МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

СЕВЕРО-КАВКАЗСКИЙ ФИЛИАЛ ОРДЕНА ТРУДОВОГО КРАСНОГО ЗНАМЕНИ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
СВЯЗИ И ИНФОРМАТИКИ»

И.В.РЕШЕТНИКОВА

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Учебное пособие

Ростов-на-Дону
2022

УДК 004
ББК 32.97
Ж 86

Решетникова И.В. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ . *Учебное пособие*. – Ростов-на-Дону: СКФ МТУСИ, 2022. – 52 с.

В учебном пособии, предназначенном для студентов, изучающих дисциплины «Программно-аппаратные средства защиты информации» изложены краткие теоретические сведения об особенностях построения систем защиты информации.

Изложен порядок проведения изучения построения систем защиты информации, содержание требования к отчету, приведен перечень контрольных вопросов по проведенному лабораторному исследованию.

Лабораторные исследования позволят студентам, обучающимся по направлениям подготовки бакалавров: 10.03.01 «Информационная безопасность» более глубоко изучить дисциплины «Программно-аппаратные средства защиты информации , закрепить полученные знания, а также получить практические навыки в работе с информационно-коммуникационными системами.

Пособие также будет интересно широкому кругу студентов технических специальностей и инженерам, интересующимся принципами построения систем передачи информации.

Рецензенты:
Ведущий научный сотрудник «Ростовский-на-Дону НИИ радиосвязи», д.т.н., доцент А.В. Елисеев;
Ведущий научный сотрудник «Ростовский-на-Дону НИИ радиосвязи», д.т.н. доцент В.А. Погорелов;

СОДЕРЖАНИЕ

1 Организация аттестации выделенного помещения по требованиям безопасности информации

1.1 Краткие теоретические сведения

Аттестация защищаемого помещения по требованиям безопасности информации предшествует началу обработки подлежащей защите информации и вызвана необходимостью официального подтверждения эффективности комплекса используемых на конкретном объекте информатизации мер и средств защиты информации.

Целью защиты объекта информатизации является предотвращение утечки информации по техническим каналам. Опыт организации специальных исследований говорит, что, с целью сокращения времени, перед проведением подготовительного этапа Заказчик должен подготовить следующие исходные данные:

1. Атрибуты объекта – т.е. полный адрес Заказчика, полное наименование объекта, а также его размещение (этаж, Х или название помещения).
2. Контролируемая зона (КЗ) – Реквизиты документа, устанавливающего КЗ. Кроме этого должна быть дана планировка, определяющая размещение объекта на генплане, его месторасположение с указанием названия улиц, скверов и т.п. Минимальное расстояние от объекта до границы КЗ.
3. Установленная категория объекта.
4. Граничащие помещения (спереди, сзади, справа, слева, снизу, сверху).
5. Ограждающие конструкции (спереди, сзади, справа, слева, сни-зу, сверху). Необходимо по каждому направлению указать вид материала конструкции и его толщину. Если конструкция сложная, т.е. исполнение в несколько слоев, необходимо перечислить все слои с указанием толщины каждого. Указать наличие сквозных щелей и пустот в ограждающих конструкциях.

Например: ограждающими конструкциями помещений являются железобетонные стены здания толщиной 500 мм (монолитный железобетон) и внутренние перегородки в капитальном исполнении (в один кирпич, 250 мм). Перегородка комнаты отдыха кабинета заместителя руководителя с залом заседаний выполнена из двух слоёв оргалита (6 мм) на деревянном каркасе (брус 5-50 мм). Перекрытия пола и потолка железобетонные (стандартные плиты пустотелого железобетона 305 мм).

6. Наличие фальшпола и фальш потолка (с указанием модели материала, толщины и расстояния от перекрытия до фальшпола/потолка).
7. Описание дверей помещения (материал, размеры, двойные / одинарные, одностворчатые/двухстворчатые, наличие порога и его высо- та).
8. Описание окон помещения (материал, размеры, двойные/одинарные, толщина остекления). Куда выходят окна – внутренний двор, улица и т.п.
9. Система отопления. Где расположен тепловой пункт. Как по- строена система отопления (тип радиаторов отопления, как осуществляется подача (розлив) теплоносителя, количество радиаторов, количество стоя- ков отопления в помещении).
10. Система водоснабжения (описание аналогично системе отопления).
11. Система вентиляции(количество вентиляционных каналов, сечение коробов и их местопрохождение с указанием ближайших выходов в другие

помещения).

12. Описание применяемых средств защиты (марка, вид аппаратуры защиты, места установок датчиков и т.п.).

На подготовительном этапе проводится качественная оценка вибро-и звукоизоляции помещения с целью определения наиболее вероятных разведопасных направлений. Анализируются архитектурно-планировочные решения помещения, конструктивные особенности его ограждающих конструкций (стен, перекрытий, дверей, окон) и инженерно-технических систем. Обследуются коммуникации трубопроводов различных систем жизнеобеспечения, выявляются неоднородности в ограждающих конструкциях, обследуются конструктивные особенности элементов отделки.

Уточняются пространственные соотношения ограждающих конструкций помещения и элементов технических систем относительно установленной границы контролируемой зоны и относительно прилегающих к контролируемой зоне зданий, строений и пр.

Оценивается (или уточняется) степень секретности речевой информации (категории объекта защиты) и определяется необходимое значение нормированного показателя противодействия акустической речевой разведке, на соответствие которому необходимо проводить инструментальный контроль.

Уточняются условия речевой деятельности в контролируемом помещении. Проводится слуховой (качественный) контроль звукоизоляции ограждающих конструкций путем прослушивания сигналов, формируемых в контролируемом помещении. В качестве таких сигналов рекомендуется использовать естественную речь, записанную, например, на диктофон.

1.2 Лабораторное исследование № 1. Организация аттестации выделенного помещения по требованиям безопасности информации

Цель исследования:

изучить общие характеристики и требования к организация аттестации выделенного помещения по требованиям безопасности информации

Время работы: 4 часа

Задания на выполнение лабораторного исследования

(В работе составляются самостоятельно путем осмотра выделенного помещения и прилегающей территории)

Представитель ОАО «ХХХ», как представитель Заказчика, представил следующие исходные данные на исследуемое помещение:

1. Атрибуты объекта – ОАО «ХХХ», г. С-Петербург, ул. Строителей, дом №.., расположено на первом этаже 3-х этажного здания. На 2-ом и 3-ем этажах расположены сторонние организации. Имеется общая охраняемая территория. Допуск посторонних лиц и автомашин только с согласия руко- водителя ОАО «ХХХ» и руководителей сторонних организаций. Все сотрудники ОАО «ХХХ» имеют допуск не ниже третьего. Сторонние организации с гостайной не работают. В ОАО «ХХХ» имеется одно выделенное помещение (ВП) – кабинет руководителя. Планируется

аттестовать в качестве выделенного помещения – помещение для переговоров.

2. Контролируемая зона (КЗ) объекта проходит по ограждающим конструкциям третьего этажа, за исключением лестницы на верхние этажи. Исследуемое ВП–переговорная-граничит с КЗ по одной стене, накоторой расположено одно окно и дверь, и по потолку. Средства звукоусиления в переговорной отсутствуют. Источник речи не локализован.

3. Помещению планируется установить 2-уюкатегорию.

4. Граничащие помещения (спереди, сзади, справа, слева, снизу, сверху).

5. Ограждающие конструкции:

Стены 1 и 2 выполнены из кирпича. Толщина 2,5 кирпича. Внутренняя штукатурка толщиной 1см.

Боковые стены 3 и 4 выполнены из кирпича. Толщина 1 кирпич.

Внутри и снаружи штукатурка толщиной 1см.

Пол и потолок выполнены из стандартных бетонных плит перекрытия толщиной 30 см. Подвала нет. Сквозных щелей и пустот не обнаружено. Пол деревянный на лагах, покрыт линолеумом. Фальшпотолканет.

6. Двери двойные с тамбуром. Ширина тамбура – 0,5 м. По пери- метру каждой двери проложен уплотнитель. Двери тяжелые деревянные. Дверные коробки отделены друг от друга и от стены резиновыми уплотнителями. Дверь выходит на границу КЗ.

7. Окно пластиковое в специальном исполнении. Рама окна отделе- на от стены резиновыми прокладками. Окно граничит сКЗ.

8. В помещении имеется одна батарея отопления. Трубы системы отопления выполнены из металлопластика. Ввод трубы системы отопления осуществлен со второго этажа, выход трубы идет под пол. Тепловой пункт размещен за пределами КЗ. Таким образом, система отопления имеет вы- ход за пределы КЗ.

9. Система вентиляции выполнена в виде вентиляционных коробов и имеет ближайший выход в общий коридор первого этажа и затем выходит на второй и третий этаж (по легенде).

10. На элементах ограждающих конструкций и инженерных коммуникаций имеются средства активной защиты.

Методика проведения осмотра помещений

Ниже приведены общие рекомендации по поиску устройств негласного съема информации. Всю процедуру поиска можно условно разбить на несколько этапов:

- Подготовительный этап;
- физический поиск и визуальный осмотр;
- обнаружение радио-закладных устройств;
- выявление технических средств с передачей информации по токоведущим линиям;
- обнаружение ЗУ с передачей информации по ИК-каналу;
- проверка наличия акустических каналов утечки информации.

Подготовительный этап

Предназначен для определения глубины поиска, а также формирования перечня и порядка проводимых мероприятий Он включает в себя следующие элементы:

1. Оценку возможного уровня используемых технических средств.

Объем проводимых мероприятий существенным образом зависит от того, в

чьих интересах они проводятся. Одно дело - проверка помещений представителей малого бизнеса, другое - крупнейших корпораций или государственных учреждений, так как при этом значительно отличаете уровень выявляемых устройств, который может колебаться от примитивных радио-микрофонов до специальной профессиональной техники, и, соответственно, меняется уровень привлекаемой поисковой техники.

2. Анализ степени опасности, исходящей от своих сотрудников и представителей соседних организаций. Хороший способ проверки - организация контролируемой утечки информации. Это может быть сделано посредством «случайного» присутствия по стороннего человека, «забытого» документа или другим доступным способом.

3. Оценку возможности доступа посторонних лиц в помещения.

4. Изучение истории здания, в котором планируется проводить поисковые мероприятия.

Оценивается возможность установки закладок как во время строительства, так и оставления их в наследство от предыдущих обитателей.

5. Определение уровня поддерживаемой безопасности в соответствии с экономическими возможностями и степенью желания заказчика, а также фактической необходимостью.

6. Выработку плана действий, который должен отвечать следующим условиям:

- время поиска должно приходиться на рабочие часы, когда ЗУ активизированы;
- должны быть созданы условия, провоцирующие к действию возможно внедренные «жучки», поскольку в них могут быть использованы как схемы VOX, включающие устройства только при определенном уровне акустического сигнала, так и системы дистанционного управления (проведение фиктивных, но правдоподобных деловых переговоров — хороший повод, чтобы побудить противоположную сторону активизировать свои устройства);
- должна быть обеспечена скрытность проводимыхмероприятий
- если есть необходимость ведения своей «контрразведывательной» игры, то следует помнить, что разговоры с коллегами и заказа ком, приход, развертывание аппаратуры, характерный шум поиска раскрывают содержание и результат проводимых мероприятий;
- неожиданность - поиск следует проводить регулярно, но через случайные промежутки времени.

Физический поиск и визуальный осмотр

Физический поиск и визуальный осмотр является важным элементом выявления средств негласного съема информации, особенно таки как про- водные и волоконно-оптические микрофоны, пассивные и полуактивные радио-закладные устройства, дистанционно управляемые «ждущие» устройства и другие технические средства, которые невозможно обнаружить с помощью обычной аппаратуры.

Помните: физический поиск является базой для любой поисковой методики. Будьте предельно внимательны, смотрите тщательно!

Проведение поисковых мероприятий следует начинать с подготовки помещения, подлежащего проверке.

1. Необходимо закрыть все окна и занавески для исключения визуального

контакта.

2. Включить свет и все обычные офисные устройства, характерные для данного помещения.

3. Включить источник «известного звука» (тестового акустического сигнала) в центре зоны контроля. Во время поиска он будет выполнять важные функции: маскировать большинство шумов, производимых во время физического поиска; работать как источник для звуковой обратной связи, необходимой для выявления радио-микрофонов; активизировать устройства, оснащенные системой VOX. Источник «известного звука» не должен настораживать противоположную сторону, следовательно, это может быть любой плейер. Необходимо только помнить, что лучшие результаты достигаются при использовании аппаратуры средних размеров. Это объясняется оптимальными размерами громкоговорителя. Выберите наиболее уместную в данной ситуации запись, будь то музыка, бизнес - семинар или курс самообучения. Подберите соответствующую длительность, поскольку качественный поиск может занять много часов.

Примечание: в качестве источника «известного звука» не рекомендуется использовать радиоприемник, поскольку эту же станцию может поймать и ваша поисковая аппаратура, что может привести к ошибке и радио- станция будет зафиксирована как нелегальный радиопередатчик.

4. За пределами зоны контроля (в незащищенной комнате/зоне) как можно более бесшумно разверните вашу аппаратуру. Незащищенная зона - это место, которое не вызывает интереса у противоположной стороны и не контролируется ею, поэтому ваши действия останутся скрытыми.

5. Установите обычный уровень радиоизлучения окружающей среды перед поиском в зоне контроля.

Основные процедуры поиска

Визуально, а также с помощью средств видеонаблюдения и металлодетекторов, обследуйте все предметы в зоне контроля, размеры которых достаточно велики для того, чтобы можно было разместить в них технические средства негласного съема информации. Тщательно осмотрите и вскройте, в случае необходимости, все настольные приборы, рамы картин, телефоны, цветочные горшки, книги, питаемые от сети устройства (компьютеры, ксероксы, радиоприемники и т. д.).

Для поиска скрытой проводки обследуйте плинтуса и поднимите ковровые покрытия. Тщательно осмотрите потолочные панели, а также все устройства, содержащие микрофоны, магнитофоны и камеры.

С особой тщательностью обследуйте места, где ведутся наиболее важные переговоры (обычно это стол с телефоном). Большинство нелегальных устройств располагаются в радиусе 7 м от этого места для обеспечения наилучшей слышимости и (или) видимости.

Если вы при этом используете металлодетектор, то скрупулезно выполняйте требования его инструкции на эксплуатацию.

Особо следует обратить внимание на проверку телефонных линий, сетей пожарной и охранной сигнализации. Следует обязательно разобрать телефонный аппарат, розетки и датчики и искать детали, непохожие на обычные, с разноцветными проводами и спешной или неаккуратной установкой. Затем осмотрите линию от аппарата (датчика) до стены и, удалив стенную панель, проверьте, нет ли за ней нестандартных деталей.

Проведите физический поиск в коммутационных панелях и коммуникационных каналах, в случае необходимости используйте эндоскопические и портативные телевизионные средства видеонаблюдения. Проверьте места входа/выхода проводов внутри и снаружи здания.

С целью облегчения последующих поисковых мероприятий после завершения всех работ скрытно пометьте шурупы на стенных панелях, сетевых розетках, телефонных корпусах и других местах, куда могут быть установлены закладки. Тогда при проведении повторных проверок видимые в ультрафиолетовых лучах метки покажут нарушение целостности ранее обследованного объекта, если оно имело место, а соответствующие записи в вашем журнале проверок помогут сориентироваться в будущей работе. Для контроля изменений в окружающих устройствах очень удобны ультрафиолетовыемаркеры.

При проведении поиска ЗУ в автомобиле тщательно осмотрите не только салон, но и раму автомашины, багажник и т. п., внимательно про- верьте цепи, имеющие выход на автомобильную антенну. При проведении этих операций досмотровые портативные телевизионные системы также могут оказаться очень полезными.

Порядок выполнения работы

Составить самостоятельно (или получить у преподавателя) документацию на контролируемое помещение, изучить ее, определить возможные разведопасные направления и возможные виды разведки.

Изобразить план-схему исследуемого помещения.

На основании нижеприведенной методики, составить план проведения визуального осмотра помещения и выявить объекты, требующие при обследовании использования имеющихся средств видеонаблюдения и металодетектора.

Сделать выводы по результатам проделанной работы и подготовить отчет.

Содержание отчета

При подготовке отчета по лабораторной работе необходимо:

Придерживаться рекомендаций, указанных в Лабораторном практикуме

Выполнить требования стандартов по оформлению отчетов (ЕСКД, ЕСПД) в соответствии с образцами типовых форм отчетных документов.

Использовать рабочие материалы, подготовленные на этапе, предшествующем выполнению лабораторной работы.

Предъявить отчет преподавателю для подтверждения факта выполнения лабораторной работы.

Выводы по проведенному исследованию.

Контрольные вопросы

При сдаче отчета по лабораторному исследованию студент должен быть готов ответить на следующие вопросы:

1. Средства акустического контроля.
2. Аппаратура для съема информации с окон.
3. Специальная звукозаписывающая аппаратура.
4. Микрофоны различного назначения и исполнения.

5. Электросетевые подслушивающие устройства.
6. Приборы для съема информации с телефонной линии связи и сотовых телефонов.
7. Специальные системы наблюдения и передачи видеоизображений.
8. Специальные фотоаппараты.
9. Приборы наблюдения в дневное время и приборы ночного видения.
10. Специальные средства радиоперехвата и приема ПЭМИН и др

2 Загрузка заданного радиодиапазона и обнаружение радиозакладных устройств в защищаемом помещении

1.2 Краткие теоретические сведения

Для обнаружения радиозакладок применяют индикаторы электромагнитного поля, частотомеры, нелинейные локаторы, рентгенотелевизионную аппаратуру и специальные сканирующие приемники. С их помощью осуществляется поиск и фиксация рабочих частот радиозакладок, а также определяется их местонахождение.

Если радиозакладки выключены в момент поиска и не излучают сигналы, то для их поиска, а также для поиска микрофонов подслушивающих устройств и минимагнитофонов, применяют специальную рентгеновскую аппаратуру и нелинейные локаторы, излучения которых проникают сквозь стены, потолки, пол, мебель, портфели, утварь – в любое место, где могут быть спрятаны радиозакладка, микрофон.

В тех случаях, когда нет приборов либо нет времени на поиск радиозакладок, можно пользоваться генераторами помех для подавления закладочных устройств.

К средствам оперативного контроля, то есть средствам обнаружения факта использования радиозакладки, а иногда и ее локализации, относятся индикаторы или детекторы поля, частотомеры и некоторые поисковые приемники. Основное их преимущество – способность выявлять источники излучения или передающие устройства независимо от типа применяемой в них модуляции. Принцип поиска заключается в выявлении максимума уровня излучения в помещении.

Далее представлено краткое описание комплексов.

Комплекс «RS turbo Mobile-L». Компьютеризированный комплекс «RS turbo Mobile-L» предназначен для быстрого обнаружения, идентификации, определения местоположения (локализации) и нейтрализации подслушивающих устройств и других источников несанкционированных излучений, передающих сигналы по радиоканалу, проводным линиям и в оптическом ИК-диапазоне.

В состав комплекса «RS turbo Mobile-L» входят:

− радиоприемное устройство на базе AR5000 с встроенными контроллером RS turbo (или RS digital) и конвертором RS/L plus;

− антенна RS/A;

− двухканальная акустическая система;

− портативный персональный компьютер (ноутбук) с операционной системой Windows XP;

− управляющая программа.

Комплекс «RS turbo Mobile-L» имеет удобные программные средства накопления, обработки, анализа и хранения данных, регистрации демодулированных сигналов и идентификации источников излучений. Основная задача управляющей программы комплекса – облегчить оператору анализ поступающей информации о многочисленных источниках излучений.

В процессе просмотра заданных диапазонов и обработки полученных данных программа составляет списки с параметрами и классификационными признаками обнаруженных сигналов. Затем, с помощью средств анализа программы оператор может детально исследовать характеристики интересующего сигнала, например, его спектр, гармонический состав или реак цию на импульсы акустического

зондирования и получить необходимую информацию для принятия обоснованного решения о наличии в помещении подслушивающих устройств.

Сохраняя все положительные качества изделий серии Turbo (компактность, надежность, простоту освоения и эксплуатации), эта система отличается целым рядом новых возможностей и, прежде всего, скоростью работы. Так время полного обзора радиодиапазона до 2,6 ГГц при отсутствии априорных данных о его загрузке составляет от 0,5 до 2-х мин. Оболочка управляющей программы работает в среде Windows 95/98/NT/2000/XP.

Комплекс «RS turbo Mobile-L» в автоматическом режиме с высокой достоверностью выявляет в контролируемом помещении радиомикрофоны и телефонные радиопередатчики, с достаточной точностью указывает место положение обнаруженных микрофонов с обычной частотной модуляцией.

Комплекс «RS turbo» выполняет все функции комплекса «RS turbo Mobile-L», однако позволяет сканировать радиодиапазон вплоть до 12 ГГц с дополнительным конвертером. С помощью конвертера RS/L комплекс обнаруживает сигналы, которые передаются подслушивающими устройствами по сети электропитания или любым проводным линиям в диапазоне от 0,6 кГц до 10 МГц, а также в инфракрасной части оптического диапазона. Одновременно комплекс с достаточной точностью указывает местоположение обнаруженных радиомикрофонов с обычной частотной модуляцией, а при необходимости нейтрализует их излучения с помощью программируемых генераторов сигналов RS/N.

Для выполнения базовых операций поиска подслушивающих устройств в радиоканале достаточно подключить к контроллеру персональный компьютер, сканирующий радиоприемник и двухканальную акустическую систему. Комплекс «RS turbo» работает со сканерами AR5000, AR8600 и AR8200 японской фирмы AOR Ltd. Для управления может использоваться любой компьютер с операционной системой Windows 95/98/2000/NT и одним свободным последовательным портом RS232. В случае необходимости конфигурацию системы легко расширить с помощью дополнительных устройств, разработанных для комплексов радиоконтроля. В частности, для анализа проводных и оптических каналов используется конвертер RS/L, а для нейтрализации выявленных источников радиоизлучений – программируемый генератор RS/N (до 1800 МГц). С помощью антенного коммутатора RS/K комплекс может контролировать радиообстановку с помощью нескольких антенн, предназначенных для различных диапазонов или установленных в пространственно разнесенных помещениях. Контроллеры акустических систем RS/Z используются для обнаружения и определения местоположения радиомикрофонов методом акустического зондирования в удаленных помещениях.

Основные операции.

Сканирование – это базовая операция, которая предшествует обнаружению, классификации и идентификации источников излучений (сигналов). В процессе сканирования выявляются занятые участки исследуемого частотного диапазона и оцениваются спектры присутствующих в нем сигналов. Частота настройки сканирующего приемника изменяется дискретно с фиксированным шагом 8 МГц и на каждом шаге вычисляемый контроллером «RS turbo» результат измерений уровней, принимаемых во всем спектре сигналов, заносится в компьютер. В анализаторе «RS turbo» быстрое сканирование выполняется с широким (200 кГц) или узким (12,5 кГц)шагом. По результатам сканирования компьютер формирует спектральную

панораму исследуемого диапазона, в которой каждому значению частоты настройки соответствует измеренный спектр сигнала.

Операции сканирования выполняются в порядке их размещения в списке операций задания. Это дает возможность в первую очередь просматривать те участки спектра, где вероятность найти излучения несанкционированных источников выше. Один частотный диапазон можно включать в задание несколько раз, чтобы реализовать различные алгоритмы идентификации и классификации излучений.

Выполнив один цикл сканирования, программа составляет таблицу, в которой каждому значению частоты настройки ставится в соответствие измеренный последовательным анализатором контроллера «RS turbo» спектр сигналов в полосе анализа 8 МГц, снятый для сигналов, превышающих заданный порог, с разрешением 12.5 кГц. Эта таблица называется спектральной панорамой. Программа комплекса «RS turbo» позволяет формировать спектральные панорамы с учетом данных, полученных в ходе текущего и любого числа предшествующих циклов сканирования. После выполнения первого цикла сканирования таблица спектральной панорамы сохраняется в памяти компьютера. На следующем цикле формируется новая (текущая) таблица, а значения уровней в таблице предыдущей панорамы модифицируются в соответствии с выбранным методом обработки:

−обновление (в таблицу записывается новое значение, а старое стирается);

−накопление (в таблицу записывается больший из двух уровней);

−усреднение (в таблицу записывается среднее двух уровней).

Первый из перечисленных методов обычно используется в процессе обнаружения излучений, а следующие два – для сбора данных, характеризующих обстановку в заданных диапазонах при продолжительных наблюдениях со статистической обработкой результатов измерений. Накопление максимальных значений обеспечивает наиболее полный учет всех излучений, появлявшихся за время наблюдения. Накопление средних значений позволяет при большом числе циклов сканирования свести к нулю уровни случайных сигналов, например, импульсных помех. Текущая панорама отображается на экране зеленым цветом и показывает уровни, измеренные в текущем цикле сканирования.

Данные, полученные в результате обработки уровней предшествующих циклов сканирования, отображаются красным цветом и располагаются на заднем плане. В любой момент после остановки сканирования таблица панорамы, отражающая результаты выполненных циклов сканирования, может быть сохранена в виде файла (файл панорамы спектра, расширение pan) с заданным программой или пользователем именем. Спектральные панорамы, характеризующие обстановку в заданном диапазоне частот, называются диаграммами загрузки диапазона. Такие панорамы на экране отображаются синим цветом и используются в качестве фона для обнаружения «неизвестных» излучений.

При необходимости данные, отражающие результаты предшествующих циклов сканирования, могут быть удалены из списка командой очистки. При этом в исходную таблицу панорамы записываются нулевые уровни. Если программа работает с несколькими заданиями, то таблица уровней составляется и модифицируется для каждого из них. При этом на экране отображаются панорамы спектров активного задания. В процессе анализа проводных линий с помощью конвертора «RS/L plus» текущий спектр зеленого цвета выводится на экран на фоне спектра красного цвета, полученного на предыдущем цикле.

Для повышения скорости работы комплекс «RS turbo» выполняет сканирование с помощью последовательного анализатора спектра с разрешением 12,5 КГц с шагом 8 МГц. После запуска сканирование ведется с указанным шагом по сетке частот. Начальная и конечная частоты указанного в задании диапазона заменяются ближайшими частотами этой сетки. На каждом шаге контроллер «RS turbo» измеряет уровни принимаемых сигналов, т.е. снимает спектр на широкополосном выходе промежуточной частоты приемника, и передает данные в компьютер.

Обнаружение – базовая операция выявления всех радиоизлучений (сигналов), уровень которых в заданном диапазоне превосходит установленное в задании пороговое значение (порог обнаружения). В процессе обнаружения программа оценивает параметры сигнала: ширину спектра, максимальный уровень, несущую частоту, а также классифицирует обнаруженные излучения, распределяя их по группам в соответствии с определенными признаками. Обнаруженные излучения автоматически классифицируются программой RS turbo по следующим признакам:

− «известные» и «неизвестные»;

− «обнаруженные ранее» и «вновь появившиеся»;

− «стандартные» и «нестандартные».

Анализ. Операции анализа необходимы для выявления среди множества обнаруженных сигналов «опасных» излучений, которые могут быть созданы передатчиками подслушивающих устройств. Идентификация (опознавание) сигналов подслушивающих устройств в программе «RS turbo» выполняется автоматически или в ручном режиме с помощью следующих операций:

− анализ гармонического состава излучений;

− корреляционный анализ откликов на акустические импульсы;

− спектральный анализ;

− временной и спектральный анализ сигналов на выходе демодулятора.

Кроме того, в процессе анализа откликов на импульсы акустического зондирования программа измеряет расстояния от колонок акустической системы комплекса до микрофона и определяет местоположение микрофона в помещении (локализация источника излучения).

1.2 Лабораторное исследование № 2. Загрузка заданного радиодиапазона и обнаружение радиозакладных устройств в защищаемом помещении

Цель исследования:

изучить общую методику обнаружения радиозакладок применяют индикаторы электромагнитного поля, частотомеры, нелинейные локаторы, рентгенотелевизионную аппаратуру и специальные сканирующие приемники. С их помощью осуществляется поиск и фиксация рабочих частот радиозакладок, а также определяется их местонахождение.

Время работы: 6 часов

Задания на выполнение лабораторного исследования

Ознакомиться с видами радиозакладок и изучить методы их обнаружения.

Изучить работу комплексов в режиме обнаружения радиозакладок.

Произвести настройку программы для работы в режиме «Радио».
Выполнить один или несколько циклов сканирования заданного радиодиапазона. Обнаружить излучения без учета априорных данных за один цикл сканирования.

Порядок выполнения работы

Посмотреть и проанализировать списки обнаруженных сигналов.
Для интересующего сигнала выполнить:
− спектральный анализ сигналов излучений;
− анализ гармонического состава сигналов излучений;
− корреляционный анализ откликов на акустические импульсы.
Выявить наличие радиозакладного устройства в контролируемом помещении.
Сделать выводы по результатам проделанной работы и подготовить отчет.

Подготовка отчета

Содержание отчета

Отчет должен содержать:
1. Цель работы
2. Рабочие материалы, подготовленные на этапе, предшествующем выполнению лабораторной работы.
3. Предъявить отчет преподавателю для подтверждения факта выполнения лабораторной работы.
4. Скриншоты с кратким описанием основных технических характеристик для каждого типа.
5. Результаты сравнительного анализа с аналогичным по функционалу двумя другими типами кабельной продукции из предложенного списка или выбранных студентом самостоятельно.
6. Выводы по проведенному исследованию.

Контрольные вопросы

При сдаче отчета по лабораторному исследованию студент должен быть готов ответить на следующие вопросы:

Приведите определение закладочного устройства.
Перечислите демаскирующие признаки автономных некамуфлированных акустических закладок.
Перечислите демаскирующие признаки полуактивных акустических радиозакладок.
Какие технические средства применяют для выявления радиозакладочных устройств?
Назначение комплекса «RS turbo Mobile-L».
Перечислите состав комплекса «RS turbo Mobile-«L.
Радиозакладки с каким видом модуляции обнаруживает комплексRS turbo?

3 Исследование детектора электромагнитного поля

3.1 Краткие теоретические сведения

Большую часть технических каналов утечки информации представляют собой каналы, получающие информацию, переносимую тем или иным видом промодулированного электромагнитного сигнала. Для передачи сигнала обязательно должно иметься передающее устройство (передатчик) того или иного вида. Наиболее часто радиозакладки работают в метровом, дециметровом и сантиметровом диапазонах на частотах 24...28, 64...70, 88...108,134... 174, 370...512, 1100... 1300 МГц. Для передач используют сигналы с амплитудной (АМ), частотной широкополосной (WFM) и узкополосной (NFM) модуляцией несущей. Ширина спектра излучаемого сигнала составляет при WFM 50...120 кГц, при АМ и NFM – 6...12 кГц, что позволяет значительно увеличить дальность передачи при наличии специального приемника. Для повышения скрытности используют также сложные шумоподобные сигналы, передатчики с псевдослучайной перестройкой несущей частоты и кодирование информации.

Одним из основных признаков наличия нелегального передатчика являются незарегистрированные радиоизлучения. Поэтому в арсенале средств обеспечения информационной безопасности важное место занимают устройства, предназначенные для обнаружения средств несанкционированной передачи информации за пределы контролируемой зоны по радиоканалу. К числу простейших изделий этой группы аппаратуры относятся детекторы (индикаторы) электромагнитных излучений.

Такой индикатор поля обычно состоит из слабонаправленной антенны линейной поляризации, широкополосного радиоусилителя, амплитудного де-тектора и порогового устройства,что позволяет сего помощью обнаруживать работающие радиозакладки, использующие для передачи информации практически любые виды сигналов. Прибор регистрирует интегральный уровень электромагнитных излучений в месте приема. В случае, когда текущее значе-ние превысит установленный порог, соответствующий естественному уровню внешних излучений (фону), срабатывает световая или звуковая сигнализация. Радиозакладка обнаруживается в том случае, когда интенсивность создаваемого ею электромагнитного поля, превышает уровень фоновых излучений, что обычно бывает при внесении антенны индикатора в ближнюю зону передатчика. Для повышения способности обнаружения применяют аттенюаторы, полосовые и режекторные («вырезающие» определенныйд иапазон)фильтры, настроенные на частоты наиболее мощных внешних источников, и нейтрализующие влияние, например, местных телевизионных и радиовещательных станций.

Введение в схему индикатора усилителя низкой частоты и громкоговорителя дает возможность выделить на фоне внешних сигналов тестовый акустический сигнал, т.е. реализовать «акустическую завязку», суть которой состоит в следующем. Модулированное тестовым звуковым сигналом излучение принимается антенной индикатора, детектируется и после усиления поступает на вход динамика. Между микрофоном радиозакладки и динамиком индикатора устанавливается положительная обратная связь, проявляющаяся в виде характерного звукового сигнала, напоминающего свист.

Индикаторы электромагнитных излучений характеризуют следующие

параметры:

- Рабочий диапазон частот;
- чувствительность по напряженности электромагнитного поля;
- радиус обнаружения закладки с известной мощностью радиопередатчика;
- пределы регулирования порога чувствительности, методы ее повышения;
- наличие режима «акустическойзавязки»;
- типи ндикации;
- возможность прослушивания информации, передаваемой радио-закладкой;
- тип источника электропитания и время непрерывной работы от него в режимах обнаружения и поиска;
- габариты, масса, конструкция.

Простейшие детекторы поля (типа датчиков в устройствах обнаружения работы диктофонов) осуществляют включение индикации при превышении уровнем входного сигнала некоторого ранее установленного значения (порога). Индикация таких приборов, как правило, имеет смысл – Да/Нет. Более сложные индикаторы имеют регулятор чувствительности, с помощью которого устанавливается порог срабатывания. Такие приборы могут успешно применяться для обнаружения источников непрерывного электромагнитного излучения в ближней зоне (1 ... 2 м). К их достоинствам следует отнести малые габариты, простоту работы и невысокую стоимость. Недостатками являются низкие технические показатели, в частности невысокая чувствительность, а также отсутствие режимов идентификации источника сигнала (акустозавязка, измерение уровня сигнала, измерение частоты). Они могут при- меняться для грубой локализации источников излучения.

Профессиональные индикаторы предназначены для обнаружения ЗУ, путем проведения поисковых мероприятий, а именно, для поиска и точной локализации источников электромагнитных излучений. Они обладают высокими техническими характеристиками и более широкими функциональными возможностями. Имеют режим акустической завязки, регулятор чувствительности, полосовые фильтры, обладают высокой чувствительностью. Не- которые приборы имеют возможность производить замер частоты, позволяют измерять уровень сигнала, находящегося в ближней зоне, имеют тональную индикацию уровня сигнала, что дает возможность определить местоположение его источника по принципу – «тепло/ холодно». Такие приборы обладают большими преимуществами по сравнению с остальными типами индикаторов поля. Недостатком является довольно высокая цена и сложность работы с ними.

Если у индикатора есть функция радиочастотомера, то он фиксирует и частоту сигналов, превысивших установленный порог. В основу работы та- ких приборов положен принцип мгновенного «захвата» частоты радиосигнала с последующей обработкой микропроцессорным блоком, производящим

запись сигнала в устройство памяти, цифровую фильтрацию, проверку его на стабильность и когерентность. Значение частоты, измеряемой с точностью до единиц герц, отображается на индикаторе. В ряде приборов имеется воз-можность определения относительного уровня сигнала.

Присущие радиочастотомерам новые функциональные возможности

значительно расширили область и эффективность применения индикаторов электромагнитных излучений, сохранив, однако, существенный их недоста- ток – обнаружение источника излучения только в непосредственной близо- сти от него.

Общее описание устройства

Детектор электромагнитного поля ST107 предназначен для обнаруже-ния и локализации радиоизлучающих закладных устройств (ЗУ) и других технических средств, использующих для передачи информации радиоканал. Он способен работать в двух диапазонах – ВЧ (канал 1) и СВЧ (канал 2).

Составкомплектаизделия:

- основнойблок
- ВЧантенна
- СВЧантенна
- кабель USB
- зарядноеустройствопитания
- USB флеш-карта

Принцип действия ST107 основан на широкополосном детектировании электрического поля. Для измерения частот обнаруженного сигнала предусмотрен частотомер. Идентификация сигналов цифровых каналов передачи данных реализована на основе оригинальных алгоритмов анализа и обработки сигнала. Вывод графической информации осуществляется на цветной OLED дисплей, звукового продетектированного сигнала – на встроенный динамик или наушники. Управление осуществляется при помощи шестикнопочной пленочной клавиатуры, расположенной на основном блоке.

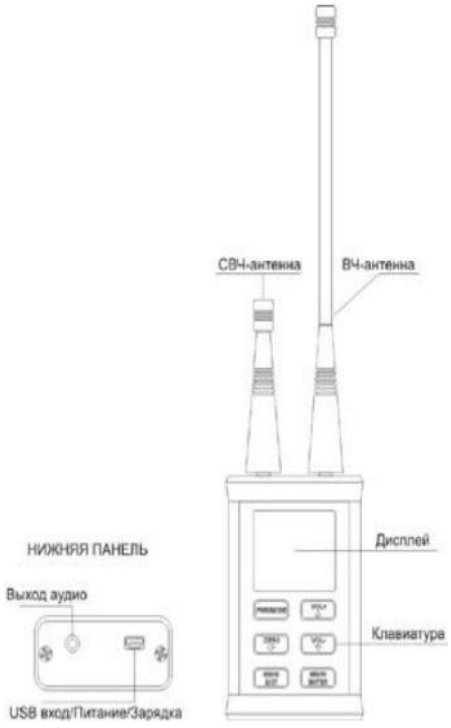


Рисунок.1 Общий вид ST107

На передней поверхности основного блока расположены цветной графический дисплей. На верхней поверхности размещены SMA разъемы подключения антенн 1-го (ВЧ) и 2-го (СВЧ) каналов. На нижней поверхности изделия расположены 3,5 мм разъем для подключения наушников и «miniUSB» разъем, используемый как для

питания/зарядки изделия, так и для подключения к РС.

Специальное программное обеспечение обеспечивает работу ST107 под управлением РС, что расширяет возможности пользователя по визуализации полученной информации, ее архивированию для последующего анализа.

Техническиепараметры:

- Внутренний источник питания – Li-pol аккумуляторнаябатарея
- Потребляемыйтокнеболее – 100мА
- Габариты – 92х57х26мм;
- Вес не более – 1,2 кг *Канал1.*
- Диапазончастот – 50-2500МГц
- Пороговаячувствительностьповходу – 60дБм
- Динамическийдиапазон – 60дБ;
- Чувствительностьчастотомера. – 40дБ
- Погрешностьизмерениячастоты – 0,01%;
- Частотасреза ФНЧ – 650МГц
- Ослабление вне полосы ФНЧ – 40 дБ. *Канал2.*
- Диапазончастот – 2400–7500МГц
- Пороговаячувствительностьповходу – 60дБм
- Динамическийдиапазон– 60дБ

Питание ST107 осуществляетсяот:

- встроенного Li-Polаккумулятора
- блокапитания/зарядногоустройства
- USB-портакомпьютера

Режимы работы детектора электромагнитного поля ST107

Прибор ST107 имеет два основных режима работы: «ПОИСК» и «МОНИТОРИНГ». Дополнительными режимами являются: «ПРОСМОТР ПРОТОКОЛА», «ОСЦИЛЛОГРАФ» и «САМОПИСЕЦ».

Режим «ПОИСК»

Этот режим предназначен для обнаружения и локализации РТС. Использование данного режима основано на визуальной оценке уровня сигнала на 32-сегментной шкале. Дополнительно используется раздельная индикация непрерывного и импульсного видов сигналов. Отображение идентифициро- ванных сигналов – GSM, DECT, BLUETOOTH, WLAN, а также индикация частоты, стабильного во времени сигнала. Обеспечена возможность акусти-ческого контроля посредством головных телефонов и встроенного динамика.

Режим «МОНИТОРИНГ»

Предназначен для автономной работы ST107 по предварительно остановленным условиям. Сохранение информации об обнаруженных сигналах осуществляется в энергонезависимой памяти изделия. (9 банков по 999 со-бытий). Возможна работа по расписанию.

Режим «ОСЦИЛЛОГРАФ»

Предназначен для просмотра осциллограммы продетектированного сигнала. Предусмотрена ручная и автоматическая установка амплитуды и развертки сигнала, а также маркерные измерения параметров, исследуется в работе как дополнительное задание наиболее подготовленным учащимся.

Режим «ПРОСМОТР ПРОТОКОЛА»

Предназначен для просмотра протокола событий, произошедших в ре-зультате

работы изделия в режиме «МОНИТОРИНГ» Предусмотрена воз- можность сортировки событий по времени наступления, длительности или уровню сигнала. Данный режим в работе не исследуется

Режим «САМОПИСЕЦ»

Данный режим показывает изменение уровня принимаемых сигналов в течение времени, задаваемого пользователем (от 30 секунд до 60 минут), и в лабораторной работе не исследуется.

Работа с детектором электромагнитного поля ST107 Органы управления и индикации

Индикация

Индикация результатов работы отображается на цветном экране с ре- шением160x128.

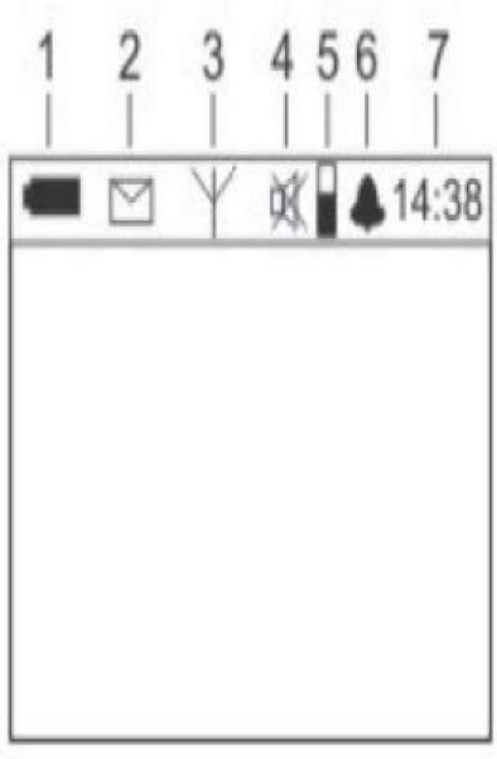


Рис. 2. Общая индикация

Общая индикация для двух основных режимов представлена на рис. 2.

1. уровеньзарядааккумуляторнойбатареи
2. индикаторсвязи сPC
3. включениеВЧ-модулей
4. отключениезвуковойиндикации
5. установленныйуровеньгромкости
6. индикатор работы по расписанию в режиме«МОНИТОРИНГ»
7. часы реального времени (если они установлены пользователем)
8. Управление

Включение и выключение ST107 осуществляется кнопкой PWR/MODE. При включении на дисплее кратковременно появляется сооб-щение: «ST107 Version X.X.», где X.X. – номер версии программного обес- печения. Функциикнопокуправленияприведены в таблице1.

Работа с прибором в различных режимах

Включение прибора ST107.

Подключите антенны к основному блоку. Включите изделие. В случае появления надписи «АККУМУЛЯТОР РАЗРЯЖЕН», зарядите аккумулятор. При работе от встроенной аккумуляторной батареи ее состояние отображает пиктограмма . Полностью заштрихованное изображение соответствует полностью заряженной аккумуляторной батарее. Полностью обесцвеченная и мигающая пиктограмма, обозначает, соответственно, состояние батареи, близкое к полному разряду. Время работы ST107 от полностью заряженной аккумуляторной батареи составляет около 5 часов. Чтобы осуществить заряд аккумулятора. Подключите к разъему USB основного блока зарядное устрой-ство или USB порт PC. Если изделие находится в выключенном состоянии, началу процесса зарядки соответствует надпись «ЗАРЯД АККМУЛЯТОРА». Если зарядка производится при включенном изделии, о процессе заряда сви-детельствуют бегущие сегментыпиктограммы.

Об окончании процесса зарядки говорят полностью заштрихованная пиктограмма и по завершении процесса зарядки аккумуляторной батареи на экране, на десять секунд появится надпись: «АККУМУЛЯТОР ЗАРЯЖЕН». Время полного заряда от зарядного устройства составляет 3 часа, от USB порта PC – около 5 часов. Установите необходимый режим работы индика- тора.

Режим «ПОИСК».

Вид экрана при первом включении представлен на рисунке 3.

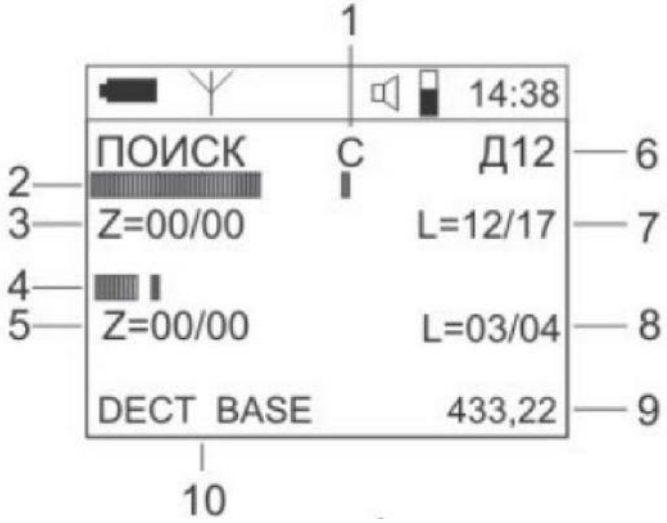


Рис.3. Экран ST107 в режиме «ПОИСК».

1. 32-х сегментный индикатор уровня 1-го канала для интегрального (белая шкала) и пикового (красная) значений мощностисигнала;
2. 32-х сегментный индикатор уровня 2-го канала для интегрального (белая шкала) и пикового (красная) значений мощностисигнала;
3. Начальное значение нулевого уровня для интегрального/пикового 1-гоканала;
4. Начальное значение нулевого уровня для интегрального/пикового 2-гоканала;
5. Значение измеряемого интегрального/импульсного уровня сигна- ла для 1-гоканала;
6. Значение измеряемого интегрального/импульсного уровня сигна- ла для 2-гоканала;

7. Включенные каналы (Д1, Д2, Д12 илиД12Ф);
8. Чувствительностьшкалиндикации;
9. Идентифицированныестандартыпередачиданных;
10. Значениечастотысигнала.

При работе только с одним каналом в нижней части дисплея отобража-ется график изменения уровня сигнала в зависимости от времени (от 30 сек. до 60 мин.).

Управление режимом.

Установка порога индикации относительно текущего уровня радиосиг-налов (вычитание фона) осуществляется при кратковременном нажатии на кнопку ZERO. В В этот момент, на дисплее, кратковременно появляется надпись «НОЛЬ» (позиция 7, рис. 3) и происходит обнуление индикаторов с отображением численного значения в позициях 3 и 4.

Численное значение текущего уровня сигналов относительно установ- ленного нулевого значения порога будет отображаться в позициях 5 и 6.

Отмена установки порога индикации с обнулением показаний в пози-ции 10 производится нажатием кнопки ZERO во время индикации «НОЛЬ» в позиции 3 (рисунок 3).

Установка чувствительности шкал индикации производится кратковре-менным последовательным нажатием на кнопку SENS/EXIT. При этом в по-зиции 8 (рисунок 2) индицируется выбранное значение чувствительности шкал индикации:

«Н» - низкая, вся шкала;

«С» - средняя, вся шкала;

«В» - высокая, вся шкал.

Управление громкостью осуществляется кнопками VOL+/VOL-.

Выбор количества каналов и включение фильтра низких частот описан в п. 6.7 таблицы 10 «Инструкции по эксплуатации».

Режим «МОНИТОРИНГ».

Вид экрана дисплея в данном режиме, при первом включении, пред-ставлен на рисунке 4.

Рис. 4. Экран ST107 в режиме «МОНИТОРИНГ».

1, 2 – Индикаторы уровня сигналов для 1 и 2 каналов соответственно; 3, 4 – Численное значение уровня тревоги;

7, 8, 9, 10 – Графическое отображение уровня тревоги; 5, 6 – Численное значение уровней сигналов;

Установки, соответствующие данному режиму, выбираются из МЕ- НЮ. В

этомрежимевсегдасоблюдаютсяусловия:

- шкалы индикации показывают уровни от 0 до 60dB;
- кнопки ZERO и SENS/EXITзаблокированы.

Управление режимом.

Первые 5 секунд после перехода в данный режим, будет наблюдаться обратный пятисекундный отсчет в правом верхнем углу экрана. Этот период времени предназначен для измерения пикового уровня электромагнитного поля. Данные измерений служат базисом для автоматической установки от-носительного уровня тревоги. При необходимости изменение данного значе-ния производится из МЕНЮ. Для использования расширенных критериев установки уровня тревоги необходимо воспользоваться возможностями про-граммного обеспечения ST107.

Правильность выбора определяется экспериментально, исходя из необ-ходимой дальности обнаружения и помеховой обстановки с использование легальных источников радиоизлучения (сотовый или DECT телефоны, ра- диостанция и т.д.).

В случае превышения сигналом установленного порога на экране по-

явится полноэкранная надпись «ALARM». Для предотвращения хаотичного заполнения протокола событий, при проведении подготовительных меропри-ятий, по умолчанию установлен запрет записи информации в «ПРОТОКОЛ СОБЫТИЙ», (знак «-» в позиции 3). Разрешение записи осуществляется че- рез МЕНЮ (см. п.6.7. Таблицы 2).

При выборе разрешения записи проконтролируйте появление в пози-ции 10 счетчика событий. «ООО» и мигание надписи МОНИТОР. Это будет означать, что при выполнении условий тревоги информация о событии будет фиксироваться в энергонезависимой памяти ST107.

События за один сеанс мониторинга записываются в отдельный банк. Всего 9 банков. Банк под номером 1 всегда содержит информацию о самых последних событиях (под номером 9 – о самых старых). При заполнении всех банков, события из банка 9 теряются. Максимальное число событий в одном банке 999. Максимальное число событий во всех банках –4096.

Минимальное время между двумя однотипными событиями составляет 1 секунду (изменение данного значения производится через «МЕНЮ»). Эти события будут зафиксированы в двух записях протокола. При условии появ-ления нового события (в одном частотном диапазоне) в период времени ме- нее 1 секунды, оно не будет определено, как новое событие. Фиксироваться будет увеличение длительности предшествующего события.

В режиме «МОНИТОРИНГ» обеспечена возможность автоматического включения/выключения изделия по расписанию, задаваемых в подменю

«СИСТЕМА» – (Таблица 5 Инструкции по эксплуатации). Для использова-ния данной возможности необходимо предварительно установить часы ре- ального времени.

Режим «ПРОСМОТР ПРОТОКОЛА».

Выбор данного режима осуществляется из «МЕНЮ». При отсутствии событий в протоколе индицируется надпись: «ПРОТОКОЛ ПУСТ». Видэкрана в режиме «ПРОСМОТР ПРОТОКОЛА» показаннарисунке 5.

Рис. 5. Экран ST107 в режиме «ПРОСМОТР ПРОТОКОЛА».

1 - Номер просматриваемого банка/Количество задействованных банков.

2 - Номер просматриваемого события/Количество событий вбанке.

3 - Частотный диапазон, в котором произошла тревога (Д1 или Д2).(рис.5).

4 - Параметры сигнала в момент превышенияпорога.

Переключение между банками осуществляется кнопкой ZERO. Кнопками VOL+ и VOL- осуществляется переключение между событиями в бан- ке. События пронумерованы в соответствии с заданным критерием сорти-ровки (настройка через МЕНЮ).

Если в меню выбран вид сортировки, отличный от сортировки по вре-мени, то возможно появление сообщения «Сортировка. Подождите...»

Выход из просмотра осуществляется кнопкой SENS/EXIT.

Режим «ОСЦИЛЛОГРАФ»

Внимание – данный режим работает только в случае подключения од-ного из двух каналов обнаружения. Видэкрана в режиме ОСЦИЛЛОГРАФ показаннарисунке 6.

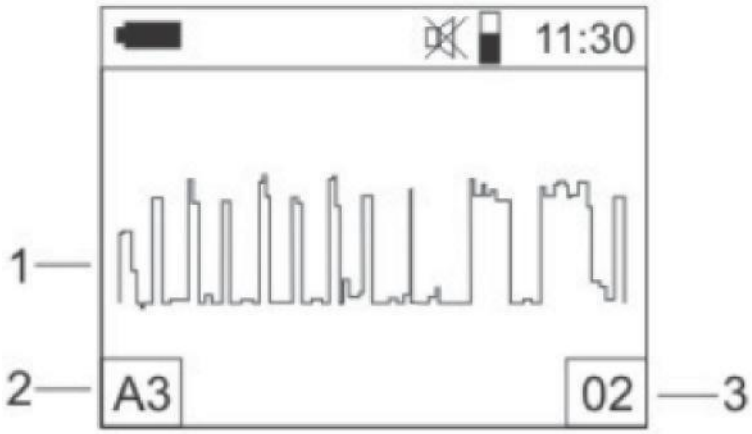


Рис. 6. Экран ST107 в режиме «ОСЦИЛОГРАФ».

1. Осциллограмма.

2. Вариант установки (А - автоматическое, Р - ручное) и относитель- ное значение вертикальной развертки (от 1 до7).

3. Значение горизонтальной развертки в пересчете на экран (1, 2, 4, 8,

16 и 32 мс).

Управление режимом

Установка автоматического выбора значения вертикальной развертки осуществляется нажатием на кнопку SENS/EXIT с появлением в позиции 1 знака «А» выбранного относительного значения (от 1 до 7).

Ручной выбор значения вертикальной развертки осуществляется последовательным нажатием на кнопку ZERO (символ «Р» в позиции 1). Выбор осуществляется относительными значениями от 1 до 7.

Выбор значения горизонтальной развертки осуществляется кнопками VOL+ и VOL- между значениями 2, 4, 8, 16 и 32 мс. «Замораживание» изоб-ражения осциллограммы происходит при нажатии на кнопку МЕЫU с появ- лением надписи в нижней строке дисплея «марк». Возобновление динамиче-ской индикации осуществляется нажатием кнопки SEЫS/EXIT. При повтор-ных нажатиях на кнопку MENU происходит переключение между тремя подрежимами маркерных измерений: «марк», «время» и «сдвиг». Из этих трех подрежимов нажатием на кнопку ZERO можно перейти в дополнитель-ныйподрежим «ноль». Индикация подрежимов размещена в нижней строке

дисплея. В подрежиме «марк» осуществляется «замораживание» просматриваемого временного отрезка длительностью, определенной в позиции 3 с возможностью проведения маркерных измерений. Это подтверждает, появивша-яся в нижней части экрана надпись «марк» и относительное численное значе- ние положения маркера (вертикальная белая линия) на временной шкале.

В подрежиме «время» обеспечивается возможность изменения значе-ния горизонтальной развертки для «замороженного» изображения.

В подрежиме «сдвиг» обеспечивается «прокрутка» всего зафиксиро- ванного временного отрезка при помощи кнопок VOL+ и VOL- в пределах32 мс.

Нажатием на кнопку ZERO из любого подрежима маркерных измере-ний любого видимого временного отрезка на дисплее. При этом происходит переход в подрежим «ноль» и обнуляется маркерное значение. Кнопками VOL+ и VOL- можно осуществлять перемещение маркера относительно «ну- левого» значения, с соответствующей индикацией численного значения из- меряемого временного отрезка в нижней части дисплея. Выход из подрежи-ма «ноль» осуществляется нажатием кнопки МЕЫU.

Выход в режим «ОСЦИЛЛОГРАФ» из подрежимов маркерных измере-ний производится нажатием кнопки SEЫS/EXIT. Надо отметить, что при входе в режим маркерных измерений происходит запоминание осцилло- граммы длительностью 32 мс и имеющей 5120 отсчетов. Чтобы производить детальный анализ такой осциллограммы можно воспользоваться предлагае-мымиподрежимами «время», «сдвиг» и «ноль». В подрежиме «время» обес-печивается возможность изменения значения горизонтальной развертки для

«замороженного» изображения.

Выход из режима «ОСЦИЛЛОГРАФ» осуществляется нажатием на кнопку SEЫS/EXIT.

МЕНЮ

Вход в МЕНЮ осуществляется нажатием кнопки MENU. Пункты ме- ню представлены в таблице 2 «Инструкции по эксплуатации». Выбор нужного пункта осуществляется при помощи кнопок VOL+ и VOL-. Подтвер-ждение выбора –

кнопкой MENU. Возвращение в предыдущий пункт – кнопкой ZERO.

3.2 Лабораторное исследование №3. Исследование детектора электромагнитного поля ST107

Цель: изучить устройство, технические характеристики, инструкцию по эксплуатации детектора электромагнитного поля ST107 и меры безопасности при работе с ним.

Время работы: 6 часов

Задания на выполнение лабораторного исследования

По техническому описанию прибора и настоящему пособию изучит устройство, технические характеристики, инструкцию по эксплуатации детектора электромагнитного поля ST107 и меры безопасности при работе с ним.
Руководствуясь инструкцией по эксплуатации, подготовить прибор к работе, произвести проверку его работоспособности, настройку и юстировку.
Обеспечить удаление из зоны действия прибора мощных помеховых объектов.
Провести обследование помещения лаборатории. Выявить и тщательно зафиксировать все источники ЭМС, и определить их характеристики, пользуясь всеми возможностями детектора электромагнитного поляST107.
Провести обследование контрольных образцов имитаторов ЗУ и провести их идентификацию с использованием и без использования частотомера.

Содержание отчета

Цель работы
Описание индикатора, принципа его действия, характеристик и основных приемы работы;
Данные, полученные при исследовании ЭМО в лаборатории;
Результаты идентификации контрольных образцов с подробным обоснованием принятого решения.
Отчет составляется персонально каждым учащимся, и полученные в нем результаты подлежат защите у преподавателя.
Выводы по проведенному исследованию.

Контрольные вопросы

При сдаче отчета по лабораторному исследованию студент должен быть готов ответить на следующие вопросы:

1. Как решается проблема выделения информационных излучений?
2. Для чего необходим эталон тестового сигнала?
3. Каким образом происходит сравнение обнаруженного сигнала иобраза эталонного сигнала?
4. Зачем необходим контроль ЭМО?
5. В каких режимах управляющая программа позволяет производить измерение ПЭМИН?

4 Обнаружение сигналов линейных и сетевых закладок

4.1 Краткие теоретические сведения

Перед поиском акустических радиозакладок необходимо установить порог срабатывания (чувствительность) индикатора ноля. С этой целью оператор, находясь в точке помещения на удалении нескольких метров от возможных мест размещения закладок (это, как правило, середина контролируемого помещения), должен установить регулятор чувствительности в такое положение, при котором световые или стрелочные индикаторы находятся на грани срабатывания или частота следования звуковых и световых импульсов была бы минимальной. Для этого он сначала, вращая регулятор, добивается срабатывания индикаторов, а затем медленным вращением его в обратную сторону их выключает. Если регулятор уровня чувствительности отсутствует, то порог срабатывания устанавливают путем уменьшения длины телескопической антенны.

При работе в сложной помеховой обстановке (например, в крупном городе) часто используются индикаторы поля, имеющие режекторные и полосовые фильтры. Центральная частота режекторного фильтра, как правило, совпадает с частотой излучения одной из мощных станций, работающих в данном районе (телевизионной, радиовещательной, радиорелейной станции или центральной станции системы сотовой связи и т.д.). Выбором того или иного режекторного фильтра оператор добивается максимального ослабления помехового сигнала. Но при этом надо помнить, что частота радиозакладки может находиться в полосе режекции фильтра. Полосовые фильтры осуществляют подавление принимаемых сигналов на частотах выше и ниже граничных частот фильтров и значительно повышают чувствительность индикатора поля. Но при этом время поиска значительно возрастает, так как обход помещения необходимо проводить столько раз, сколько используется полосовых фильтров.

Для активизации работы акустических радиозакладок, оборудованных системой VOX, в помещении необходимо создать тестовый акустический сигнал. В качестве источников тестового сигнала могут использоваться любые источники звуковых сигналов (специальные акустические генераторы, магнитофоны, CD-проигрыватели и другие средства). Создать тестовый сиг- нал может и сам оператор, например, давая счет или постукивая пальцем по обследуемым предметам. Если требуется провести поиск закладных устройств скрыто (идея создания тестового акустического сигнала) целесообразно использовать средства, постоянно находящиеся в помещении. Наиболее часто в них используется радиоприемник, настроенный на частоту какой-либо радиовещательной станции. В режиме скрытого поиска закладок рекомендуется отключить звуковую сигнализацию и устройство акустической «завязки» индикатора поля. Прослушивание детектированных сигналов необходимо осуществлять через наушники.

Поиск акустических радиозакладок осуществляется путем последовательного обхода помещения, двигаясь вдоль стен и обходя мебель и предметы, находящиеся в помещении. При обходе помещения антенну необходимо ориентировать в разных плоскостях, совершая медленные повороты кисти руки и добиваясь максимального уровня сигнала. При этом расстояние от антенны до обследуемых объектов должно быть не более 5 ... 20 см. В процессе поиска динамик индикатора поля все время

должен быть обращен в сторону обследуемых предметов или объектов. Обход помещения необходимо прово-дить два раза: первый с полностью выдвинутой телескопической антенной, второй – с антенной, выдвинутой на два колена.

При приближении индикатора к излучающей закладке напряженность электромагнитного поля возрастает, соответственно повышается и уровень сигнала на его входе. При превышении уровня сигнала порогового значения,

устанавливаемого регулятором чувствительности, срабатывают световые и звуковой индикаторы, и при включении устройства акустической «завязки» у прибора появляется характерный сигнал самовозбуждения (свист). Уменьшая уровень громкости акустического сигнала в динамике, оператор может сузить зону, в которой возникает режим самовозбуждения (акустическая за- вязка), и тем самым локализовать место расположения закладки. Необходимо помнить, что эффект акустической «завязки» наблюдается далеко не у всех радиозакладок, поэтому основным демаскирующим признаком при их обнаружении является наличие излучения. В этом случае локализация закладки с помощью индикатора поля осуществляется путем последовательного уменьшения чувствительности или длины антенны в зоне максимального уровня электромагнитного поля. Возможное местоположение радиозакладки определяется по максимальному уровню сигнала, при этом ошибка определения местоположения маломощных закладок (10 ... 20 мВт) составляет 5 ... 10 см.

Источником обнаруженного в помещении сигнала (электромагнитного поля) не обязательно является радиозакладка. В результате многочисленных переотражений электромагнитных волн различных внешних источников (мощных радиовещательных и телевизионных станций, радиомодемов ПЭВМ, оргтехники и т.п.) от стен помещения, различных металлических предметов и радиоаппаратуры распределение энергии в пространстве комнаты имеет весьма сложный вид с минимумами (мертвыми зонами) и максимумами. Поэтому окончательно обнаруживаются закладки визуальным осмотром места (объекта), где уровень излучения максимален. Наиболее эффективны для выявления закладок индикаторы поля, имеющие амплитудные и частотные детекторы. Прослушивание через динамик или наушники тестового акустического сигнала однозначно говорит о наличии радиозакладки.

Поиск радиозакладок с использованием индикаторов поля наиболее целесообразен и эффективен в местах с низким уровнем общего электромагнитного поля, т.е. вдали от крупных городов, телевизионных, передающих центров, объектов с большой концентрацией мощных радиоэлектронныхсредств и т.п. (например, при удалении от города Москвы на расстояние свыше 20 ... 40 км). В этих условиях дальность обнаружения даже маломощной радиозакладки индикатором поля составляет несколько метров. Процесс поиска радиозакладок с использованием индикаторов поля в крупных городах и местах с высоким общим уровнем электромагнитного поля очень трудоемкий и длительный по времени. В этих условиях дальность обнаружения маломощной радиозакладки не превышает 10 ... 50 см. Возникают неудобства и с обследованием труднодоступных мест, например, подвесного потолка (особенно, если он высокий), люстр, воздуховодов и т. п.

Методика поиска радиозакладок с использованием детекторов поля, неимеющих частотомера.

Методика заключается в следующем. Оператор, находясь в контролируемом помещении, включает тестовый акустический сигнал и включает интерсептор,

который захватывает и детектирует наиболее мощный сигнал. Если детектированный и прослушиваемый с помощью динамика сигнал не соответствует тестовому, данная частота вводится оператором в память LOCKOUT и исключается из рабочего диапазона. Процесс продолжается до появления в динамике тестового сигнала (т. е. до обнаружения излучения радиозакладки) или до пропадания всех сигналов (когда уровень оставшихся сигналов становится ниже чувствительности интерсептора). Обнаружение излучения радиозакладки и ее локализация осуществляется путем последовательного обхода всего помещения. В процессе поиска динамик интерсептора все время должен быть обращен в сторону обследуемых предметов или объектов. При приближении интерсептора к излучающей закладке на некоторое критическое расстояние появляется характерный сигнал самовозбуждения (акустической «завязки»). Уменьшая уровень громкости акустического сигнала в динамике, оператор может сузить зону, в которой возникает режим акустической «завязки», и тем самым локализовать закладку. Если интерсептор имеет индикатор уровня сигнала (например «Xplorer»), то возможное местоположение радиозакладки определяется по максимальному уровню сигнала.

Перед поиском акустических радиозакладок прежде всего необходимо установить порог срабатывания (чувствительность) индикатора ноля, с этой целью оператор, находясь в точке помещения на удалении нескольких метров от возможных мест размещения закладок (это, как правило, середина контролируемого помещения), должен установить регулятор чувствительности в такое положение, при котором световые или стрелочные индикаторы находятся на грани срабатывания или частота следования звуковых и свето-вых импульсов была бы минимальной. Для этого он сначала, вращая регулятор, добивается срабатывания индикаторов, а затем медленным вращением его в обратную сторону их выключает. Если регулятор уровня чувствительности отсутствует, то порог срабатывания устанавливают путем уменьшения длины телескопической антенны.

При работе в сложной помеховой обстановке (например, в крупном городе) часто используются индикаторы поля, имеющие режекторные и полосовые фильтры. Центральная частота режекторного фильтра, как правило, совпадает с частотой излучения одной из мощных станций, работающих в данном районе (телевизионной, радиовещательной, радиорелейной станции или центральной станции системы сотовой связи и т.д.). Выбором того или иного режекторного фильтра оператор добивается максимального ослабления помехового сигнала. Но при этом надо помнить, что частота радиозакладки может находиться в полосе режекции фильтра. Полосовые фильтры осуществляют подавление принимаемых сигналов на частотах выше и ниже граничных частот фильтров и значительно повышают чувствительность индикатора поля. Но при этом время поиска значительно возрастает, так как обход помещения необходимо проводить столько раз, сколько используется полосовых фильтров.

Для активизации работы акустическихрадиозакладок, оборудованных системой VOX, в помещении необходимо создать тестовый акустический сигнал. В качестве источников тестового сигнала могут использоваться любые источники звуковых сигналов (специальные акустические генераторы,магнитофоны, CD-проигрыватели и другие средства). Создать тестовый сигнал может и сам оператор, например, давая счет или постукивая пальцем по обследуемым предметам. Если требуется провести поиск закладных устройств скрыто (идея создания тестового акустического сигнала)

целесообразно использовать средства, постоянно находящиеся в помещении. Наиболее часто в них используется радиоприемник, настроенный на частоту какой-либо радиовещательной станции. В режиме скрытого поиска закладок рекомендуется отключить звуковую сигнализацию и устройство акустической “завязки” индикатора поля. Прослушивание детектированных сигналов необходимо осуществлять через наушники.

Поиск акустических радиозакладок осуществляется путем последовательного обхода помещения, двигаясь вдоль стен и обходя мебель и предметы, находящиеся в помещении. При обходе помещения антенну необходимо ориентировать в разных плоскостях, совершая медленные повороты кисти руки и добиваясь максимального уровня сигнала. При этом расстояние от антенны до обследуемых объектов должно быть не более 5 ... 20 см. В процессе поиска динамик индикатора поля все время должен быть обращен в сторону обследуемых предметов или объектов. Обход помещения необходимо проводить два раза: первый с полностью выдвинутой телескопической антенной, второй – с антенной, выдвинутой на два колена.

При приближении индикатора к излучающей закладке напряженность электромагнитного поля возрастает, соответственно повышается и уровень сигнала на его входе. При превышении уровня сигнала порогового значения, устанавливаемого регулятором чувствительности, срабатывают световые или звуковой индикаторы, и при включении устройства акустической “завязки” появляется характерный сигнал самовозбуждения (свист). Уменьшая уровень громкости акустического сигнала в динамике, оператор может сузить зону, в которой возникает режим самовозбуждения (акустическая завязка), и тем самым локализовать место расположения закладки. Необходимо помнить, что эффект акустической “завязки” наблюдается не у всех радиозакладок, поэтому основным демаскирующим признаком при их обнаружении является

наличие излучения. В этом случае локализация закладки с помощью индикатора поля осуществляется путем последовательного уменьшения чувствительности или длины антенны в зоне максимального уровня электромагнитного поля. Возможное местоположение радиозакладки определяется по максимальному уровню сигнала, при этом ошибка определения местоположения маломощных закладок (10 ... 20 мВт) составляет 5 ... 10 см.

Источником обнаруженного сигнала (электромагнитного поля) не обязательно является радиозакладка. В результате многочисленных переотражений электромагнитных волн внешних источников (мощных радиовещательных и телевизионных станций, ПЭВМ, оргтехники и т.п.) от стен помещения, различных металлических предметов и радиоаппаратуры распределение энергии в пространстве комнаты имеет сложный вид с минимумами и максимумами. Поэтому обнаруживаются закладки визуальным осмотром места (объекта), где уровень излучения максимален. Наиболее эффективны для выявления закладок индикаторы поля, имеющие амплитудные и частотные детекторы. Прослушивание через динамик или наушники тестового акустического сигнала однозначно говорит о наличии радиозакладки.

Поиск радиозакладок с использованием индикаторов поля наиболее целесообразен и эффективен в местах с низким уровнем общего электромагнитного поля, т.е. вдали от крупных городов, телевизионных, передающих центров, объектов с большой концентрацией мощных радиоэлектронных средств и т.п. (например, при

удалении от города Москвы на расстояние свыше 20 ... 40 км). В этих условиях дальность обнаружения даже маломощной радиозакладки индикатором поля составляет несколько метров. Процесс поиска радиозакладок с использованием индикаторов поля в крупных городах и местах с высоким общим уровнем электромагнитного поля очень трудоемкий и длительный по времени. В этих условиях дальность обнаружения маломощной радиозакладки не превышает 10 ... 50 см. Возникают неудобства с обследованием труднодоступных мест, например, потолка (особенно, если он высокий), люстр, воздуховодов и т.п.

Методика поиска радиозакладок с использованием этих приборов заключается в следующем. Оператор, находясь в контролируемом помещении, включает тестовый акустический сигнал и включает интерсептор, который захватывает и детектирует наиболее мощный сигнал. Если детектированный и прослушиваемый с помощью динамика сигнал не соответствует тестовому, данная частота вводится оператором в память LOCKOUT и исключается из рабочего диапазона. Процесс продолжается до появления в динамике тестового сигнала (т.е. до обнаружения излучения радиозакладки) или до пропадания всех сигналов (когда уровень оставшихся сигналов становится ниже чувствительности интерсептора). При обнаружении излучения радиозакладки ее локализация осуществляется путем последовательного обхода помещения. В процессе поиска динамик интерсептора все время должен быть обращен в сторону обследуемых предметов или объектов. При приближении интерсептора к излучающей закладке на некоторое критическое расстояние появляется характерный сигнал самовозбуждения (акустической “завязки”). Уменьшая уровень громкости акустического сигнала в динамике, оператор может сузить зону, в которой возникает режим акустической “завязки”, и тем са- мым локализовать закладку. Если интерсептор имеет индикатор уровня сиг- нала (например “Xplorer”), то возможное местоположение радиозакладки определяется по максимальному уровню сигнала.

Методика поиска радиозакладок с использованием радиочастотомеров практически аналогична методике поиска с использованием индикаторов поля. Поиск радиозакладок осуществляется путем последовательного обхода помещения. Особенно внимательно стоит проверить места наиболее вероят-ного расположения жучков – это вентиляционные отверстия и углы. При обходе помещения антенну необходимо ориентировать в разных плоскостях, совершая медленные повороты кисти руки и добиваясь максимального уровня сигнала. Расстояние от антенны до обследуемых объектов должно быть не более 5 ... 20 см. При этом оператор фиксирует частоту принимаемого сигнала и его относительный уровень. Радиочастотомер захватывает наиболее мощный в точке приема сигнал и измеряет его частоту. Знание частоты позволяет оператору грубо классифицировать принимаемый радиосигнал по возможным его источникам (радио- или телевизионное вещание, служебная связь, сотовая радиотелефонная связь и т.д.). Как правило, радиочастотомер захватывает сигналы мощных радиовещательных станций (при этом при каждом измерении на жидкокристаллическом дисплее показания частоты меняются). При перемещении по комнате (в режиме автозахвата частоты) относительный уровень этих сигналов изменяется незначительно, и максимальный уровень наблюдается около оконных рам и труб парового отопления.

При приближении к радиозакладке на некоторое критическое расстояние сигнал от нее начинает превышать сигналы радиовещательных станций. Радиочастотомер

захватывает этот сигнал и фиксирует его частоту. Наличие захвата сигнала радиозакладки подтверждается стабильностью частоты сигнала (при отключенной функции автозахвата частоты) и его высоким уровнем. Возможное местоположение радиозакладки определяется по максимальному уровню сигнала. Обнаружение радиозакладки осуществляется путем визуального осмотра подозрительных мест и предметов.

Радиочастотомеры, имеющие высокоомные входы, могут использоваться и для поиска закладок, передающих информацию по проводным линиям (электропитания, телефонным и т.д.) на высокой частоте. Для этого частотомер подключается к контролируемой линии с помощью щупа. При проверке линии электропитания частотомер подключается к нулевому проводу, который определяется обычным индикатором напряжения. Решение о наличии сетевой закладки в линии принимается при обнаружении в ней сигнала высокого уровня с высокой стабильностью частоты (при отключенной функции автозахвата частоты). Обычно частота передачи информации закладки лежит в пределах от 40 до 600 кГц, а в некоторых случаях – до 7 МГц. Поиск радио-закладки осуществляется путем визуального осмотра розеток, распределительных коробок и электрощитов, осветительных и электрических приборов (при осмотре они отключаются от сети и разбираются), а также непосредственно линий.

Аналогично поиску акустических радиозакладок осуществляется поиск телефонных радиозакладок. При поиске телефонных радиозакладок необходимо снять телефонную трубку и поднести индикатор поля (интерсептор) к телефонному аппарату. При наличии в корпусе телефонного аппарата радио- закладки срабатывают световые или звуковой индикаторы поискового устройства, а в динамике или головных телефонах будут прослушиваться непрерывный тональный сигнал или короткие гудки телефонной станции. Радиочастотомером определяется частота закладки. Поиск телефонной закладки производится путем разборки и осмотра телефонного аппарата, трубки и розетки. Далее поиск телефонных радиозакладок осуществляется путем последовательного обхода помещений вдоль телефонного кабеля. При обходе антенну необходимо ориентировать параллельно телефонной линии на минимально возможном расстоянии от нее. Особое внимание обращается на распределительные коробки и места, где телефонная линия проложена скрытой проводкой. Осмотр проводится вплоть до центрального распределительного щитка здания, который находится, как правило, на первом этаже или в подвале. При наличии на линии телефонной радиозакладки в месте ее расположения уровень сигнала поискового устройства будет максимален, а в динамике или головных телефонах индикатора поля или интерсептора будут прослушиваться непрерывный тональ- ный сигнал или короткие гудки телефонной станции.

Предложенная методика поиска не отражает всех нюансов, возникаю-щих в конкретных случаях, и носит скорее рекомендательный, чем обяза- тельный характер, поэтому не возбраняется применение оригинальных мето- дов и приемом, обнаруженных учащимся при изучении других пособиях, или на основании своего практического опыта.

4.2 Лабораторное исследование № 4.
Обнаружение сигналов линейных и сетевых закладок

Цель: изучить принцип действия и порядок работы комплекса на выявление сетевых и линейных закладок

Время: 2 часа.

Задания на выполнение лабораторного исследования

Изучить способы внедрения сетевых и линейных закладок.

Изучить принцип действия и порядок работы комплекса на выявление сетевых и линейных закладок.

Выявить наличие скрытно установленного выносного микрофона с питанием от телефонной линии связи.

Выявить наличие выносного скрытно установленного микрофона с питанием от линии сети электропитания.

Сделайте соответствующие выводы.

Содержание отчета

цель работы;

рабочие материалы, подготовленные на этапе, предшествующем выполнению лабораторной работы.

Привести задание на выполнение лабораторной работы.

Отобразить результаты экспериментальных данных, полученных при выполнении задания.

Сделать выводы по результатам работы.

Контрольные вопросы

Назовите демаскирующие признаки сетевых акустических закладок.

Назовите демаскирующие признаки проводной микрофонной системы подслушивания.

Перечислите демаскирующие признаки акустических и телефонных закладок с передачей на высокой частоте.

Перечислите способы прослушивания беседы, ведущейся в комнате, при положенной на рычаг трубке.

Поясните назначение акустического зондирования при выявлении линейной или сетевой закладки.

Результаты сканирования какого диапазона поднесущих частот проводных линий отображает закладка меню «Сеть»?

Какие действия производят в окне спектроанализатора?

Практическая работа 1

Изучение законодательной и нормативной базы правового регулирования вопросов защиты информации

Цель: изучение системы нормативных правовых актов по технической защите информации, закрепление теоретических знаний в области правового обеспечения информационной безопасности.

Методические указания

Отчет к практической работе оформляется в тетради и в электронном документе, который сохраняется на своем носителе или ресурсе, указанном преподавателем.

Каждый из документов содержит название и цель работы, в электронном документе в колонтитуле указывается фамилия, имя студента, номер группы и дата выполнения работы.

Текстовый электронный документ оформляется в соответствии с ГОСТ 2.105-95. Межгосударственный стандарт. Единая система конструкторской документации. Общие требования к текстовым документам (введен Постановлением Госстандарта от 08.08.1995, 426 ред. от 22.06.2006). Основные требования: цвет шрифта – черный, размер – 14 пт, гарнитура – Times New Roman, начертание – обычное (если не указано иное), выравнивание текста – по ширине, межстрочный интервал – полуторный, размеры полей: левое – 3 см, правое – 1,5 см, верхнее и нижнее – 2 см; абзацный отступ – 1,25 см. Допускается использовать компьютерные возможности акцентирования внимания на определенных терминах, утверждениях применяя различные варианты начертания шрифта.

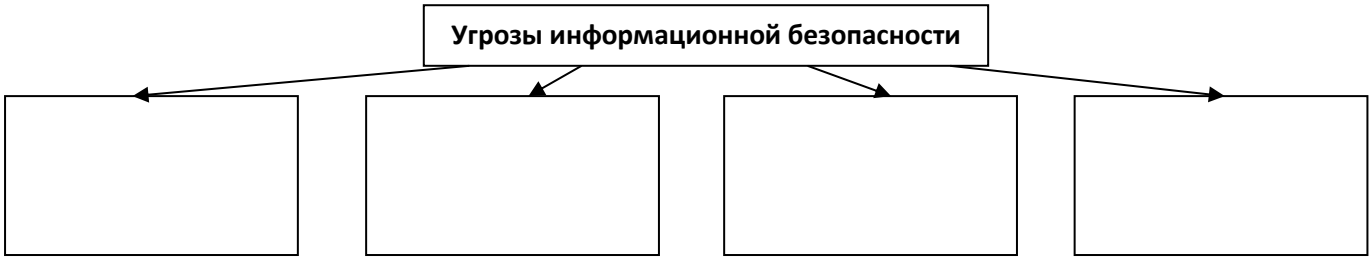
Ответы на задания даются полные, в соответствие с вопросом. При работе с нормативными документами указывается название документа, на который ссылается обучающийся. В качестве источников законодательных актов необходимо использовать справочно-правовые системы КонсультантПлюс, Гарант, официальные сайты организаций и структур.

Выполнение работы

Задание 1. Дайте ответы на вопросы в тетради, продолжите фразу.

1. Объектами технической защиты информации (ТЗИ) могут быть…
2. Концепция защиты информации – ...
3. Доктрина информационной безопасности РФ отображает ...
4. Нормативные правовые акты по технической защите информации – ...
5. Организационные документы – ...
6. Государственные стандарты – …
7. Руководящие документы – …

Задание 2. Заполните схему *Угрозы информационной безопасности* в соответствии с Доктриной информационной безопасности (в тетради).



Задание 3. Составьте перечень основных правоустанавливающие документов, связанных с технической защитой информации **(**ФЗ, стандарты, руководящие документы, постановления правительства и т.п.).

Указание. Перечень сохранятся в электронном документе под названием *Основные правоустанавливающие документы по ТЗ*.

Контрольные вопросы

1. Назовите основные виды конфиденциальной информации.
2. Какие сведения, в соответствии с законодательством, не могут быть отнесены к информации с ограниченным доступом?
3. Охарактеризуйте место правовых мер в системе комплексной защиты информации.
4. Назовите интересы государства в области обеспечения информационной безопасности.
5. Перечислите основные нормативные акты РФ, связанные с правовой защитой информации.
6. Какой закон определяет понятие «официальный документ»?
7. Какой закон определяет понятие «электронный документ»?
8. В каком законе приведена классификация средств защиты информации?
9. Назовите основные положения Доктрины информационной безопасности РФ.
10. Какая система обозначения сведений, составляющих государственную тайну, принята в РФ?
11. Дайте определение системы защиты государственной тайны и укажите ее составляющие.
12. Что в соответствии с законодательством РФ представляет собой засекречивание информации.
13. Перечислите основные принципы засекречивания информации.
14. Что понимается под профессиональной тайной?
15. Какие виды профессиональных тайн вам известны?
16. Что представляет собой электронная подпись?

Список используемых источников

1. Справочно-правовая система КонсультантПлюс.
2. Справочно-правовая система Гарант.
3. Сайт Федеральной службы по техническому и экспортному контролю.: http://fstec.ru/
4. Сайт федерального агентства по метрологии.: http://www.gost.ru/wps/portal/

Практическая работа 2

Изучение задач и функций органов по технической защите информации в РФ

Цель: ознакомление со структурой и функциями государственного аппарата обеспечения информационной безопасности РФ; изучение задач и функций органов по технической защите информации в РФ.

Методические указания

Отчет к практической работе оформляется в тетради и в электронном документе, который сохраняется на своем носителе или ресурсе, указанном преподавателем.

Каждый из документов содержит название и цель работы, в электронном документе в колонтитуле указывается фамилия, имя студента, номер группы и дата выполнения работы.

Ответы на задания даются полные, в соответствие с вопросом. При работе с нормативными документами указывается название документа, на который ссылается обучающийся. В качестве источников законодательных актов необходимо использовать справочно-правовые системы КонсультантПлюс, Гарант, официальные сайты организаций и структур.

Выполнение работы

Задание 1. Охарактеризуйте систему государственного регулирования и контроля в области информационной безопасности РФ.

Указание. Характеристику оформите в виде таблицы в тетради, отразите название специальных государственных органов и структур, кто руководит этими органами, кому подчиняются, дайте их определение.

Задание 2. Дайте ответы на вопросы, продолжите фразы:

1. ФСБ РФ в области технической защиты информации отвечает за …
2. Когда создана ФСТЭК? На месте, какого государственного органа?
3. Укажите документ, в котором описаны основные цели, задачи и функции ФСБ (названия, дата утверждения, последние изменения)?
4. Укажите документ, в котором описаны основные цели, задачи и функции ФСТЭК (названия, дата утверждения, последние изменения)?

Задание 3. В электронном документе под названием *Органы_ТЗ_РФ* дайте ответы на вопросы:

1. Каковы основные задачи ФСБ, связанные с технической защитой информации (по документу из вопроса 3 задания 2)?
2. Каковы основные функции ФСБ, связанные с технической защитой информации (по документу из вопроса 3 задания 2)?
3. Каковы основные задачи ФСТЭК (по документу из вопроса 4 задания 2)?

Задание 4. Изучите полномочия ФСТЭК (по документу из вопроса 4 задания 2), будьте готовы дать ответы на контрольные вопросы.

Контрольные вопросы

1. Перечислите органы государственного регулирования и контроля в области информационной безопасности РФ. Каковы основные направления их деятельности?

2. Какие организации в области технической защиты информации являются ключевыми органами?

3. Назовите документы, которым руководствуется ФСБ России в своей деятельности?

3. Перечислите основные задачи ФСБ в области технической защиты информации.

4. Перечислите основные функции ФСБ в области технической защиты информации.

5. В каком случае ФСБ России имеет право проводить плановые проверки?

6. Перечислите основные задачи ФСТЭК в области технической защиты информации.

7. Перечислите основные функции ФСТЭК в области технической защиты информации.

8. Каковы полномочия ФСТЭК?

Список используемых источников

1. Справочно-правовая система КонсультантПлюс.

2. Справочно-правовая система Гарант.

3. Сайт Федеральной службы по техническому и экспортному контролю. http://www.fstec.ru/

4. Сайт Федерального агентства по метрологии. ://www.gost.ru/wps/portal/

5. Сайт Федеральной службы безопасности РФ.://www.fsb.ru/

Практическая работа 3

Изучение положений о государственном лицензировании деятельности в области защиты информации

Цель: изучение положений о государственном лицензировании деятельности в области защиты информации; ознакомление с лицензирующими органами по каждому виду деятельности в области защиты информации.

Методические указания

Отчет к практической работе оформляется в тетради и в электронном документе, который сохраняется на своем носителе или ресурсе, указанном преподавателем.

Каждый из документов содержит название и цель работы, в электронном документе в колонтитуле указывается фамилия, имя студента, номер группы и дата выполнения работы.

Ответы на задания даются полные, в соответствие с вопросом. При работе с нормативными документами указывается название документа, на который ссылается обучающийся. В качестве источников законодательных актов необходимо использовать справочно-правовые системы КонсультантПлюс, Гарант, официальные сайты организаций и структур.

Выполнение работы

Задание 1. Изучите положения №99-ФЗ «О лицензировании отдельных видов деятельности» и дайте в тетради ответы на следующие вопросы.

1. Какова сфера деятельности настоящего закона?
2. Какие положения настоящего Федерального закона не применяются к отношениям, связанным с осуществлением лицензирования (в области защиты информации)?
3. Каковы цели лицензирования отдельных видов деятельности?
4. Что такое лицензия?
5. Что понимают под лицензионными требованиями?
6. С какого времени юридическое лицо или индивидуальный предприниматель, получившие лицензию, вправе осуществлять деятельность, на которую предоставлена лицензия?
7. На какой срок выдается лицензия?
8. Каким образом представляются заявление о предоставлении лицензии и прилагаемые к нему документы?
9. В каком случае лицензия подлежит переоформлению?
10. Какие проверки проводятся в отношении лицензиата лицензирующим органом? Особенности этих проверок.
11. В каких случаях действие лицензии приостанавливается лицензирующим органом?
12. Куда вносятся сведения о приостановлении действия лицензии?
13. За исключением, каких случаев информация по вопросам лицензирования (в том числе сведения, содержащиеся в реестрах лицензий) является открытой?

Задание 2. Изучите положения №99-ФЗ «О лицензировании отдельных видов деятельности» и выполните задания, сохранив их в файл под именем *Лицензирование.*

1. Составьте список лицензионных требований.
2. Перечислите сведения, которые указываются в заявление о предоставлении лицензии для индивидуального предпринимателя.
3. Составьте перечень оснований для отказа предоставления лицензии.
4. Составьте список сведений включаемых в реестре лицензий.
5. Сохраните в отдельные электронные документы формы:

а) типовая форма лицензии;

б) заявление о предоставлении лицензии.

Задание 3. Составьте перечень видов деятельности, на которые требуются лицензии в области защиты информации (перечень оформите в виде таблицы в тетради, во второй колонке, указав лицензирующий орган по каждому виду деятельности).

Задание 4. Составьте перечень положений о лицензировании конкретного вида деятельности, связанных с защитой информации (перечень сохраните в электронный документ см. задание 2).

Задание 5. Изучите *Реестр лицензий на деятельность по технической защите конфиденциальной информации* на сайте ФСТЭК.

1. Составьте перечень организаций Смоленска и Смоленской области, умеющих данный вид лицензии: номер лицензии, дату выдачи лицензии, адрес организации (перечень оформите в виде таблицы в электронный документ под именем *Реестр по ТЗ КИ*, оставив колонку для пункта 2).
2. На сайтах выбранных организаций изучите направления их деятельности и отразите их в таблице пунка 1.

Задание 6. Изучите *Реестр лицензий на деятельность по разработке и производству средств защиты конфиденциальной информации* на сайте ФСТЭК. В соответствии с задание 5 составьте таблицу.

Контрольные вопросы

1. Сформулируйте основные понятия, принятые в сфере государственного лицензирования в области защиты информации.
2. Организационная структура системы государственного лицензирования в области защиты информации.
3. Функции государственных органов по лицензированию в области защиты информации.
4. Функции лицензионных центров по лицензированию в области защиты информации.
5. Права и обязанности лицензиатов.
6. Порядок проведения лицензирования и контроля за деятельностью лицензиатов.
7. Назовите случаи приостановления или прекращения действия лицензии.
8. В каких случаях предприятию отказывают в выдаче лицензии?
9. Какие документы предоставляются для получения лицензии?

10.Каковы особенности лицензирования деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах?

11.Какие средства относятся к шифровальным?

12.Каковы особенности лицензирования видов деятельности, связанных с шифровальными (криптографическими) средствами?

13.Назовите лицензионные требования и условия при распространении шифровальных (криптографических) средств.

14.Назовите лицензионные требования и условия при осуществлении разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

15.Назовите лицензионные требования и условия при предоставлении услуг в области шифрования информации.

16.Назовите лицензионные требования и условия при осуществлении деятельности по техническому обслуживанию шифровальных (криптографических) средств.

Список используемых источников

1. Справочно-правовая система КонсультантПлюс.

2. Справочно-правовая система Гарант.

3. Сайт Федеральной службы по техническому и экспортному контролю. http://www.fstec.ru/

4. Сайт Федеральной службы безопасности РФ. http://www.fsb.ru/

Практическое занятие №4

Изучение положений о сертификации средств защиты информации по требованиям безопасности информации

Цель: изучить порядок сертификации средств защиты информации в Российской Федерации; функции органов системы сертификации средств защиты информации**.**

Методические указания

Отчет к практической работе оформляется в тетради и в электронном документе, который сохраняется на своем носителе или ресурсе, указанном преподавателем.

Каждый из документов содержит название и цель работы, в электронном документе в колонтитуле указывается фамилия, имя студента, номер группы и дата выполнения работы.

Ответы на задания даются полные, в соответствие с вопросом. При работе с нормативными документами указывается название документа, на который ссылается обучающийся. В качестве источников законодательных актов необходимо использовать справочно-правовые системы КонсультантПлюс, Гарант, официальные сайты организаций и структур.

Выполнение работы

Задание 1. Изучите положения о сертификации средств защиты информации по требованиям безопасности информации. В тетради дайте ответы на следующие вопросы.

1. В соответствии с чем производится сертификация средств защиты информации?
2. Дайте определение *сертификации* и *сертификата соответствия*.
3. Что является *средствами защиты информации*?
4. Перечислите основных участников системы сертификации средств защиты информации по требованиям безопасности информации.
5. Каковы основные виды и схемы проведения сертификации средств защиты информации?

Задание 2. Изучите функций и области деятельности органов сертификации средств защиты информации и выполните задания 1-3 в тетради, задания 4- в электронном документе, сохранив его под именем *Сертификация СЗИ.*

1. Назовите основные органы сертификации в области технической защиты информации РФ
2. Каковы области действия этих органов?
3. Каковы их требования по сертификации?
4. Перечислите функции ФСТЭК в области сертификации средств защиты информации.
5. Перечислите функции органов сертификации средств защиты информации.

6. Перечислите функции испытательных лабораторий (центров).

7. Перечислите функции заявителей.

8. Перечислите сведения, указываемые в заявке на сертификацию во ФСТЭК России.

9. В каком случае орган по сертификации средств защиты информации принимает решение об отказе в выдаче сертификата и направляет изготовителю мотивированное заключение?

Задание 3. Составьте перечень средств защиты информации, подлежащих сертификации (ответ сохраните в электронном документе).

Контрольные вопросы

1. Сформулируйте цели системы сертификации средств защиты информации по требованиям безопасности информации.
2. Какова организационная структура системы сертификации средств защиты информации по требованиям безопасности информации?
3. Назовите виды и схемы сертификации средств защиты информации.
4. Каковы функции ФСТЭК в области сертификации средств защиты информации?
5. Каковы функции органов сертификации средств защиты информации?
6. Каковы функции испытательных лабораторий (центров)?
7. Каковы функции заявителей?
8. Каков общий порядок проведения сертификации средств защиты информации.
9. Перечислите виды контроля в области сертификации средств защиты информации?
10. Чем определяются сроки проведения сертификационных испытаний?
11. На какой срок выдается сертификат?
12. Назовите причины приостановления или аннулирования действия сертификата.

Список используемых источников

1. Справочно-правовая система КонсультантПлюс.

2. Справочно-правовая система Гарант.

3. Сайт Федеральной службы по техническому и экспортному контролю. www.fstec.ru/

4. Сайт Федеральной службы безопасности РФ.: http://www.fsb.ru/

Практическая работа 5

Изучение положения о сертификации средств вычислительной техники и связи

Цель: изучить порядок сертификации средств вычислительной техники и связи в Российской Федерации**.**

Методические указания

Отчет к практической работе оформляется в тетради и в электронном документе, который сохраняется на своем носителе или ресурсе, указанном преподавателем.

Каждый из документов содержит название и цель работы, в электронном документе в колонтитуле указывается фамилия, имя студента, номер группы и дата выполнения работы.

Ответы на задания даются полные, в соответствие с вопросом. При работе с нормативными документами указывается название документа, на который ссылается обучающийся. В качестве источников законодательных актов необходимо использовать справочно-правовые системы КонсультантПлюс, Гарант, официальные сайты организаций и структур.

Выполнение работы

Задание 1. Изучите положения о сертификации технических, программно-технических, программных автоматизированных систем и локальных вычислительных сетей на соответствие требованиям по безопасности информации. В тетради дайте ответы на следующие вопросы.

1. В соответствии с чем производится сертификация технических, программно-технических, программных автоматизированных систем и локальных вычислительных сетей на соответствие требованиям по безопасности информации?
2. Перечислите основных участников системы сертификации технических, программно-технических, программных автоматизированных систем и локальных вычислительных сетей на соответствие требованиям по безопасности информации.
3. Каковы виды и схемы сертификации средств вычислительной техники и связи?

Задание 2. Изучите функции участников системы сертификации технических, программно-технических, программных автоматизированных систем и локальных вычислительных сетей на соответствие требованиям по безопасности информации, выполнив задания, сохраните их в электронном документе под именем *Сертификация ТС и ВС.*

1. Перечислите функции участников системы сертификации технических, программно-технических, программных автоматизированных систем и локальных вычислительных сетей на соответствие требованиям по безопасности информации.

2. Перечислите особенности подготовки и проведения сертификации средств вычислительной техники и связи по требованиям безопасности информации.

Задание 3. Изучите Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) и сохраните в электронный документ формы нормативной документации под именем *Документы сертификации*.

1. Акт классификации автоматизированной системы обработки информации.
2. Аттестат соответствия автоматизированной системы требованиям по безопасности информации.
3. Форма технического паспорта на автоматизированную систему

Контрольные вопросы

1. Какова организационная структура системы сертификации технических, программно-технических, программных автоматизированных систем и локальных вычислительных сетей на соответствие требованиям по безопасности информации?
2. Назовите виды и схемы сертификации средств вычислительной техники и связи по требованиям безопасности информации.
3. Каковы функции органов сертификации, испытательных лабораторий и заявителей в системе сертификации средств вычислительной техники и связи по требованиям безопасности информации?
4. Каковы особенности порядка подготовки и проведения сертификации средств вычислительной техники и связи по требованиям безопасности информации.
5. Перечислите виды контроля в области сертификации средств вычислительной техники и связи по требованиям безопасности информации.
6. На какой срок выдается сертификат?
7. Назовите причины приостановления или аннулирования действия сертификата.

Список используемых источников

1. Справочно-правовая система КонсультантПлюс.
2. Справочно-правовая система Гарант.
3. Сайт Федеральной службы по техническому и экспортному контролю. www.fstec.ru/
4. Сайт Федеральной службы безопасности РФ. www.fsb.ru/

Практическое работа 6

Изучение типовой методики испытаний объектов информатики по требованиям безопасности информации

Цель: изучение методику испытаний объектов информатики по требованиям безопасности информации.

Методические указания

Отчет к практической работе оформляется в тетради и в электронном документе, который сохраняется на своем носителе или ресурсе, указанном преподавателем.

Каждый из документов содержит название и цель работы, в электронном документе в колонтитуле указывается фамилия, имя студента, номер группы и дата выполнения работы.

Ответы на задания даются полные, в соответствие с вопросом. При работе с нормативными документами указывается название документа, на который ссылается обучающийся. В качестве источников законодательных актов необходимо использовать справочно-правовые системы КонсультантПлюс, Гарант, официальные сайты организаций и структур.

Выполнение работы

Задание. Используя Положение по аттестации объектов информатизации по требованиям безопасности информации" (утв. Гостехкомиссией РФ 25.11.1994) дайте ответы на следующие вопросы.

1. Перечислите объекты испытаний? (Ответ сохраните в электронный документ под именем *Методика испытаний*).
2. Каков цели и задачи проверок и испытаний? (Тетрадь)
3. Каковы условия и порядок проведения испытаний? (Эл. Документ)
4. Перечислите методы испытаний методы испытаний?
5. Каковы испытания объектов на соответствие организационно-техническим требованиям по защите информации? (Эл. Документ)
6. Каковы испытания объектов на соответствие требованиям по защите информации от утечки по каналам ПЭМИН? (Эл. Документ)
7. Каковы испытания объектов на соответствие требованиям по защите информации от несанкционированного доступа (НСД)? (Эл. Документ)
8. В чем состоит проверка правильности применения криптографических средств защиты информации? (Эл. Документ)
9. Каковы испытания объекта на соответствие требованиям по защите информации от утечки по акустическим каналам? (Эл. Документ)
10. Как проводится проверка выполнения требований по защите информации от утечки за счет строенных технических средств? (Эл. Документ)
11. Назовите виды оформления отчетных материалов. (Эл документ)

Контрольные вопросы

1. Назовите цели и задачи испытаний и проверок.
2. Каковы условия проведения испытаний?
3. Перечислите общие методы испытаний.
4. В чем состоит суть испытаний объектов на соответствие организационно-техническим требованиям по защите информации?
5. В чем состоит суть испытаний объектов на соответствие требованиям по защите информации от утечки по каналам ПЭМИН?
6. В чем состоит суть испытаний объектов на соответствие требованиям по защите информации от утечки по цепям заземления и электропитания?
7. В чем состоит суть испытаний объектов на соответствие требованиям по защите информации от утечки по кабельным линиям передачи данных ЛВС и сетей связи?
8. В чем состоит суть испытаний объектов на соответствие требованиям по защите информации от НСД?
9. В чем состоит суть испытаний объектов на соответствие требованиям по защите информации от утечки по акустическим каналам?
10. В чем состоит суть проверки выполнения требований по защите информации от течки за счет встроенных технических средств?
11. В чем состоит суть проверки правильности применения криптографических средств защиты информации?
12. Каким образом осуществляется оценка результатов испытаний и оформление отчетных материалов?

Список используемых источников

1. Справочно-правовая система КонсультантПлюс.
2. Справочно-правовая система Гарант.
3. Сайт Федеральной службы по техническому и экспортному контролю.://www.fstec.ru/

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Зайцев, А. П. Технические средства и методы защиты информации: Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В.Мещеряков; Под ред. А.П.Зайцева - 7 изд., исправ. - Москва : Гор. линия-Телеком, 2012. - 442с.; - (Уч. для вузов). ISBN 978-5-9912-0233-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/390284 . – Режим доступа: по подписке.

2. Душкин А.В., Барсуков О.М., Кравцов Е.В. Программно-аппаратные средства обеспечения информационной безопасности: Учебное пособие для вузов / Душкин А.В., Барсуков О.М., Кравцов Е.В. - Москва :Гор. линия-Телеком, 2016. - 248 с. (Специальность) ISBN 978-5-9912-0470-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/973806 . – Режим доступа: по подписке.

3. Новиков, С.Н. Методология защиты пользовательской информации на основе технологий сетевого уровня мультисервисных сетей связи / С.Н. Новиков ; под ред. В.П. Шувалова. -- Москва : Горячая линия -Телеком, 2018. - 128 с. - ISBN 978-5-9912-0410-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1040260 – Режим доступа: по подписке..

4. Новиков, В. К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области ...: Уч. пос./НовиковВ.К. - Москва : Гор. линия-Телеком, 2015.- 176с. (О)ISBN 978-5-9912-0525-2, 500 экз. - Текст : электронный. - URL: https://znanium.com/catalog/product/536932 . – Режим доступа: по подписке.

5. Меньшаков Ю.К. Защита объектов и информации от технических

средств разведки. М.: Российск. гос. гуманит. ун-т, 2002.

6. Хорев А.А. Защита информации от утечки по техническим каналам.

Часть 1. Технические каналы утечки информации. Учебное пособие. М.:Гостехкомиссия России, 2008. – 320 с.

7. Барсуков В.С., Марущенко В.В., Шигин В.А. Интегральная безо-пасность: Информационно-справочное пособие. – М.: РАО «Газпром»,2004. – 170 с.

8. Зайцев А.П., Шелупанов А.А. Справочник по техническим средствам защиты информации и контроля технических каналов утечки информации. Изд. Томского гос. ун-та систем управления и радиоэлектроники,2014. – 197 с.