МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

**Национальный исследовательский
Нижегородский государственный университет им. Н.И. Лобачевского**

**Р.А. Васильев
Л.Ю. Ротков**

# ОБНАРУЖЕНИЕ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ И НАВОДОК С ПОМОЩЬЮ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА «ЛЕГЕНДА»

***Учебно-методическое пособие***

Рекомендовано методической комиссией радиофизического факультета
для студентов ННГУ, обучающихся по специальностям 10.05.02
«Информационная безопасность телекоммуникационных систем»
и слушателей курсов послевузовского краткосрочного повышения
квалификации специалистов по информационной безопасности

Нижний Новгород
2018

УДК 004.056.53
ББК 32.81
В19

Васильев Р.А., Ротков Л.Ю. Обнаружение побочных электромагнитных излучений и наводок с помощью программно-аппаратного комплекса «Легенда»: Учебно-методическое пособие. – Нижний Новгород: Нижегородский госуниверситет, 2018. – 45 с.

Рецензент: начальник 1 отдела Нижегородского государственного университета им. Н.И. Лобачевского, к.т.н., доцент **Казачков А.П.**

Методическая разработка содержит описание к лабораторной работе «Обнаружение побочных электромагнитных излучений и наводок с помощью программно-аппаратного комплекса «Легенда».

Лабораторная работа предназначена для изучения программно-аппаратных комплексов для обнаружения побочных электромагнитных излучений и наводок (ПЭМИН) на примере программно-аппаратного комплекса (ПАК) «Легенда». В описании приведены общие принципы проведения поиска и измерения ПЭМИН по электрической составляющей и расчет параметров защищенности технических средств (ТС) от утечки информации. Дан обзор архитектуры комплекса семейства «Легенда». В работе изучаются основные защитные функции комплекса, его возможности, особенности применения.

Пособие предназначено для студентов, обучающихся по специальностям 10.05.02 «Информационная безопасность телекоммуникационных систем» и слушателей курсов послевузовского краткосрочного повышения квалификации специалистов по информационной безопасности.

Ответственный за выпуск:
зам. председателя методической комиссии радиофизического факультета ННГУ,
д.ф.-м.н., профессор **Е.З. Грибова**



УДК 004.056.53
ББК 32.81

# СОДЕРЖАНИЕ

# ВВЕДЕНИЕ

Одной из наиболее вероятных угроз перехвата информации в системах обработки данных считается утечка за счет перехвата побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами. ПЭМИН существуют в диапазоне частот от единиц Гц до полутора ГГц и способны переносить (распространять) сообщения, обрабатываемые в автоматизированных системах. Дальность распространения ПЭМИН исчисляется десятками, сотнями, а иногда и тысячами метров. Наиболее опасными источниками ПЭМИН являются дисплеи, проводные линии связи, накопители на магнитных дисках и буквопечатающие аппараты последовательного типа.

Например, с дисплеев можно снять информацию с помощью специальной аппаратуры на расстоянии до 500-1500 метров, с принтеров до 100-150 метров. Перехват ПЭМИН может осуществляться и с помощью портативной аппаратуры.

Защита информации, обрабатываемой техническими средствами, осуществляется с применением пассивных и активных методов и средств, а также организационными мероприятиями. В данной курсовой работе рассматриваются активные методы и организационные мероприятия защиты информации от утечки по каналам ПЭМИН.

# 1. ПРИРОДА ВОЗНИКНОВЕНИЯ ПЭМИН. КЛАССИФИКАЦИЯ КУИ

## 1.1. Природа возникновения ПЭМИН

Физическую основу случайных опасных сигналов, возникающих во время работы в выделенном помещении радиосредств и электрических приборов, составляют побочные электромагнитные излучения и наводки (ПЭМИН).

Рассмотрим некоторые простейшие теоретические основы, без понимания которых невозможно представить себе, что именно, какие побочные излучения следует ожидать от некого обобщённого сигнала в цепях средств вычислительной техники (СВТ).

Напомним, что изначальная постановка задачи «от лица» потенциального противника состоит в том, что он должен решать простейшую бинарную задачу – что передавалось в данный момент, «ноль» или «единица». То есть задача решается для одного двоичного разряда. При этом предполагается, что потенциальный противник точно знает структуру устройства, алгоритм обработки информации, вид кодировки и т.д.

Исходя из этого, и будем рассматривать модель сигнала и её предполагаемый спектр.

На рис. 1 слева приведён простейший одиночный импульсный сигнал, так называемая «дельта – функция». Такой сигнал характеризуется бесконечно малой длительностью и единичной амплитудой, а площадь такого импульса всегда равен 1. Спектр такого сигнала приведён на том же рисунке справа. То есть спектр такого сигнала сплошной, (без учета свойств случайных антенн в ТС) бесконечный по частоте и его огибающая плоская.

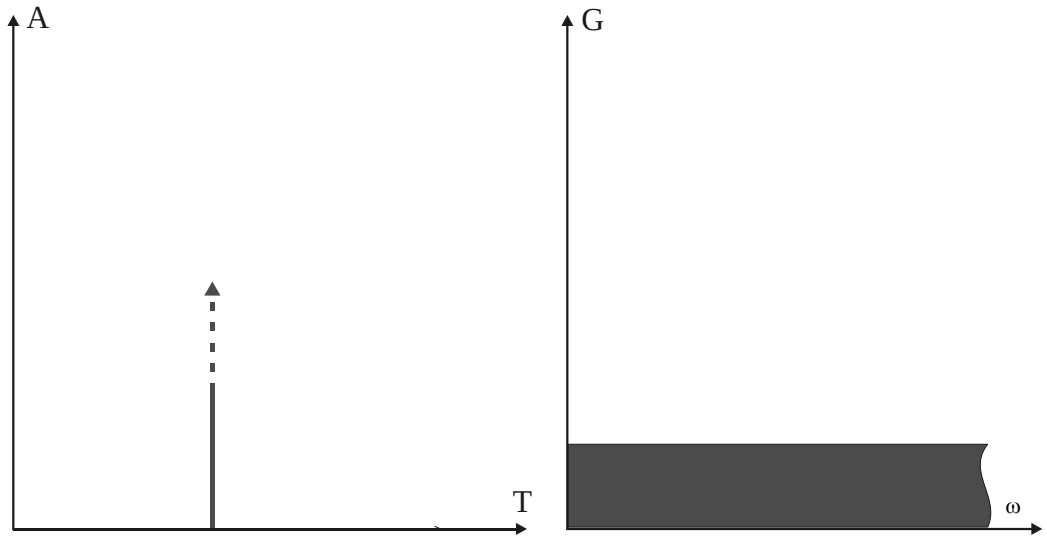


Рис. 1. Дельта – функция и её спектр

Однако в реальности таких импульсов не бывает. Приблизим модель к реальности и рассмотрим одиночный импульс конечной длительности (рис. 2).

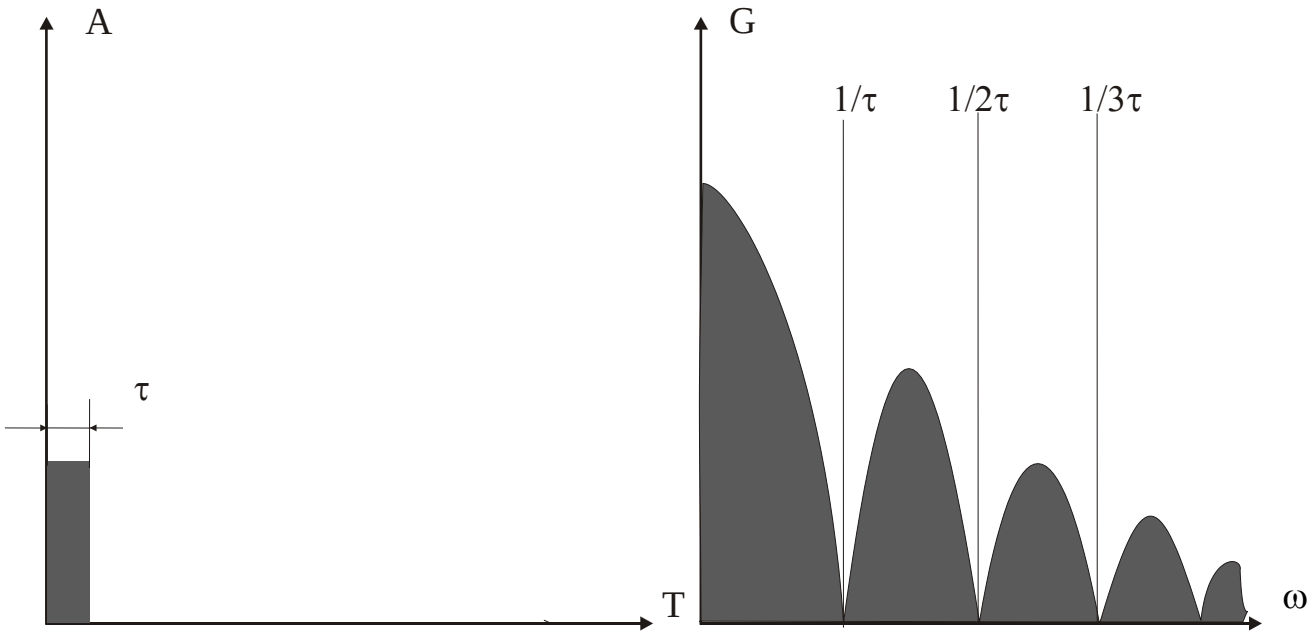


Рис. 2. Однократный импульс конечной длительности и его спектр

Как видим, огибающая спектра стала неравномерной. На рисунке огибающая представлена по абсолютной величине, в реальности каждый чётный лепесток направлен во второй квадрант [1]. Такого рода огибающая спектра описывается простым выражением:

$$G= U*\tau_и \sin(x)/x \qquad (1)$$

Где $\tau_и$ - длительность информационного импульса тест-сигнала, G - амплитуда тест-сигнала, U - пиковое значение опасного сигнала.

Сделаем следующий шаг в приближении модели к реальным сигналам. Рассмотрим бесконечную последовательность импульсов конечной длительности. Такой сигнал и его спектр приведены на рис. 3.

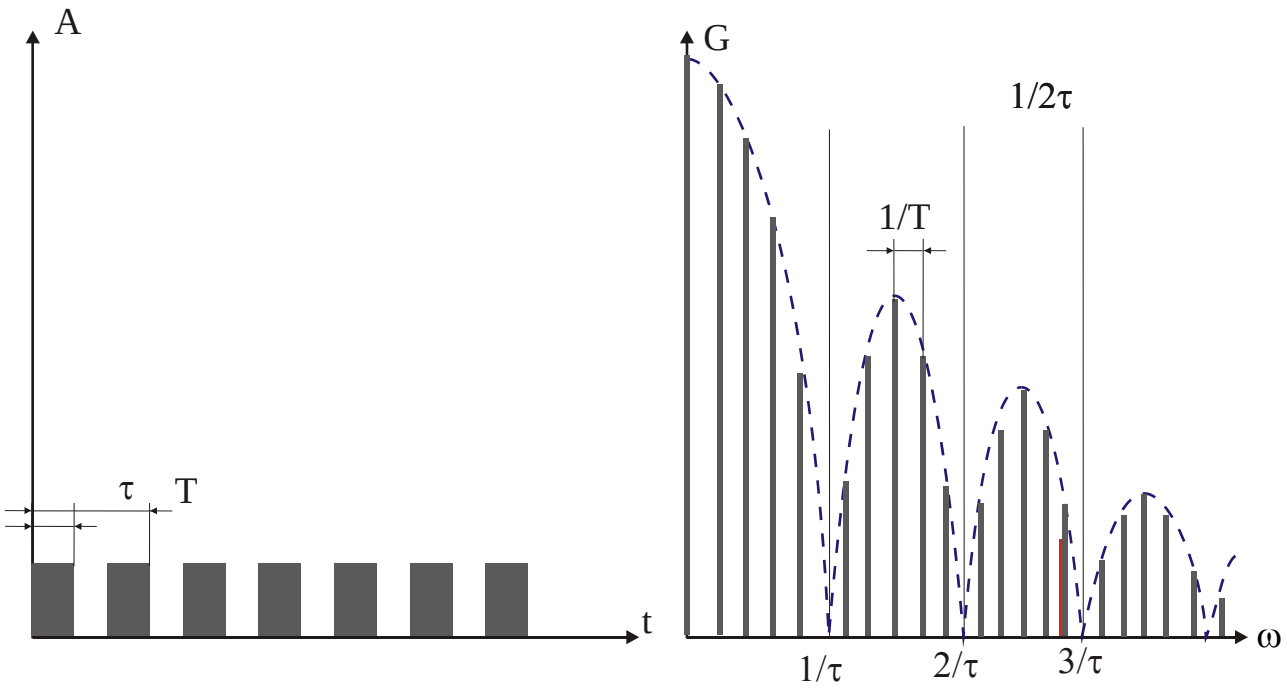


Рис. 3. Спектр бесконечной последовательности импульсов

Следует обратить внимание, что амплитуда импульсов меньше, чем одиночного импульса на предыдущем рисунке, а амплитуды гармонических составляющий спектра даже выросли. Это не случайное нарушение масштаба. Это, разумеется, только качественно, отражение реальности. Это свойство спектра импульсной последовательности лежит в основе существующих методов СИ [1].

$$|E_n| = 2A\sin(n\omega\tau_и/2)\ /\pi n \qquad (2)$$

Где $\tau_и$ - длительность информационного импульса тест-сигнала, n - число обнаруженных опасных сигналов, ω – частота обнаруженного тест-сигнала, $E_n$ - измеренные пиковые значения опасного сигнала.

Таким образом, спектр последовательности импульсов становится «линейчатым», сохраняя огибающую одиночного импульса («лепестки» огибающей, по-прежнему, имеют «ширину» 1/τ). Причём «шаг» гармоник по частоте обратен периоду следования импульсов. А вот амплитуда гармониче-

ских составляющих выросла. Именно этот эффект и позволяет резко улучшить соотношение сигнал/шум при измерении сигналов ПЭМИН.

Все приведённые выше спектры иллюстрируют предельно идеализированную картину. Реальные спектры ПЭМИН, при совпадении частот, составляющих с теорией, имеют абсолютно случайные распределения амплитуд. Нельзя забывать, что реальное излучение есть сумма, суперпозиция большого числа излучателей (случайных антенн), у каждого из которых своя амплитудно-частотная характеристика со своими пиками и провалами, резонансами и т.д.

Особо следует отметить следующее. В понимании физики этих процессов есть одна особенность. Практически всегда инженер уверен, что именно такой спектр существует реально, объективно. Мы привыкли, априори, считать, что наши приборы отражают реальную, объективно существующую, картину мира. В данном случае мы «видим» отображение объективной реальности узкополосным, селективным, прибором. И эти частотные составляющие, гармоники, возникают только в нашем средстве измерения. В реальности существует только сплошной спектр от каждого фронта каждого импульса. Естественно, что он конечен, поскольку конечна длительность фронта. Он не равномерный, поскольку искажён свойствами реальных случайных антенн. Но всегда сплошной. А линейчатым он становится только в нашем приёмнике, за счёт инерционности, своеобразной «памяти» входного устройства, и нигде иначе.

В реальных устройствах импульсные последовательности не бывают бесконечными. Практически без исключений любая пересылка, обработка и т.д. выполняется «пакетами». Поэтому, наиболее реальной моделью сигнала в цепях СВТ будет последовательность таких пакетов, в которых длина пакета существенно больше длительности одного импульса. Такая модель и её спектр приведены на рис. 4.

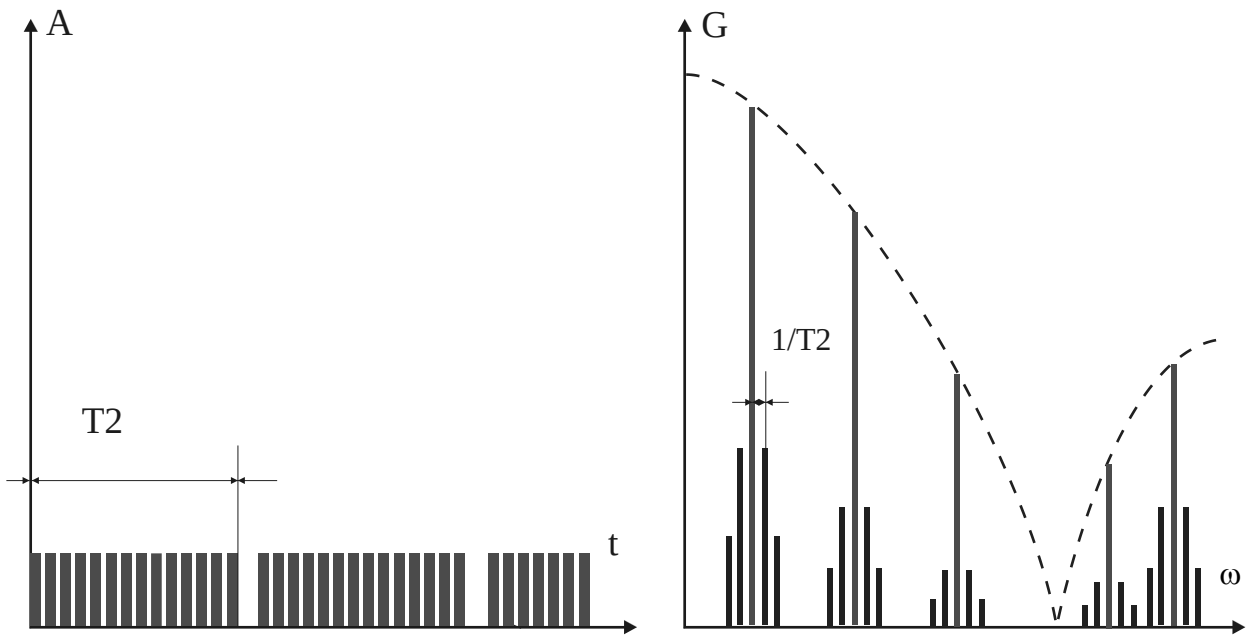


Рис. 4. Спектр последовательности пакетов импульсов

Как видно на рисунке (масштаб изображений изменён для наглядности, изображены не все боковые составляющие) около каждой спектральной составляющей, обусловленной самими импульсами, появились боковые составляющие, обусловленные частотой следования пакетов.

Функционирование любого технического средства информации связано с протеканием по его токоведущим элементам электрических токов различных частот и образованием разности потенциалов между различными точками его электрической схемы, которые порождают магнитные и электрические поля, называемые побочными электромагнитными излучениями.

Узлы и элементы электронной аппаратуры, в которых имеют место большие напряжения и протекают малые токи, создают в ближней зоне электромагнитные поля с преобладанием электрической составляющей. Преимущественное влияние электрических полей на элементы электронной аппаратуры наблюдается и в тех случаях, когда эти элементы малочувствительны к магнитной составляющей электромагнитного поля.

Узлы и элементы электронной аппаратуры, в которых протекают большие токи и имеют место малые перепады напряжения, создают в ближней зоне электромагнитные поля с преобладанием магнитной составляющей. Преимущественное влияние магнитных полей на аппаратуру наблюдается также в случае, если рассматриваемое устройство малочувствительно к электрической составляющей или последняя много меньше магнитной за счет свойств излучателя.

Переменные электрическое и магнитное поля создаются также в пространстве, окружающем соединительные линии (провода, кабели) ТСПИ.

Побочные электромагнитные излучения ТСПИ являются причиной возникновения электромагнитных и параметрических каналов утечки, информации, а также могут оказаться причиной возникновения наводки информационных сигналов в посторонних токоведущих линиях и конструкциях. Поэтому снижению уровня побочных электромагнитных излучений уделяется большое внимание.

## 1.2. Классификация утечки информации по каналам ПЭМИН

Возможные каналы утечки информации создаются:

1) низкочастотными электромагнитными полями, которые возникают во время работ ТСПИ и ВТСС;

2) во время влияния на ТСПИ и ВТСС электрических, магнитных и акустических полей;

3) при возникновении паразитной высокочастотной (ВЧ) генерации;

4) при прохождении информативных (опасных) сигналов в цепи электропитания;

5) при взаимном влиянии цепей;

6) при прохождении информативных (опасных) сигналов в цепи за-

земления;

7) при паразитной модуляции сигнала;

8) вследствие ошибочных коммутаций и несанкционированных действий.

В зависимости от физической природы возникновения информационных сигналов, а также среды их распространения и способов перехвата, технические каналы утечки информации по каналам ПЭМИН можно разделить на электромагнитные и электрические.

### 1.2.1. Электромагнитные КУИ

К электромагнитным каналам утечки информации относятся:

- перехват побочных электромагнитных излучений (ПЭМИ) элементов ТСПИ;
- перехват ПЭМИ на частотах работы высокочастотных (ВЧ) генераторов в ТСПИ и ВТСС;
- перехват ПЭМИ на частотах самовозбуждения усилителей низкой частоты (УНЧ) ТСПИ.

#### 1.2.1.1. Побочные электромагнитные излучения элементов ТСПИ

В ТСПИ носителем информации является электрический ток, параметры которого (амплитуда, частота либо фаза) изменяются по закону изменения информационного сигнала. При прохождении электрического тока по токоведущим элементам ТСПИ вокруг них возникает электрическое и магнитное поля. В силу этого элементы ТСПИ можно рассматривать как излучатели электромагнитного поля, несущего информацию.

#### 1.2.1.2. ЭМИ на частотах работы ВЧ-генераторов ТСПИ и ВТСС

В состав ТСПИ и ВТСС могут входить различного рода высокочастотные генераторы. К таким устройствам можно отнести: задающие генераторы, генераторы тактовой частоты, генераторы стирания и подмагничивания магнитофонов, гетеродины радиоприемных и телевизионных устройств и т.д.

В результате внешних воздействий информационного сигнала (например, электромагнитных колебаний) на элементах ВЧ-генераторов наводятся электрические сигналы, которые могут вызвать паразитную модуляцию собственных ВЧ-колебаний генераторов. Эти модулированные ВЧ-колебания излучаются в окружающее пространство.

#### 1.2.1.3. ЭМИ на частотах самовозбуждения УНЧ ТСПИ.

Самовозбуждение УНЧ ТСПИ (например, усилителей систем звукоусиления и звукового сопровождения, магнитофонов, систем громкоговорящей связи и т.п.) возможно за счет образования случайных паразитных обратных связей, что приводит к переводу усилителя в режим автогенерации сигналов. Сигнал на частотах самовозбуждения, как правило, оказывается промодулированным информационным сигналом. Самовозбуждение наблюдается, в основном, при переводе УНЧ в нелинейный режим работы, т.е. в режим перегрузки.

Перехват побочных электромагнитных излучений ТСПИ осуществляется средствами радио-, радиотехнической разведки, размещенными вне контролируемой зоны.

### 1.2.2. Электрические КУИ

Электрические каналы утечки информации включают:

1) съем наводок ПЭМИ ТСПИ с соединительных линий ВТСС и посторонних проводников;

2) съем информационных сигналов с линий электропитания ТСПИ;

3) съем информационных сигналов с цепей заземления ТСПИ и ВТСС;

4) съем информации путем установки в ТСПИ электронных устройств перехвата информации.

Пространство вокруг СВТ, в пределах которого на случайных антеннах наводится информационный сигнал выше допустимого (нормированного) уровня, называется зоной r1.

Случайные антенны могут быть сосредоточенными и распределенными. Сосредоточенные случайные антенны (ССА) представляют собой компактное техническое средство, например, телефонный аппарат, громкоговоритель трансляционной сети. К распределенным случайным антеннам (РСА) относятся случайные антенны с протяженными параметрами: кабели, провода, металлические трубы и другие токопроводящие коммуникации.

#### 1.2.2.1. Наводки электромагнитных излучений ТСПИ.

Наводки электромагнитных излучений СВТ возникают при излучении информационных сигналов элементами ТС, а также при наличии гальванических связей со средствами ВТ.

Просачивание информационных сигналов в сети электропитания возможно при наличии реакции выпрямителя на работу устройств с информационными сигналами.

Просачивание информационных сигналов в цепи заземления объекта возможно при работе локальной вычислительной сети по кабелям при значительной их протяженности.

Уровень наводимых сигналов в значительной степени зависит от мощности излучаемых сигналов, расстояния до проводников, а также длины совместного пробега соединительных линий ТСПИ и посторонних провод-

ников. Случайной антенной является цепь ВТСС или посторонние проводники, способные принимать побочные электромагнитные излучения.

# 2. МЕТОДИКА ОБНАРУЖЕНИЯ И ИЗМЕРЕНИЯ ПЭМИН

## 2.1. Методика обнаружения и измерения ПЭМИН

Существуют две основных методики оценки защищённости ТС от утечки по каналу ПЭМИН. Это методика собственно специальных исследований, результатом применения которой является определение значений радиуса зоны R2 вокруг технического средства (ТС), на границе и за пределами которой напряженность электромагнитного поля информативного сигнала не превышает нормированного значения, радиуса зоны r1 вокруг ТС в пределах которого не допускается размещение сосредоточенных антенн и радиуса зоны r1’ вокруг ТС, в пределах которого не допускается размещение случайных антенн [2].

Результатом второй методики оценки защищённости являются измеренное и рассчитанное соотношение сигнал/шум на границе КЗ.

Часто задаётся вопрос, какая из этих двух методик должна применяться. Исходя из того, что в первой из упомянутых методик, весь расчёт производится из предположения, что электромагнитное поле распространяется в свободном пространстве над полупроводящей поверхностью, эта методика и применима в условиях, близких к таковым. Вторая методика учитывает реальное затухание от исследуемого ТС до границы КЗ. Однако в её рамках не определяются значения r1 и r1’ и сама она является заметно упрощённой. В связи с этим для объектовых исследований наиболее объективной следует признать методику специальных исследований (определения R2, r1 и r1’), дополненную методом реальных зон. Какую методику применять в каждом конкретном случае – выбор за специалистом.

Рассмотрим источники ПЭМИН типового СВТ. К ним относятся: накопители на жёстком и гибком дисках (включая внешние ZIP, JAZ), устройства CD и DVD, устройства внешней «Флешь» памяти, клавиатура, последова-

тельный порт (COM), последовательный порт (USB), принтеры, видеоподсистема.

Накопители на магнитных носителях, с точки зрения СИ, должны разделяться на, как минимум, на две части. Это интерфейс, обеспечивающий передачу информации от материнской платы в буфер устройства. И, собственно, цепи записи на носитель. Для накопителя на жёстком диске интерфейс всегда параллельный и, минимум, 32-разрядный, а цепи записи всегда последовательны. То же самое можно сказать и о дисках ZIP, JAZ. Интерфейс может быть и параллельным, например – LPT, и последовательным – USB, а головка записи – это всегда последовательный код.

Оптические диски разных моделей по интерфейсу, как правило – параллельные. По узлам считывания/записи - последовательные.

Клавиатура – классическое устройство с последовательным кодированием. Клавиатура весьма низкоскоростное устройство (тактовая частота 6-10 кГц).

Виды кодирования в портах COM и USB. Порт по протоколу USB 1.1 работает строго на частоте 12 МГц, а если и порт и внешнее устройство поддерживают версию протокола USB 2.0, то они сами «договариваются» об взаимообмене на произвольной частоте, которая может оказаться в диапазоне до 400 МГц. Эту частоту необходимо определять непосредственными измерениями в интерфейсе, так как проведение СИ без знания этого значения невозможно.

У принтеров следует различать интерфейс передачи данных и печатающий узел отдельно. Стандартный интерфейс – LPT (8 разрядов). У лазерных принтеров узел печати (лазерный диод) - это всегда последовательно. А печатающая головка матричного, а, тем более, струйного принтера – параллельно (весьма важно правильно определить число «разрядов»).

Для мониторов с отображением информации на экране ЭЛТ сигнал в аналоговом RGB интерфейсе (в физических линиях от видеокарты к монито-

ру) передается потенциальным кодом с различной амплитудой, то есть классический АИМ и ШИМ сигнал.

В настоящее время практическое применение описанных выше методик реализовано в системе оценки защищенности технических средств по каналу ПЭМИН «СИГУРД» и в программно - аппаратном комплексе «Легенда». Для понимания принципа действия данных комплексов возможно провести их сравнение.

Приведём результат работы системы «Сигурд» в режиме исследования видеоподсистемы. При этом тестовое изображение на экране монитора исследуемой СВТ представляет собой «картинку», приведённую на рис. 5. «Скрин» с экрана системы «Сигурд» сигнала видеоподсистемы СВТ при загруженном тесте изображен на рис. 6. В каждой строке растра чередуются чёрные и белые минимальные элементы изображения. Каждому прямоугольному «импульсу» на рис. 5 соответствует одна «серая» полоса на рис. 6. Группе из 5 полос – один кадр развёртки. Уровни шумов в промежутках между «импульсами» - это времена пауз в работе теста (промежутки между «серыми» полосами»).

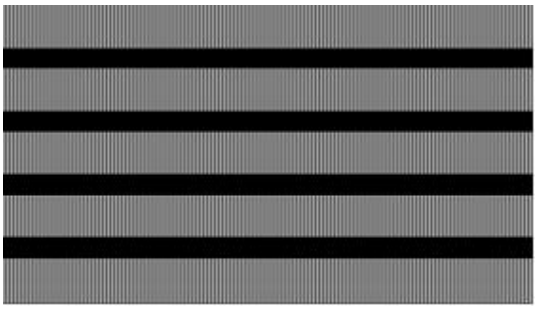

Рис. 5. «Скрин» с экрана системы «Сигурд»
сигнала видеоподсистемы СВТ при загруженном тесте

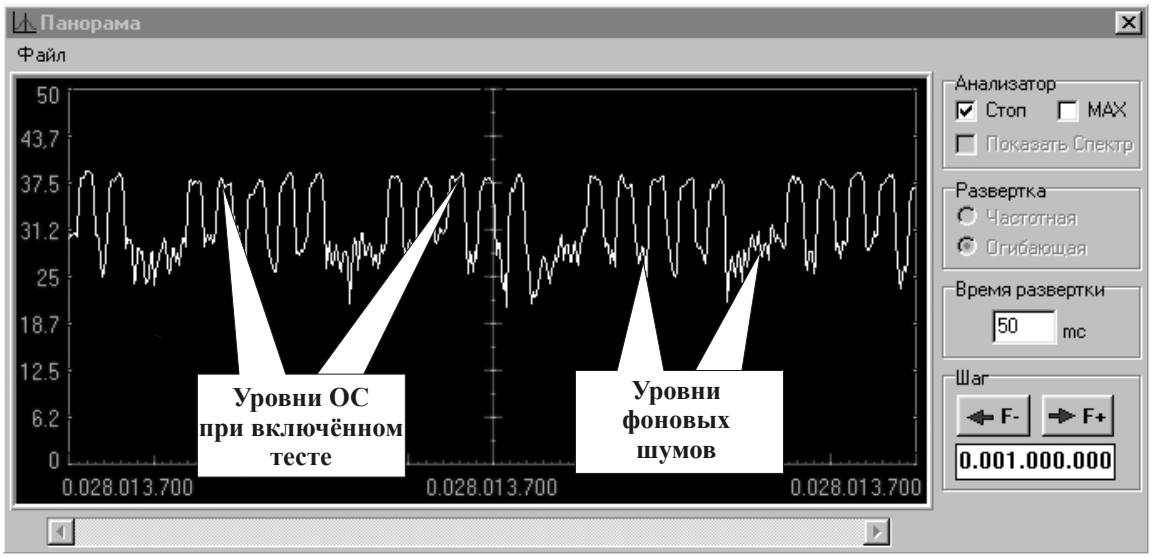


Рис. 6. «Скрин» с экрана исследуемой СВТ теста видеоподсистемы на экране монитора исследуемой СВТ.

Приведём результат работы комплекса «Легенда» в режиме исследования видеоподсистемы. Стандартный тест-режим для СИ этого устройства — это вывод на экран видеосигнала, представляющего собой чередование прямоугольных импульсов с такими же по времени промежутками между ними (сигнал типа «меандр»). Каждая строка растра при этом представляет собой пакет импульсов. Число импульсов в пакете равно половине разрешения экрана по горизонтали (для режима 1024*768 это составит 512 импульсов). Далее пауза, обусловленная обратным ходом строчной развёртки, и новый пакет. На рис. 7 приведен «Скрин» с экрана комплекса «Легенда», где на спектрограмме представлена гармоника тактовой частоты с огибающей, обусловленной длительностью пикселя сигнала.

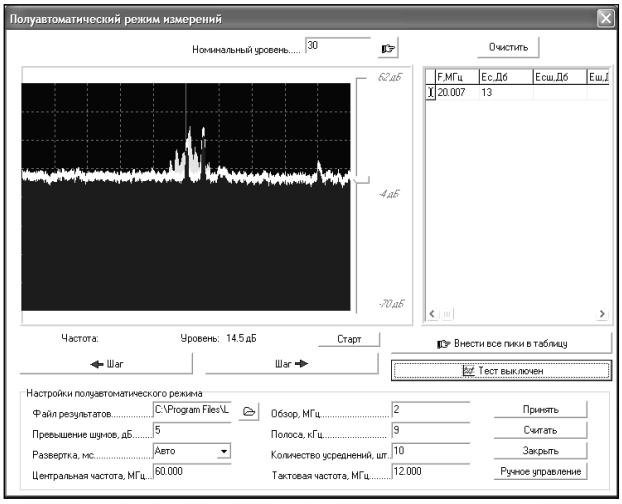


Рис. 7. «Скрин» с экрана комплекса «Ленента»

спектра ОС от видеоподсистемы

Согласно действующим нормативно-методическим документам, при проведении специальных исследований требуется измерять информативные сигналы, при этом «полезная» информация хранится в малой части полного спектра сигнала. Все прочие излучения не должны фиксироваться при измерениях. Для того чтобы выделить информационные составляющие ПЭМИН, на исследуемом техническом средстве предусматривают специальные тестовые режимы его работы. Требования к тестам определяются в соответствующих ГОСТ и методиках [4].

В соответствии с методикой проведения специальных исследований технических средств по измерению их собственного электромагнитного излучения проводятся следующие операции:

1. Контролируемое устройство включается в тестовый режим.

2. На определенном расстоянии (обычно 1 м) от устройства устанавливаются поочередно антенны для приема электрической и магнитной составляющих поля, излучаемого анализируемым устройством (рис. 9).

3. Электрический сигнал с выхода антенны подается на вход прием-

норегистрирующего измерительного устройства, с помощью которого по результатам измерений по определенной методике производится расчет опасных зон.

На рис. 8 изображена типовая схема измерения ПЭМИН

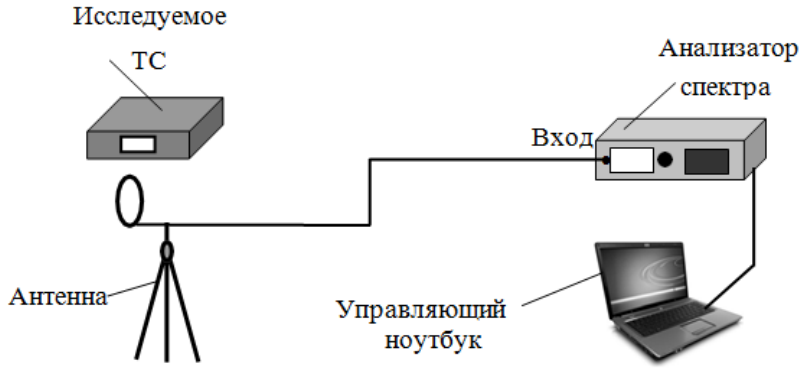


Рис. 8. Схема измерения ПЭМИН

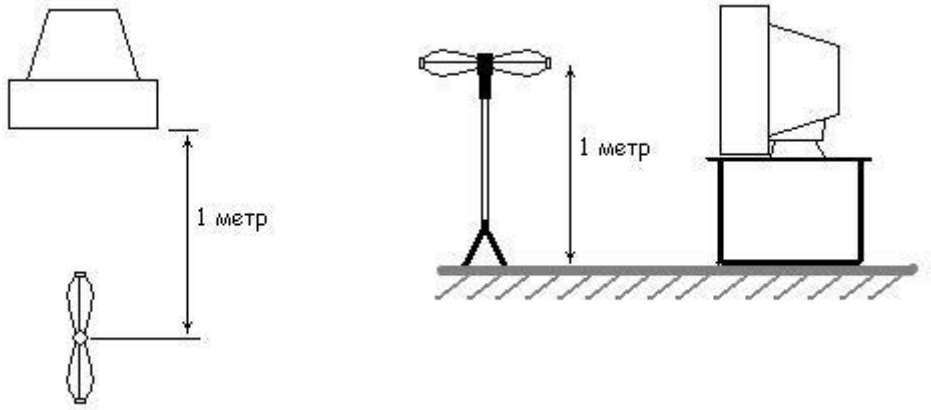


Рис. 9. Порядок установки приемных антенн

## 2.2. Методика измерения наводок и реального затухания

Наводки информативного сигнала (ИС) на линии оцениваются по методике оценки защищённости, результатом которой является измеренное и рассчитанное соотношение сигнал/шум на границе КЗ. Достаточно часто возникают определённые затруднения при использовании метода реальных зон. Собственно говоря, это уже описанный метод учёта реального затухания в канале (в линиях), только применительно к каналу утечки через ПЭМИН.

Как и всегда, при таких измерениях, необходимо ввести в канал тест-сигнал большого уровня, позволяющий надёжно измерить его значение на дальнем конце канала, то есть на границе КЗ.

В соответствии с методикой, излучающая антенна должна быть установлена на месте ТС, защищённость которого оценивается. Вполне достаточно, чтобы антенна была размещена вблизи ТС. В общем случае, расстояние между антенной и ТС должно быть значительно меньше, чем расстояние от антенны до границы КЗ, точнее – до той точки, где будет размещаться приёмная антенна.

Излучающая антенна должна быть ненаправленной, хотя бы в горизонтальной плоскости. Иначе достаточно сложно имитировать ПЭМИН исследуемого ТС. Именно поэтому рекомендуется применение антенны для измерения затухания ИС в линиях. Данная рекомендация относится к случаю измерения реального затухания для электрического поля.

В помещении, где расположен защищаемый объект ЭВТ, излучающую антенну, рекомендуется размещать на том же расстоянии от внешней стены, окна, что и исследуемое ТС. Это связано с тем, что чаще всего в современных зданиях из сборного железобетона, основной путь электромагнитной волны к границе КЗ это оконный проём и переизлучение металлоконструкциями стены. В меньшей степени, но, общем случае, присутствует и излучение линий электропитания [5].

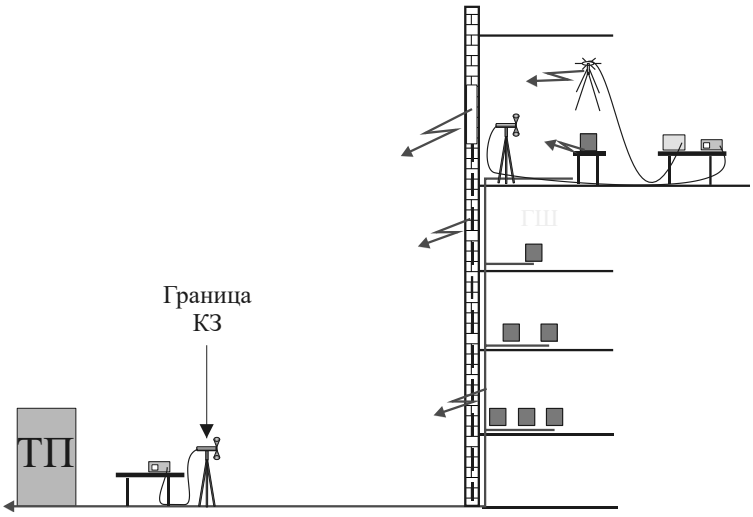


Рис. 10. Схема измерений наводок методом реальных зон

Общая схема измерений приведена на рис. 10. Как видно из схемы, напряжённость поля на границе КЗ представляет собой суперпозицию многочисленных излучателей. Особое внимание нужно обращать на электропитание приборов при этих измерениях. Зачастую генератор ВЧ может выдавать весьма заметный сигнал в эту цепь. В результате этот сигнал, во-первых, может по той же линии электропитания попасть в приёмную антенну или в сам приёмник. Результаты измерений будут искажены. Вообще, в данном случае, гораздо надёжнее автономное электропитание и антенны и приёмника. При его отсутствии необходима тщательнейшая проверка отсутствия связей «по питанию» и устранение их при наличии.

Если граница КЗ расположена в нескольких местах на равных расстояниях от исследуемого ТС, то измерения должны быть проведены во всех этих местах. В практике нередки случаи, когда затухание сигнала при его прохождении через объём здания получается меньшим, чем на таком же расстоянии в свободном пространстве. Видимо, «работают» на переизлучение какие-то случайные антенны.

В тех случаях, когда на границе КЗ не удаётся принять тестовый сигнал из-за значительного его затухания и спадания ниже уровня шумов,

в расчёт реального затухания следует подставлять сами шумы. В этих случаях оператор должен быть абсолютно уверен, что сигнал не принимается именно вследствие его малости, а не по другим причинам.

## 3. ПРОГРАММНО-АППАРАТНЫЕ КОМПЛЕКСЫ ИЗМЕРЕНИЯ ПЭМИН

Основным средством измерения в этой области является селективный измерительный прибор необходимого диапазона частот. В настоящее время это диапазон составляет от 10 Гц до, почти, 2 ГГц. Вся полоса частот перекрывается 2-3 измерительными приборами. Стандартная, принятая во всём мире, нижняя частота универсальных анализаторов спектра и измерительных приёмников составляет 9 кГц.

В области СИ цифровой техники созданы и эксплуатируются ряд автоматизированных систем (комплексов).

В настоящее время Сертификаты ФСТЭК имеют комплексы «Зарница-П» («Элерон»), «Навигатор» («Нелк»), «Легенда» («Гамма») и «Сигурд» («ЦБИ МАСКОМ»).

«Зарница» - комплекс, созданный на базе нестандартного средства. Его основой является сканирующий приёмник серии AOR. Комплекс имеет метрологический сертификат и Сертификат Гостехкомиссии РФ. «Зарница» не опознаёт самостоятельно информативные сигналы на фоне других сигналов, а работает на принципе сравнения излучения в двух режимах исследуемого устройства, с выключенным и включённым тест-режимом. Остальное должен делать оператор.

Комплекс «Навигатор» выполнен на анализаторах спектра фирм Agilent Technology и, последние версии, R&S. Этот комплекс так же не опознаёт самостоятельно ОС на фоне других, а работает на принципе сравнения излучения в двух режимах исследуемого устройства, с выключенным и включённым тест-режимом.

Два последних комплекса, построенные на анализаторах Agilent Technology и R&S («Легенда») и IFR («Сигурд»), отличаются тем, что способны самостоятельно опознавать ОС по форме их огибающих, заданных соответствующими тест-программами.

### 3.1. Программно-аппаратный комплекс «ЛЕГЕНДА»

Программно-аппаратный комплекс (ПАК) «ЛЕГЕНДА» предназначен для проведения специальных исследований по каналу ПЭМИН технических средств обработки информации.

ПАК «Легенда» сертифицирован по требованиям безопасности информации в системе сертификации ФСТЭК России (Сертификат ФСТЭК России № 3250 от 31.10.14 г., действует до 31.10.17 г.)

Описание комплекса

Комплекс является автоматизированной системой оценки защищенности средств вычислительной техники от утечки информации по каналу побочных электромагнитных излучений и наводок, позволяющей осуществить полный цикл работ по инструментальному исследованию технических средств, включая поиск и обнаружение информативных составляющих побочных излучений и наводок, измерение их параметров, а также расчет показателей защищенности технических средств и формирование протокола исследований в соответствии с требованиями нормативно-методического документа ФСТЭК России «Сборник методических документов по контролю защищенности информации, обрабатываемой средствами вычислительной техники, от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России, 2005 г.). Расчетные программы соответствует требованиям НМД ПЭМИН по обработке результатов измерений, расчету контролируемых показателей и оценки защищенности информации на объектах вычислительной техники, а также формирования протоколов исследований.

Преимущества:

- время обнаружения и измерения опасных сигналов от одного исследуемого интерфейса составляет не более 25 минут;

- совершенствованный комплект антенн «Альбатрос-3»;

- улучшенные вероятностные характеристики в режиме поиска опасных сигналов. Вероятность ложной тревоги составляет не более 12%. Вероятность пропуска сигналов составляет не более 10% (для сигналов ПЭМИН малой мощности).

Базовый состав:

- анализатор спектра Agilent E440xB;

- аналогово-цифровой преобразователь LCard E14-440;

- комплект антенн «Альбатрос-3»;

- персональная ЭВМ;

- плата National Instruments GPIB-USB или аналог;

- пробник напряжения Я6-122/1;

- операционная система Microsoft Windows 7;

- пакет программ Microsoft Office 2010;

- комплект специального программного обеспечения в составе управляющих и расчетных программ;

- упаковка (кофр);

- комплект эксплуатационных документов.

Таблица 1 – Характеристики ПАК «Легенда»

| **Параметры и характеристики** | **Значение** |
|---|---|
| Диапазон рабочих частот, не менее, МГц:<br>• электрического поля<br>• магнитного поля<br>• напряжения переменного тока | от 0,01 до 1800<br>от 0,01 до 30<br>от 0,01 до 30 |

| | |
|---|---|
| Погрешность измерения, не более, %:<br>• напряженности электрического поля<br>• напряженности магнитного поля<br>• напряжения переменного тока | <br>30<br>30<br>30 |
| Масса, не более, кг | 25 |

На рисунке 11 изображен состав ПАК «Легенда»

Рис. 11. Программно-аппаратный комплекс «ЛЕГЕНДА»

Отличительные особенности комплекса:

- два этапа обнаружения ПЭМИН исследуемых технических средств в автоматизированном режиме (устранение «чужих сигналов»):
- выделение пика на фоне шумов («энергетический» критерий);
- распознавание образа сигнала (сравнение эталонного сигнала с сигналом приемного устройства в текущий момент);
- достоверность и повторяемость результатов измерений;
- возможность применения различных антенных систем в том числе и старого парка аппаратуры (RFT);

- возможность полуавтоматического обнаружения и измерения сигналов, измерения по сформированным шаблонам (наибольшая скорость проведения исследований);

- автоматическое формирование протоколов измерений;

- использование самых распространенных текстовых редакторов – «Microsoft Office», «Word Pad» и «Note Pad» при оформлении отчетных документов.

Для обнаружения и измерения уровней сигналов создается образ эталонного сигнала с помощью специального редактора эталонов. Определяется программа проведения исследований.

По команде оператора комплекс сканирует указанный в настройках диапазон, обнаруживает и измеряет сигналы ПЭМИН СВТ.

Имеется возможность прерывать работу для подключения или изменения характеристик антенн. Измеренные значения заносятся в таблицу, которая затем может сохраняться в виде файла на диске.

ПАК «ЛЕГЕНДА» имеет управляющую и расчетную программы, которые способны опознавать заданные тест - программами опасные сигналы по форме их огибающих. В результате спец. исследований определяются опасные зоны $R_2$, $r_1$ и $r_1'$ и формируется отчетный протокол. Эти исследования могут быть дополнены исследованиями по методу реальных зон.

Внешний вид основного рабочего экрана управляющей программы «Легенда» представлен на рис. 12.

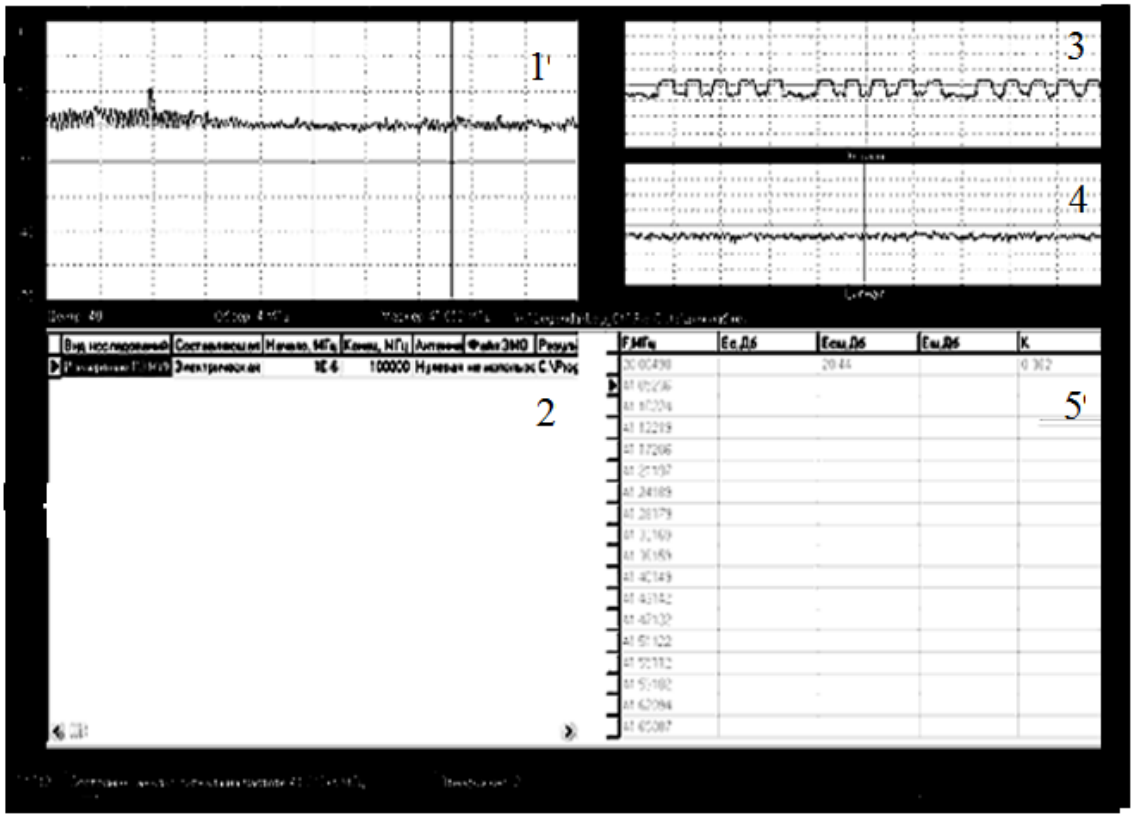


Рис. 12. Внешний вид экрана управляющей программы «Легенда»

На рис. 12 цифрами обозначены следующие элементы основного рабочего экрана (главного окна):

1 – окно спектра (отображается спектр сигнала для выбранного диапазона частот);

2 – таблица исследований (отображаются все программы исследований, которые будут выполнены в автоматическом режиме);

3 – окно эталона (осциллограмма найденного в полуавтоматическом режиме эталона тестового сигнала);

4 – окно сигнала (осциллограмма сигнала, который будет сравниваться с эталоном);

5– рабочая таблица промежуточных результатов.

### 3.2. Система оценки защищённости технических средств «СИГУРД»

Система оценки защищенности технических средств по каналу ПЭМИН «СИГУРД» предназначена для проведения специальных исследований различных технических средств с целью выявления, распознавания и измерения сигналов побочного электромагнитного излучения этих устройств с минимальным участием оператора.

Система «Сигурд» сертифицирована по требованиям безопасности информации в системе сертификации ФСТЭК России (Сертификат ФСТЭК России на 642/1 от 21.07.06 г., продлен до 21.07.18 г.)

Система создана на базе спектроанализатора фирмы IFR, стандартного IBM-совместимого персонального компьютера и комплекта антенн. Комплекс может включать в свой состав спектроанализаторы аналогичного класса и других производителей при условии доработки программного обеспечения. Могут быть применены любые антенны, предназначенные для работы в диапазоне от 9 кГц до 2 ГГц. Рекомендуется применение активных широкополосных антенн. Параметры антенн (антенный коэффициент) вводится в управляющую программу и учитывается автоматически при выборе соответствующей антенны. Замена антенн в процессе измерений осуществляется оператором в соответствии с сообщениями управляющей программы.

Система «Сигурд» обеспечивает:

-· автоматизированное исследование технического средства на наличие информативных сигналов ПЭМИН в полном соответствии с действующими нормативно-методическими документами;

-· автоматический и ручной поиск сигналов ПЭМИН исследуемого технического средства на фоне постоянно присутствующих радиосигналов

по электрической и по магнитной составляющим электромагнитного поля, а также в отходящих линиях;

-· автоматическое и ручное распознавание информативных сигналов ПЭМИН;

-· расчет показателей защищенности технических средств от утечки информации по каналу ПЭМИН в соответствии с действующими нормативными документами, с выводом результатов по выбору оператора в файл стандарта HTML или MS Word (DOC);

-· автоматизированное исследование систем активного зашумления (САЗ) и расчет показателей их эффективности;

-· дистанционное автоматическое управление измерительным приемником (анализатором спектра) при поиске сигналов ПЭМИН, а при использовании опции «Сигурд-ИК» - и дистанционное автоматическое управление состоянием исследуемого технического средства при поиске его сигналов ПЭМИН;

-· автоматическую передачу исходных данных в расчет показателей защищенности технического средства и эффективности САЗ;

-· возможность создания и пополнения базы данных по постоянно присутствующим радиосигналам в выбранном диапазоне частот;

-· возможность визуализации в процессе исследования радиосигналов, представляющих интерес;

-· формирование сообщений о неверных действиях оператора с указанием характера ошибки;

-· расчет минимально допустимых расстояний R2 от технического средства до границы контролируемой зоны;

-· расчет минимально допустимых расстояний r1 от технического средства до сосредоточенных случайных антенн;

-· расчет минимально допустимых расстояний r1’ от технического средства до распределенных случайных антенн;

-· расчет отношения «сигнал/шум» на границе контролируемой зоны;

-· расчет отношения «сигнал/шум» на границе контролируемой зоны с учетом применения систем активного зашумления;

-· расчет отношения «сигнал/шум» в отходящих линиях;

-· расчет отношения «сигнал/шум» в отходящих линиях с учетом применения систем активного зашумления.

Таблица 2 – Характеристики системы «Сигурд»

| **Параметры и характеристики** | **Значение** |
|---|---|
| Границы диапазона частот при измерении системой напряженности электрического поля | 9 кГц-2000 МГц |
| Границы диапазона частот при измерении системой напряженности магнитного поля | 9 кГц-30 МГц |
| Границы диапазона частот при измерении системой силы тока и напряжения переменного тока, наведенного электромагнитным полем | 9 кГц-300 МГц |
| Динамический диапазон измерений напряженности электромагнитного поля, силы тока и напряжения переменного тока, наведенного электромагнитным полем, не менее | 75 дБ |
| Устанавливаемые полосы пропускания, не менее | 0,1; 0,3; 1; 3; 10; 30; 100; 300 кГц |
| Продолжительность поиска | 300 с |
| Масса системы (без доп. опций), не более: | |
| - для модификаций М7, М8, М19, М22 | 25 кг |

| Параметры и характеристики | Значение |
|---|---|
| - для модификаций М3, М4, М13 | 30 кг |
| - для модификаций М5, М6 | 16 кг |

На рисунке 13 изображен состав системы «Сигурд»

Рис. 13. Система оценки защищенности по каналу ПЭМИН «СИГУРД»

На рисунке 14 изображена управляющая программа системы «Сигурд»

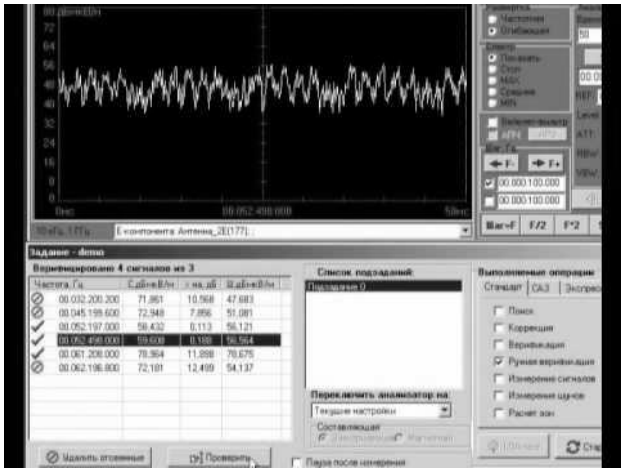

Рис. 14. Управляющая программа системы «Сигурд»

# 4. ПОРЯДОК ПРОВЕДЕНИЯ ЛАБОРАТОРНОЙ РАБОТЫ

## 4.1. Постановка задачи исследования

Исследование побочного электромагнитного излучения монитора при применении ПАК «Легенда» необходимо проводить с помощью измерительных антенн «Альбатрос».

Проблема выделения сигналов, обладающих информационными признаками и относящихся к излучению исследуемого устройства, может быть решена с использованием:

– энергетического принципа пропадания сигнала при отключении контролируемого устройства;

– информационного принципа, когда перед проведением исследования производится формирование эталонного образа искомого сигнала, и в процессе исследования осуществляется автоматическое обнаружение сигналов в эфире, похожих на этот эталонный сигнал.

Сравнение обнаруженного сигнала и образа эталонного сигнала производится путем вычисления максимума взаимнокорреляционной функции между образами сигналов. При превышении данной величиной установленного порогового значения, принимается решение о схожести образов. При этом исключается возможность причисления к перечню обнаруженных частот посторонних сигналов и неинформативных ПЭМИ исследуемого технического средства.

Работа в управляющей программе ПАК «Легенда» сводится к поиску эталона тестового сигнала в полуавтоматическом режиме, составлению программ исследований для предварительного контроля электромагнитной обстановки (ЭМО) и автоматического поиска по заданному эталону похожих сигналов.

### 4.2. Задание для проведения работы

1. Изучить методику проведения спец. исследования.

2. Провести поиск и измерение ПЭМИ монитора на ЭЛТ (монитора на ЖК) в автоматическом и режиме управляющей программы.

3. Составить протокол исследования с помощью расчетной программы.

4. Сделать выводы.

### 4.3. Порядок выполнения работы

- Подготовить комплекс и исследуемое средство к работе.
- Управляющую СВТ и измерительный прибор необходимо соединить кабелем USB.
- Подключить антенну «нулевая диполь» (А117.3) к анализатору спектра R&S FS300 с помощью кабеля А117.3.
- Включить анализатор спектра.
- Включить на исследуемом техническом средстве монитор-тест «Зебра».
- Запустить управляющую программу на персональном компьютере.

Поиск и измерение ПЭМИ в автоматическом режиме измерений.

Создание эталона тестового сигнала.

Для перехода в полуавтоматический режим измерений выберите в меню главного окна программы пункт «Измерения – Ручной режим» или нажмите соответствующую кнопку быстрого запуска. На экране управляющей СВТ выводится окно полуавтоматического режима, показанное на рис. 15.

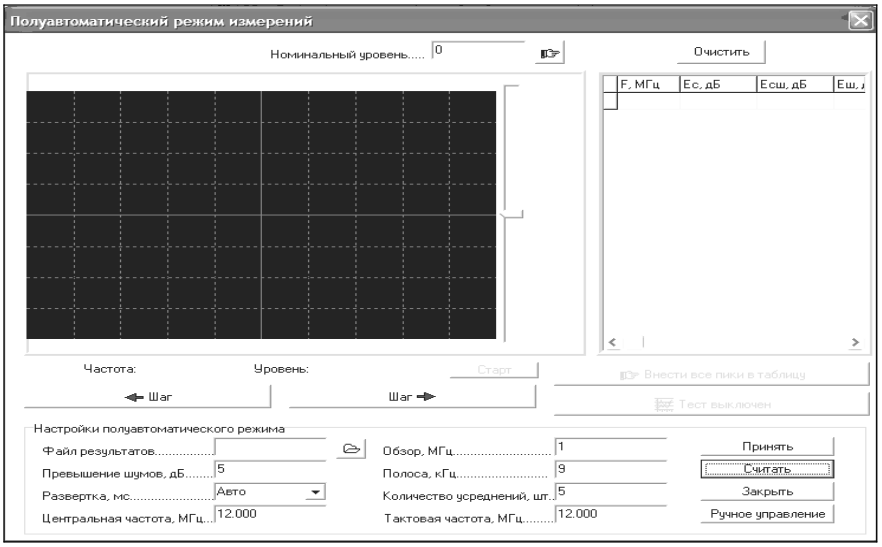


Рис. 15. Окно полуавтоматического режима

Перед созданием эталона тестового сигнала необходимо в ручном режиме с помощью анализатора спектра найти тактовую частоту теста монитора. Это значение необходимо ввести в поле «Центральная частота», обзор установите равным 4МГц, остальные поля заполните согласно рекомендациям, приведенным в предыдущей лабораторной работе. Нажмите кнопку «Принять». На дисплее окна полуавтоматического режима изображается текущее усреднение трека спектра. По завершении усреднений картинка останавливается.

Выключите тест на мониторе и нажмите «Тест выключен». На дисплее окна полуавтоматического режима отображаются в одной системе координат два графика частотного спектра (рис. 16): синим цветом с заполнением отображается график спектра при выключенном тесте, зеленым цветом – график спектра при включенном тесте. Белым цветом с заполнением показывается превышение шумов. Все видимые пики «зеленого» графика подлежат анализу как «подозрительные».

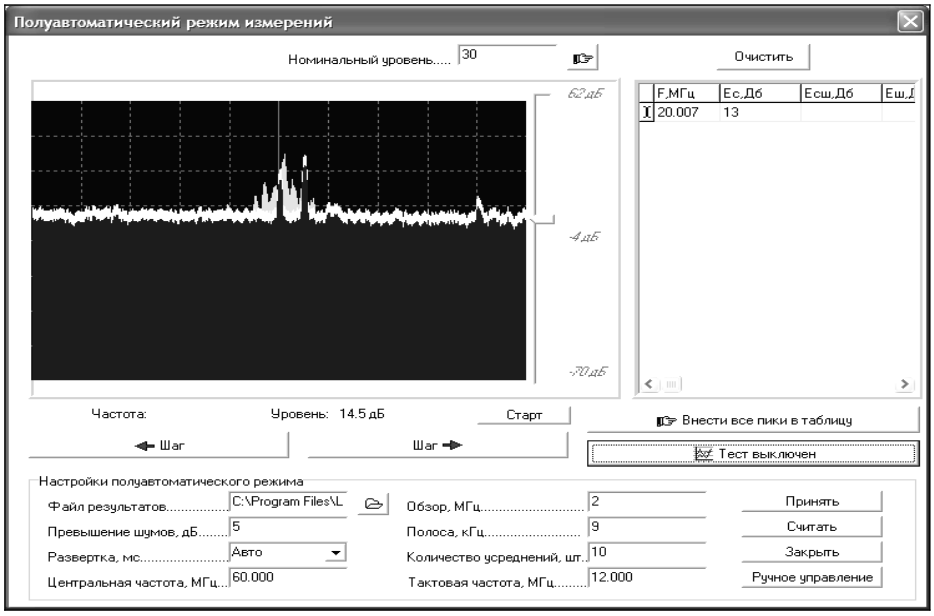


Рис. 16. Графики частотного спектра

Исследуйте все видимые пики «зеленого» графика. Для этого подведите курсор «мыши» к выбранному пику, удерживая нажатой левую кнопку «мыши». При этом внизу под дисплеем отображается значение частоты, совместно с курсором «мыши» перемещается маркер желтого цвета. На строившись на нужный пик, отпустите левую кнопку «мыши». Поверх окна полуавтоматического режима выводится окно просмотра пика (рис. 17). Включая и выключая тестовый режим работы исследуемого технического средства и наблюдая за осциллограммой, установите, принадлежит ли данное излучение гармоническим составляющим тестового сигнала. При обнаружении тестового сигнала следует сохранить его как эталон, нажав на кнопку «Сохранить как эталон» окна просмотра пика. Сохраните в созданную папку со своим номером группы.

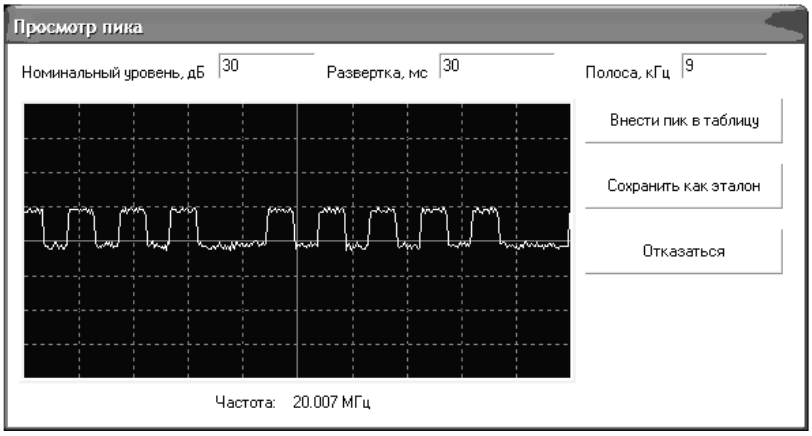


Рис. 17. Осциллограмма демодулированного сигнала

Контроль электромагнитной обстановки (ЭМО)

Выключите тест на исследуемом средстве.

Для предварительного контроля ЭМО следует составить программу исследования, для этого выберите в меню главного окна программы «Установки/Программа исследований». Поверх главного окна программы откроется окно параметров исследования на странице программы исследований (рис. 18).

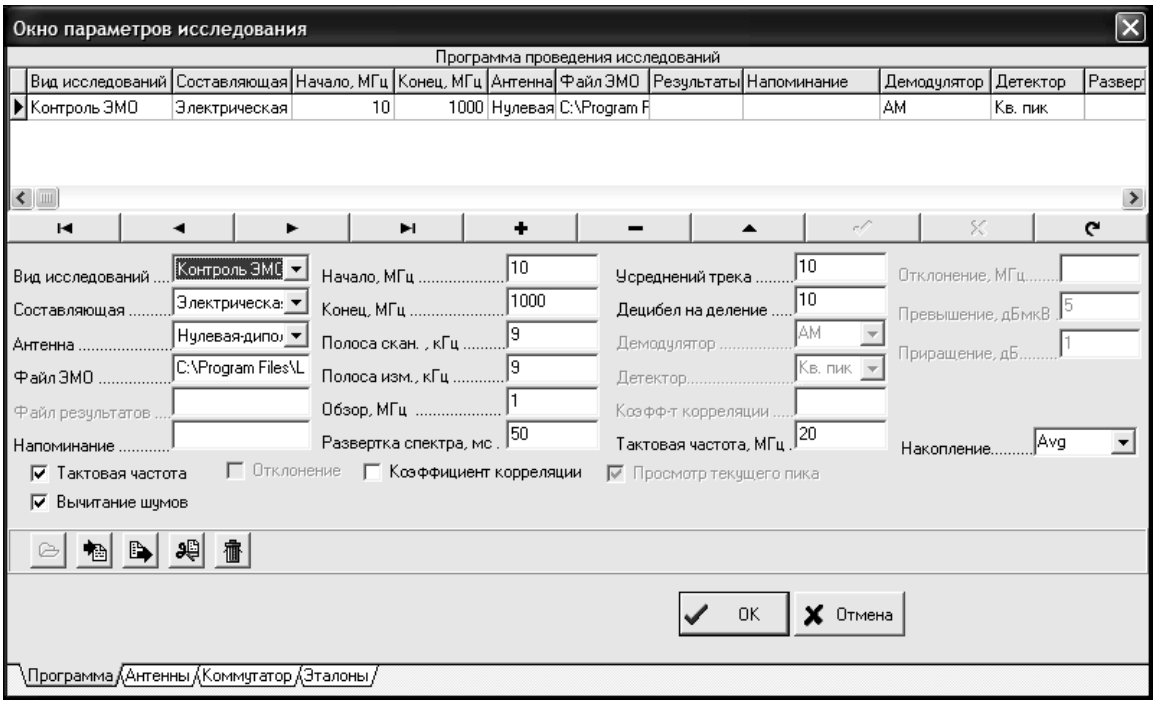


Рис. 18. Окно параметров исследования

В таблице программы исследования, расположенной в верхней части страницы, отображается готовая к исполнению программа. По умолчанию таблица содержит программу, составленную при прошлом запуске управляющей программы. Сотрите старую программу нажатием кнопки «Мусорная корзина». Для экономии времени проведите контроль в окрестностях частот, кратных 20МГц (для монитора на ЭЛТ) или 60МГц (для монитора на ЖК).

После заполнения программы, внесите ее в таблицу нажатием кнопки «Внести в таблицу».

Нажмите кнопку «Ок». Программа автоматически сканирует выбранный диапазон и по завершении выдает сообщение «Программа исследования завершена». При этом, результаты сканирования сохранены в соответствующих выбранных файлах ЭМО для каждого диапазона и их можно использовать для автоматического поиска составляющих тестового сигнала при включенном тесте.

Автоматический поиск составляющих тестового сигнала.

Автоматический поиск гармонических составляющих тестового сигнала по заданному эталону можно производить методом беспропускового контроля по всему диапазону проведения спец. исследования, либо в окрестностях частот, кратных тактовой частоте теста. Для экономии времени проведите исследование в окрестностях частот, кратных 20МГц (для монитора на ЭЛТ) или 60МГц (для монитора на ЖК).

Для поиска составляющих тестового сигнала следует заполнить программу исследований. Для этого достаточно заменить вид исследований во всех заполненных строках таблицы на «Измерение ПЭМИН».

После заполнения программы исследования загрузите эталон, найденный в полуавтоматическом режиме. Примерный вид эталона представлен на рис. 19.

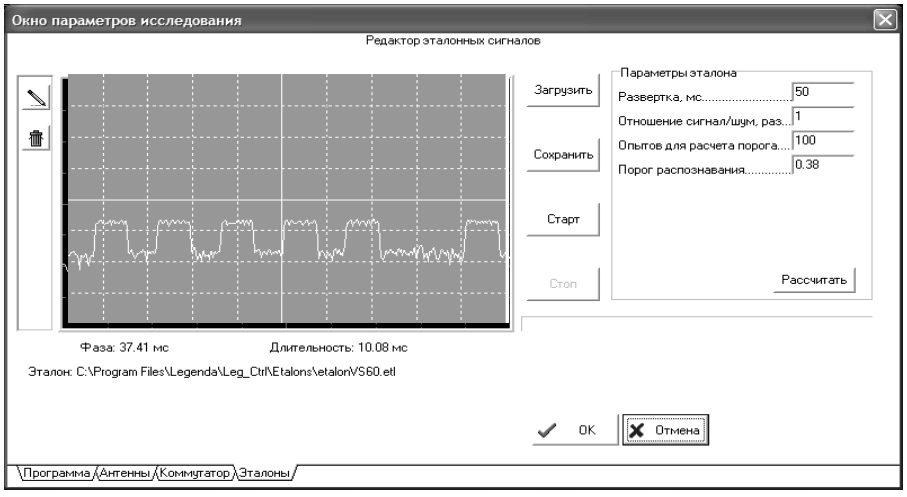


Рис. 19. Эталон тестового сигнала монитора на ЭЛТ

Рассчитайте пороговый коэффициент корреляции, нажав на кнопку «Рассчитать», после чего появится следующее окно (рис. 20).

Выберите в меню главного окна программы пункт «Измерения - Старт», либо нажмите соответствующую кнопку быстрого запуска. Программа начнет сканировать диапазон, выделять пики, превышающие на заданное значение уровень шумов при выключенном тесте (если используется файл ЭМО). Демодулированный сигнал будет сравниваться с эталоном и при превышении коэффициентом корреляции заданного порога, значение частоты будет занесено в таблицу. По завершении сканирования выдается сообщение «Выключите тест для измерения уровней шумов» и программа выполнит необходимые действия. В конце работы выдается сообщение «Программа исследований выполнена».

По завершении автоматического поиска и/или измерения ПЭМИН можно проконтролировать правильность обнаружения. Для этого щелкните «мышью» по любой строке таблицы обнаруженных частот главного окна управляющей программы. На основном дисплее главного окна программы будет отображаться в реальном времени осциллограмма демодулированного сигнала на данной частоте. Включая и выключая тест на исследуемом техническом средстве и наблюдая за изменениями формы осциллограммы, можно сделать вывод о принадлежности данного излучения к составляющим тестового сигнала.

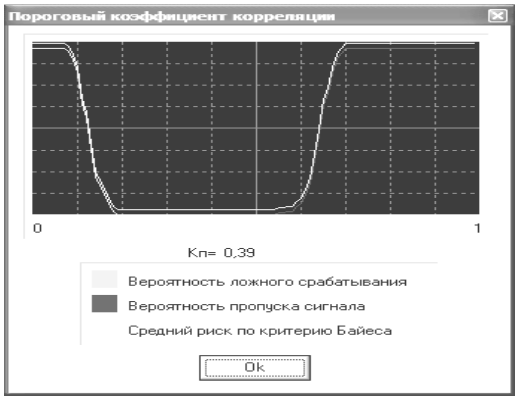


Рис. 20. Расчет порогового коэффициента корреляции

Расчет зон разведдоступности с помощью расчетной программы

Для запуска расчетной программы следует выбрать в меню «Пуск» соответствующий ярлык или вызвать исполняемый файл, на который ссылается данный ярлык («Легенда»).

Для того, чтобы загрузить данные измерений из файла в расчетную программу нужно выбрать в меню «Файл» пункт «Открыть». Появится стандартный диалог открытия файлов Windows. Далее пользователь должен указать файл, в котором содержатся данные измерений для расчета, полученные при работе управляющей программы, и нажать кнопку «Открыть». В случае правильной структуры файла в поля рабочей таблицы «*F*, МГц», «*U*, дБ» и «$U_{Ш}$, дБ» загрузятся значения частоты, уровня обнаруженных компонент тестового сигнала и уровня шума.

Для заполнения условий расчета следует выбрать в меню «Условия» команду «Заполнить». Пользуясь описанием процесса задания условий для расчета из предыдущей лабораторной работы, заполните условия, выставив отношение сигнал/шум для всех трех категорий 0,4.

После внесения и заполнения условий, нажмите Измерения - Старт. Программа рассчитает зоны разведдоступности.

После того, как программа выполнит расчет измерения, нужно сохранить результат в Microsoft Word с помощью кнопки быстрого доступа (документ Microsoft Word должен быть открыт).

### 4.4. Требования к отчету

Оформить отчет о проделанной работе. В отчете привести цель работы, задание на выполнение работы, порядок проведения работы, протоколы исследований в автоматическом и полуавтоматическом режимах. Сравнить результаты. Сделать выводы и ответить на контрольные вопросы.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Хорев А.А. Способы и средства защиты информации: учебное пособие. – М.: МО РФ, 1998. – 316 с.

2. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам, 2005. – 416 с.

3. Торокин А.А. Инженерно-техническая защита информации: учебное пособие для студентов, обучающихся по специальностям в области информационной безопасности. – М.: Гелиос, 2005. – 960 с.

4. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В., Скрыль С.В., Голубятников И.В. Технические средства и методы защиты информации, 2009. – 508 с.

5. Кондратьев А.В. Техническая защита информации. Практика работ, по оценке основных каналов утечки. – М.: Горячая линия - Телеком, 2016. – 304с.

**Приложение 1**

## Протокол измерения ПЭМИН

Ф И О студента _____
Факультет, Группа _____
Дата проверки (подпись преподавателя) _____

Таблица 1 – Состав исследуемого ТС

| № п/п | Наименование технического средства | Изготовитель | Модель | Серийный номер |
|---|---|---|---|---|
| 1 | Системный блок | | | |
| | HDD | | | |
| | DVD | | | |
| 2 | Монитор | | | |
| 3 | Клавиатура | | | |
| 4 | Манипулятор "Мышь" | | | |
| 5 | МФУ | | | |
| 6 | Flash-накопитель | | | |
| 7 | ИБП | | | |

## Измерение побочных электромагнитных излучений (ПЭМИ)

Таблица 2 – Состав измерительного оборудования для измерения ПЭМИ

| Наименования средств измерений и вспомогательного оборудования | Тип | Заводской номер | Диапазон частот | Дата очередной поверки |
|---|---|---|---|---|
| Средства измерений | | | | |
| ПАК «Легенда» в составе: | | | | |
| Анализатор спектра | Agilent | | | октябрь 2017 г. |
| Комплект измерительных антенн “Альбатрос” | АГМ-30<br>АГ-50<br>АГ-1000 | | | октябрь 2017 г. |
| Вспомогательное оборудование | | | | |
| Устройство защиты | Соната-Р2 | | | Периодическая поверка (калибровка) не требуется |

Вывод информации на экран монитора (разрешение - ____*____*___)

Таблица 3 - Результаты измерений и расчета ПЭМИ

| **f i<br>МГц** | **Eoi<br>дБ** | **Eшi<br>дБ** | **Eci<br>мкВ/м** | **Ri<br>м** |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Радиус требуемой контролируемой зоны (Ri) составляет ___ метра. Минимальное расстояние от ОТСС объекта до границы контролируемой зоны составляет ___ метра.

**Вывод:** Защищенность ОТСС от утечки конфиденциальной информации по каналу ПЭМИ не обеспечивается, так как рассчитанный требуемый радиус контролируемой зоны превышает минимальное расстояние от ОТСС до ее границы. Необходимо применение средств защиты.

Таблица 4 – Результаты измерений и расчета зон активного зашумления устройства защиты «Соната-Р2»

| **f i МГц** | **Егш i дБ** | **Еш i дБ** | **Ес гш i мкВ/м** | **Ri (с ГШ) м** |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

**Вывод:** . Зоны активного зашумления, рассчитанные для устройства защиты «Соната-Р2», зав. № _____, превышают требуемый радиус контролируемой зоны для всех составляющих спектра информативного сигнала. Защищенность ОТСС от утечки конфиденциальной информации по каналу ПЭМИ обеспечивается.

## Измерение наводок ПЭМИ на линии и коммуникации

Таблица 5 – Состав измерительного оборудования для измерения наводок

| Наименования средств измерений и вспомогательного оборудования | Тип | Заводской номер | Диапазон частот | Дата очередной поверки |
|---|---|---|---|---|
| Средства измерений | | | | |
| ПАК «Легенда» в составе: | | | | |
| Анализатор спектра | Agilent | | | октябрь 2017 г. |
| Пробник | Я6-122 | | | октябрь 2017 г. |
| Вспомогательное оборудование | | | | |
| Генератор | R&S SMB 100A | | | октябрь 2017 г. |

Результаты измерений наведенного информативного сигнала и расчета значения допустимого пробега линий (коммуникаций) до границы контролируемой зоны приведены в таблице 6

Таблица 6 – Результаты измерений и расчета наводок

| f i МГц | U(с+ш)i дБ | Uшi дБ | Uci дБ | U1изм мкв | U2изм мкв | Кпi дБ/м | Rін м | Rкз м |
|---|---|---|---|---|---|---|---|---|
| Линии электропитания и заземления \\ Вывод информации на экран монитора | | | | | | | | |

Радиус требуемой максимальной длины пробега исследуемой линии, на которой возможно выделение информативного сигнала (Rін) составляет ___ метра. Реальный пробег исследуемой линии (Rкз) до границы контролируемой зоны составляет __ метра.

**Вывод:** Защищенность конфиденциальной информации, обрабатываемой ОТСС от ее утечки за счет наводок информативного сигнала на линии и коммуникации, выходящие за пределы контролируемой зоны, не обеспечивается, так как максимальная длина пробега исследуемых линий, на которой возможно выделение информативного сигнала, больше реального их пробега до границы контролируемой зоны. Необходимо применение средств защиты.

Таблица 7 – Результаты измерений и расчета зон активного зашумления устройства защиты «Соната-Р2» в линиях и коммуникациях

| f i МГц | Uгшi дБ | Uшi дБ | Uс гшi дБ | U1изм мкв | U2изм мкв | Кпi дБ/м | Rін (с ГШ), м | Rін м |
|---|---|---|---|---|---|---|---|---|
| Линии электропитания и заземления \\ Вывод информации на экран монитора | | | | | | | | |
| | | | | | | | | |

**Вывод:** Радиус зоны активного зашумления устройства защиты «Соната-Р2», зав. № _____ в линиях и коммуникациях, выходящих за пределы контролируемой зоны, превышают требуемый радиус контролируемой зоны для всех составляющих спектра информативного сигнала. Защищенность конфиденциальной информации, обрабатываемой ОТСС, от ее утечки за счет наводок информативного сигнала на линии и коммуникации, выходящие за пределы контролируемой зоны, обеспечивается.

**Условные обозначения:**

fi, – измеренные частоты составляющих тест-сигнала, МГц;

Eoi – измеренный уровень напряженности электромагнитного поля при работе основного технического средства в тестируемом режиме, по электрической (магнитной) составляющей, мкВ/м;

Eшi – измеренный уровень напряженности электромагнитного поля помех по электрической (магнитной) составляющей, мкВ/м;

Eci – рассчитанный уровень напряженности электромагнитного поля, созданного информативным сигналом, по электрической (магнитной) составляющей, мкВ/м;

Ri – требуемый радиус контролируемой зоны для i - й составляющей спектра информативного сигнала при условии отсутствия ГШ;

Eгш i – измеренный уровень напряженности электромагнитного поля генератора шума по электрической (магнитной) составляющей, мкВ/м;

Ec гш i – рассчитанный уровень напряженности электромагнитного поля, созданного генератором шума, по электрической (магнитной) составляющей, мкВ/м;

Ri (с ГШ) – радиус зоны зашумления генератора шума для i - й составляющей спектра информативного сигнала, м;

U(с+ш)i – измеренное значение смеси обнаруженных компонент тест-сигнала и помехи в линии, дБ;

Uшi – измеренное значение помехи в линии, дБ;

Uсi – рассчитанное значение сигнала в линии, дБ;

U1 изм – напряжение специально созданного сигнала, измеренное на частоте fi исследуемой линии в непосредственной близости от ОТСС, мкВ;

U2 изм – напряжение специально созданного сигнала, измеренное на частоте fi исследуемой линии на некотором удалении от ОТСС, мкВ;

Кпi – коэффициент погонного затухания наведенных сигналов в исследуемой линии, дБ/м;

Riн– максимальная длина пробега исследуемой линии, на которой возможно выделение информативного сигнала при условии отсутствия генератора шума, м;

Rкз – реальный пробег исследуемой линии до границы контролируемой зоны, м;

Uгш i – измеренное значение сигнала генератора шума в линии, дБ;

Uш i – помеха в линии, дБ;

Uс гш i – рассчитанное значение сигнала генератора шума в линии, дБ;

U1 изм – напряжение специально созданного сигнала, измеренное на частоте fi исследуемой линии в непосредственной близости от ОТСС, мкВ;

U2 изм – напряжение специально созданного сигнала, измеренное на частоте fi исследуемой линии на некотором удалении от ОТСС, мкВ;

Кпi – коэффициент погонного затухания наведенных сигналов в исследуемой линии, дБ/м;

Riн (с ГШ) – максимальная длина пробега исследуемой линии, на которой возможно выделение информативного сигнала при условии применения генератора шума, м.

Роман Александрович **Васильев**
Леонид Юрьевич **Ротков**

# ОБНАРУЖЕНИЕ ПЭМИН С ПОМОЩЬЮ ПАК «ЛЕГЕНДА»

***Учебно-методическое пособие***

Федеральное государственное автономное образовательное учреждение высшего образования «Нижегородский государственный университет им. Н.И. Лобачевского».
603950, Нижний Новгород, пр. Гагарина, 23.