного канала структура сигнала сохранилась, и определить информативные частоты не составляет труда.

В пятой главе решена задача разработки и реализации измерительного комплекса для обнаружения информационных составляющих ПЭМИ технических средств. Проведен обзор современных измерительных комплексов на основе сканирующих приемников, селективных микровольтметров и анализаторов спектра. Показано, что представленные на отечественном рынке комплексы для проведения исследований ПЭМИ радиотехнических устройств позволяют в ручном или автоматическом режимах решать задачи анализа излучений и наводок технических средств обработки, хранения и передачи информации. Измерительные комплексы классифицируются по принципу построения и функциональным возможностям.

Простейшим устройством, позволяющим проводить измерения и поиск информативных излучений ТС является индикатор электромагнитных излучений. Такой индикатор состоит из слабонаправленной антенны, широкополосного усилителя, амплитудного детектора и порогового устройства. Прибор регистрирует интегральный уровень электромагнитных излучений в месте приема. Другой класс измерительных устройств – сканирующие приемники. Выделяют три основных режима работы сканирующих приемников: автоматическое сканирование в диапазоне частот; автоматическое сканирование на заданных частотах; сканирование в ручном режиме.

Другую группу измерительных приборов, используемых для поиска информативных излучений ТС, представляют анализаторы спектра, рабочий диапазон которых достигает десятков гигагерц. Основное достоинство анализаторов спектра заключается в возможности наблюдения за изменениями панорамы радиосигнала в выбранном частотном диапазоне и регистрации его основных параметров. Крупнейшими производителями профессиональных анализаторов спектра являются фирмы Agilent и Rohde&Schwarz.

В главе представлен разработанный и изготовленный блок формирования квадратур, включающий в себя аналого-цифровой преобразователь, сигнальный процессор и систему накопления и передачи данных в компьютер. Предложена структура измерительного комплекса, позволяющего реализовать разработанный алгоритм обнаружения информационных составляющих

побочных электромагнитных излучений технических средств на основе квадратурной обработки измеренных сигналов.

Для реализации системы обнаружения информационных составляющих ПЭМИ технических средств в рамках создания цифрового блока формирования квадратур был разработан, изготовлен и отлажен модуль аналого-цифрового преобразования. Основные характеристики цифрового блока формирования квадратур приведены в табл. 1.

Таблица 1

Технические характеристики цифрового блока формирования квадратур

Наименование параметра	Значение
Разрядность АЦП	12 бит
Частота дискретизации АЦП	200 МГц
Коэффициент децимации	128
Результирующая частота дискретизации	1,5625 МГц
Разрядность сигналов квадратур	16 бит
Несущая частота анализируемого сигнала	21,4 МГц

В системе обнаружения информационных составляющих побочных электромагнитных излучений технических средств предложено использовать модуль цифрового преобразования (МЦП) радиосигнала промежуточной частоты. Использование этого модуля позволит выполнять обработку комплексной огибающей принимаемого сигнала и осуществлять амплитудное и частотное детектирование непосредственно на управляющем компьютере. Основные функции и задачи МЦП следующие:

1. Аналого-цифровое преобразование сигнала с выхода промежуточной частоты анализатора спектра.

2. Предварительная цифровая обработка данных, полученных с АЦП:

- формирование сигналов квадратур;
- цифровая фильтрация сигналов в квадратурных каналах;
- децимация выходных потоков данных.

3. Передача данных на управляющий компьютер.

В заключение главы предложены пути автоматизации процесса обнаружения информационных составляющих побочных электромагнитных излучений технических средств.

Заключение

Диссертационная работа посвящена разработке алгоритма поиска и обнаружения информационных составляющих побочного электромагнитного излучения технических средств с использованием квадратурной обработки и реализации радиотехнической системы обнаружения. Разработанная система обнаружения и блок цифровой обработки могут быть эффективно применены для решения задач обеспечения информационной безопасности технических средств обработки, хранения и передачи информации.

Проведенный обзор по материалам отечественных и зарубежных источников в области анализа побочных электромагнитных излучений технических средств (ТС) обработки, хранения и передачи информации с точки зрения информационной безопасности показал, что выбранное направление исследований является востребованным, актуальным и перспективным.

По результатам исследований, проведенных в рамках данной диссертации, получены следующие основные результаты и сделаны следующие выводы.

1. Разработана модель формирования информационных составляющих электромагнитного излучения технических средств, учитывающая особенности сигналов, обрабатываемых в различных технических средствах обработки, хранения и передачи информации.

2. Разработана частотно-временная модель системы обнаружения информационных составляющих побочного электромагнитного излучения технических средств обработки, хранения и передачи информации, учитывающая режим работы измерительного оборудования.

3. Проведено стохастическое компьютерное моделирование процессов обнаружения информационных составляющих ПЭМИ технических средств для заданных значений полосы частот и времени наблюдения сигнала, позволившее оценить технические характеристики измерительного комплекса в разных режимах работы.

4. Разработан алгоритм обнаружения информационных составляющих ПЭМИ технических средств обработки, хранения и передачи информации, позволяющий уменьшить вероятность пропуска более чем в два раза при вероятности ложной тревоги 10 % для заданного отношения сигнал/шум по сравнению с известными алгоритмами за счет использования комплексной

огибающей измеренного сигнала и учета характеристик измерительной системы.

5. Разработан и реализован модуль аналого-цифрового преобразования с частотой дискретизации 200 МГц, осуществляющий дискретизацию радиосигнала промежуточной частоты, синхронное детектирование, выделение квадратурных составляющих, децимацию, цифровую фильтрацию и передачу обработанных данных на компьютер по шине USB 2.0. Разработанный интерфейс связи АЦП с компьютером позволяет при необходимости гибко управлять параметрами и режимами работы модуля АЦП: коэффициентом децимации, полосой сигнала, объемом накапливаемых данных, – в широких пределах.

6. Разработан и реализован измерительный комплекс для обнаружения информационных составляющих ПЭМИ технических средств, содержащий антенную систему, анализатор спектра, АЦП с блоком цифровой обработки и персональный компьютер, обеспечивающий возможность автоматизации проведения измерений излучений технических средств, динамичное управление параметрами и режимами работы измерительного комплекса и возможность проведения измерений в условиях реальной электромагнитной обстановки. Разработанный измерительный комплекс позволяет анализировать ПЭМИ ТС в диапазоне частот от единиц мегагерц до десятков гигагерц с полосой анализируемых сигналов от 10 кГц до 750 кГц, временем накопления от единиц миллисекунд до десятков секунд и динамическим диапазоном до 110 дБ.

7. Проведены экспериментальные исследования по обнаружению информационных составляющих ПЭМИ технических средств, показавшие адекватность разработанных моделей сигналов ПЭМИ и измерительной системы и подтвердившие работоспособность разработанного алгоритма обнаружения и измерительной системы в целом.

Публикации по теме диссертации:

1. Бехтин М.А., Кузнецов Ю.В., Баев А.Б., Сергеев А.А., «Развитие методов анализа электромагнитных излучений в широкой полосе частот», «Успехи современной радиоэлектроники», № 1-2, стр. 132-139, 2009 г.

2. Бехтин М.А., Кузнецов Ю.В., Баев А.Б., Сергеев А.А., «Корреляци-

онный метод обнаружения информационных составляющих побочных электромагнитных излучений технических средств», «Технологии ЭМС», № 2, стр. 3-12, 2009 г.

3. Бехтин М.А., Кузнецов Ю.В., Баев А.Б., Сергеев А.А., Непараметрические методы анализа широкополосных электромагнитных излучений. 10-я Международная конференция и выставка «Цифровая обработка сигналов и ее применение», Москва, с. 370-374, март 2008 г.

4. Бехтин М.А., Кузнецов Ю.В., Баев А.Б., Применение многоуровневого аналого-цифрового преобразования при измерении широкополосных электромагнитных излучений во временной области. Радиотехника, № 8, с. 50-58, 2006 г.

5. Бехтин М.А., Кузнецов Ю.В., Методы проведения измерений широкополосных излучений при решении задачи электромагнитной совместимости. Научно-техническая конференция молодых ученых «Информационные технологии и радиоэлектронные системы», посвященная 80-летию профессора П.А. Бакулева, Москва, МАИ, апрель 2008 г.

6. Бехтин М.А., Кузнецов Ю.В., Система измерения электромагнитного излучения технических средств. Научно-техническая конференция молодых ученых факультета «Радиоэлектроники летательных аппаратов», Москва, МАИ, с. 149-154, апрель 2007 г.

7. Бехтин М.А., Баев А.Б., Кузнецов Ю.В., Ноздрин В.В., Анализ временных и частотных методов измерения электромагнитных излучений в сверхширокой полосе частот, Юбилейная научно-техническая конференция молодых ученых «Информационные технологии и радиоэлектронные системы», Москва, МАИ, май 2006 г.

8. Бехтин М.А., Баев А.Б., Кузнецов Ю.В., Ноздрин В.В., Программно-аппаратный комплекс измерения ЭМИ в сверхширокой полосе частот во временной области, Юбилейная научно-техническая конференция «Инновации в радиотехнических информационно-телекоммуникационных технологиях», Москва, МАИ, октябрь 2006 г.

9. Бехтин М.А., «Использование вейвлет-преобразования при обработке радиолокационных сигналов», Международная молодежная научно-техническая конференция студентов, аспирантов и ученых “Молодежь и современные проблемы радиотехники и телекоммуникаций РТ-2006”, Севастополь, апрель 2005 г.

10. Бехтин М.А., Кузнецов Ю.В., Баев А.Б., Шевгунов Т.Я., «Представление широкополосных СВЧ структур с использованием передаточных функций», Международной научной конференции ИРЭМВ-2005 «Излучение и рассеяние электромагнитных волн», посвященной 110 годовщине Дня радио, Таганрог, июнь 2005.

11. Бехтин М.А., Кузнецов Ю.В., Баев А.Б., Шевгунов Т.Я., «Перспективные методы измерения и алгоритмы анализа побочных электромагнитных излучений», Международной научной конференции ИРЭМВ-2005 «Излучение и рассеяние электромагнитных волн», посвященной 110 годовщине Дня радио, Таганрог, июнь 2005.

12. Бехтин М.А., Баев А.Б., Кузнецов Ю.В., «Использование непрерывного вейвлет-преобразования при обработке сигналов в подповерхностной радиолокации», Будущее авиации и космонавтики, 2004 г.

13. Бехтин М.А., Пехтерев Е.В., «Многоскоростная обработка сверхширокополосных радиолокационных сигналов, 9-я ежегодная международная научно-техническая конференция студентов и аспирантов “Радиоэлектроника, электротехника и энергетика”, Москва, МЭИ, 2003 г.

14. Баев А.Б., Бехтин М.А., Пехтерев Е.В., Сравнительный анализ классических методов спектрального анализа, 8-я ежегодная международная научно-техническая конференция студентов и аспирантов “Радиоэлектроника, электротехника и энергетика”, Москва, стр. 5, февраль 2002 г.