|  |
| --- |
| Министерство образования Новосибирской области Государственное бюджетное профессиональное образовательное учреждение  Новосибирской области  «Новосибирский колледж почтовой связи и сервиса» |
| **ДОПУЩЕН К ЗАЩИТЕ**  зам. директора по УПР  /Т.В. Пушкарева  приказ №  от « » 2021 г |
| **«Выявление возможностей утечки информации по радиоканалам на основе спектра излучения»**  **Пояснительная записка к дипломному проекту** |
| **Специальность 12.02.08 Средства связи с подвижными объектами** |
| Студент Некрасов Т.Е.  Подпись Фамилия, И., О. студента |
| Группа ТС-43 |
| Руководитель Шабронов А.А  Подпись Фамилия, И., О. руководителя |
| Нормоконтроль  Подпись Фамилия, И., О. нормоконтролера |
| Председатель  цикловой комиссии  Подпись Фамилия, И., О. председателя |
| Новосибирск, 2021 г. |

Содержание

Изм*.*

Лист

№ докум.

Подпись

Дата

Лист

*2*

*НКПСИС 11.02.08.ТС-33 ПЗ*

Разраб.

Провер.

Реценз

Н. Контр.

Утверд.

*Частотно-территориальное проектирование сотовой связи стандарта GSM*

Лит

Листов

*ГБПОУ НСО «НКПСИС»*

**Введение**

В представленной работе рассматриваются задачи выявление возможностей утечки информации по радиоканалам на основе спектра излучения .Используя приборы сканирования радиоспектра фиксируем нарушения связи и возможные утечки информации. а фикс Умение правильно получить доступ к защищенной информации – обязательное условие для специалистов в области информационной безопасности. Чтобы охранять информацию нужно знать, как получают ее злоумышленники. Уметь создавать специальные каналы. И сейчас мы в этом подробно рассмотрим.

# **1.1. Классификация электромагнитных каналов утечки информации**

Электромагнитные волны имеют важное значение для передачи информации. Их можно передавать на тысячи километров. Утечка информации по радиоканалу протекает с помощью перехвата электромагнитных излучений диапазона, которые посылаются от отправителя к адресату. Также можно выполнить взлом сигналов у радиолокационных и радионавигационных сис­тем, радиостанций и систем связи, систем телеуправления, средств радиотелефонной связи, мониторов ПЭВМ, «радиозакладок» различного типа, перегово­ров внутри помещений предприятия с помощью беспровод­ных служебных систем связи и прочее.

Перехват информации по радиоканалам имеет ряд плюсов по сравнению с другими каналами утечки информа­ции, а именно:

– отсутствует естественный контакт с источником информации;

– на прием сигналов не влияет время года и время суток;

– информация поступает в реальном времени;

– перехват информации осуществляется достаточно незаметно ;

– у источника информации нету сведений о начатом процессе перехвата;

– дальность перехвата ограничивается только некоторыми особенно­стями распространения соответствующего диапазона радио­волн и возможностями источника информации.

Утечка информации по радиоканалу может протекать без преобразования информационного сигнала.

# **1.2. Перехват сигналов связных радиостанций**

Электромагнитные излучения передатчиков связи, помогут перехватываться с помощью обычных тех. Средств.

Упрощенная структура типового комплекса средств перехвата сигналов связанных радиостанций включает в себя:

-*приемные антенны.* Они могут изменять электромагнитные волны в электрические сигналы, амп­литуда, частота и фаза которых соотносится аналогичным характеристикам электромагнитной волны

*-радиоприемник.* Представляет поиск и селекцию радиосигналов по частоте, усиление и демодуляцию выделенных сигналов, их усиление и обработку

-*анализаторы технических характеристик сигна­лов.* Определяют параметры сигналов: частотные, времен­ные, энергетические, виды модуляции, структуру кодов и др

-*радиопеленгатор.* Дает возможность найти направле­ние на источник электромагнитного излучения и его коор­динаты

-*регистрирующее устройство.* Поставляет запись сигналов для документирования и дальнейшей обработки

Что перехватить радиосигналы связанных радиостанций применяют различные виды приемников или радиокомплексы.

К примеру, можно использовать приемные устройства AR-3000A, AR-5000, АРК-ЦТ, Winradio 3100i-DSP, радиокомплексы OSC-5000, AFK-MK1, АРК-Д1, АРК-ПК-П, R9000-DM-20 (профессиональный радиоприемник – многофункциональный комплекс).

|  |  |
| --- | --- |
|  |  |

# **1.3. Перехват радиотелефонных сигналов**

Для перехвата радиосигналов с трудной структурой, применяемой в сотовой, пейджинговой и других видах мо­бильной связи, созданы отдельные приемные комплексы.

К примеру, система контроля использования служебных ра­дио­те­лефо­нов сотовой связи стандарта NMT-450 ТТС-1 (фир­ма "Нелк") дает возможность обнаруживать и сопровождать по часто­те исходящие и входящие звонки абонентов сотовой связи, осуществлять слежение по частоте за каналом во время теле­фонного разговора, вести одновременно автоматическую за­пись разговора на диктофон и т.д. В комплексе используются ПЭВМ и два приемника AR 3000 А.

Для перехвата сообщений сотовых телефонов созданы ав­томатизированные станции перехвата сотовых систем связи. В состав станций входят: портативный компьютер, спецдемо­дулятор, приемное устройство, управляемое компьютером. Достаточно на экране компьютера задать номер интересую­щего абонента – и комплекс будет самостоятельно записывать входящие переговоры, определять номера звонящих к контро­лируемому абоненту, сопровождать мобильный объект при переходе из соты в соту.

Схожие системы существуют и для радиотелефонов российской системы "Алтай".

Обработка перехваченного радиосигнала осуществляется с помощью средств технического анализа. К ним относятся: Stabilock 4051, Stabilock 4032, HP 8920 A/D и др.

Для перехвата факсимильных передач используются спе­циальные комплексы типа 4600-FAX-INT, ФАКС-02, FAX MANAGER и др. Делают возможным автоматический перехват в реальном масштабе времени любого числа страниц, переда­ваемых по факсу со скоростью от 300 до 9600 бит/с, запись факсимильного сообщения и служебной информации, вывод их на печать.

Перехват пейджинговых передач осуществляется специализированными комплек­сами.

К примеру, разработаны АРК-Д1, АРК-ПК с использованием программного обеспе­чения СМО-ДЕМ, которое исполняет следующие функции:

– программа настройки приемника на частоты, преждевременно внесенные в файл пейджерных радиостанций;

– прием сообщений, передаваемых в формате PJCSAG со скоростями передачи 512, 1200 или 2400 Бод;

– автоматическое распознавание скорости и полярности передачи;

– регистрация сообщений (сохранение на диске), руч­ное декодирование и анализ принятых сообщений, оператив­ный просмотр принятых сообщений, поиск сообщения по шаблону (во всех таблицах кодировки);

– накопление в базе данных информации об абонентах и ее обновление;

– прием сообщений всех абонентов (режим "Обнаруже­ние");

– сохранение содержимого экрана в файле.

**Угрозы инфомационной безопасности. Построение систем защиты от угрозы нарушения конфиденциальности информации. Защита информации от утечки по техническим каналам**

**2.1. Анализ уязвимостей системы При построении системы защиты** информации обязательно нужно определить, что следует защищать и от кого (или чего) следует строить защиту. Определение информации, подлежащей защите, было дано выше. Защищаться следует от множества угроз, которые проявляются через действия нарушителя. Угрозы возникают в случае наличия в системе уязвимостей, то есть таких свойств АС, которые могут привести к нарушению информационной безопасности. Определение перечня угроз и построение модели нарушителя являются обязательным этапом проектирования системы защиты. Для каждой системы перечень наиболее вероятных угроз безопасности, а также характеристика наиболее вероятного нарушителя индивидуальны, поэтому перечень и модель должны носить неформальный характер. Защищенность информации обеспечивается только при соответствии предполагаемых угроз и качеств нарушителя реальной обстановке. При наличии в системе уязвимости потенциальная угроза безопасности может реализоваться в виде атаки. Атаки принято классифицировать в зависимости от целей, мотивов, используемого механизма, места в архитектуре системы и местонахождения нарушителя. Для предупреждения успешных атак необходим поиск и анализ уязвимостей системы. Уязвимости различаются в зависимости от источника возникновения, степени риска, распространенности, места в жизненном цикле системы, соотношения с подсистемами защиты АС. Анализ уязвимостей – обязательная процедура при аттестации объекта информатизации. В связи с возможностью появления новых уязвимостей, необходим их периодический анализ на уже аттестованном объекте.

**2.2. Основные направления и методы реализации угроз К основным** направлениям реализации злоумышленником информационных угроз относятся [3]: • непосредственное обращение к объектам доступа; • создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты; • модификация средств защиты, позволяющая реализовать угрозы информационной безопасности; • внедрение в технические средства АС программных или технических механизмов, нарушающих предполагаемую структуру и функции АС. К числу основных методов реализации угроз информационной безопасности АС относятся [3]: • определение злоумышленником типа и параметров носителей информации; • получение злоумышленником информации о программноаппаратной среде, типе и параметрах средств вычислительной 52 техники, типе и версии операционной системы, составе прикладного программного обеспечения; • получение злоумышленником детальной информации о функциях, выполняемых АС; • получение злоумышленником данных о применяемых системах защиты; • определение способа представления информации; • определение злоумышленником содержания данных, oбpaбaтываемых в АС, на качественном уровне (применяется для мониторинга АС и для дешифрования сообщений); • хищение (копирование) машинных носителей информации, содержащих конфиденциальные данные; • использование специальных технических средств для перехвата побочных электромагнитных излучений и наводок (ПЭМИН); • уничтожение средств вычислительной техники и носителей информации; • несанкционированный доступ пользователя к ресурсам АС в обход или путем преодоления систем защиты с использованием специальных средств, приемов, методов; • несанкционированное превышение пользователем своих полномочий; • несанкционированное копирование программного обеспечения; • перехват данных, передаваемых по каналам связи; • визуальное наблюдение; • раскрытие представления информации (дешифрование данных); • раскрытие содержания информации на семантическом уровне; • уничтожение машинных носителей информации; • внесение пользователем несанкционированных изменений в программно-аппаратные компоненты АС и обрабатываемые данные; • установка и использование нештатного аппаратного и/или программного обеспечения; • заражение программными вирусами; • внесение искажений в представление данных, уничтожение данных на уровне представления, искажение информации при передаче по линиям связи; • внедрение дезинформации; • выведение из строя машинных носителей информации без уничтожения; 53 • проявление ошибок проектирования и разработки аппаратных и программных компонентов АС; • искажение соответствия синтаксических и семантических конструкций языка; • запрет на использование информации. Переч исленные методы реализации угроз охватывают все уровни представления информации

**Электромагнитные каналы утечки**

Каждое электрическое (электронное) устройство является источником магнитных и электромагнитных полей широкого спектра, характер которых определяется назначением и схемными решениями, мощностью устройства, материалами, из которых оно изготовлено, и его конструкцией. Вокруг проводника, по которому протекает ток I, вызванный напряжением U, создается магнитное поле с напряженностью H и электрическое поле с напряженностью Е (рис. 3.9).

Рис. 3.9. Распределение магнитного и электрического поля вокруг проводника с током Изменение во времени тока приводит к изменению во времени электрического и магнитного полей. Вызванные изменением тока в проводнике изменяющиеся во времени электрическое и магнитное поля представляют собой единое изменяющееся электромагнитное поле, распространяющееся в пространстве, свойства которого целиком и полностью описываются уравнениями Максвелла. Известно, что характер поля изменяется в зависимости от расстояния до передающего устройства. Поле делится на две зоны: ближнюю и дальнюю. В дальней зоне (начиная от расстояний, больших 6λ от источника возмущения) электрическое поле принимает плоскую конфигурацию и распространяется в виде плоской волны, энергия которой делится поровну между электрической и магнитной компонентами. Дальняя зона — это область пространства, в которой распространение от источника существенно превышает длину волны. Граница между дальней и ближней зонами находится на расстоянии около 0,5 м от источника излучения для частоты 100 МГц и 50 м для частоты 1 МГц. В ближней зоне преобладает магнитная либо электрическая составляющая поля. Сильные магнитные поля, как правило, создаются цепями 74 с низким волновым сопротивлением, большим током и малым перепадом напряжений. Для поля с преобладающей электрической компонентой волновое сопротивление существенно больше, а для преобладающего магнитного поля — существенно меньше значения волнового сопротивления для плоской волны (Z = 377 Ом). Изменение тока во времени может носить импульсный характер или подчиняться любому другому закону. Каждый такой процесс на основе известного из математики преобразования Фурье может быть представлен в виде суммы гармонических колебаний с различными амплитудами для каждой частоты, причем частоты изменяются в пределах от нуля до бесконечности. Зависимость амплитуд этих гармонических составляющих от частоты – это спектр сигнала (в рассматриваемом случае – электромагнитного излучения). Спектр характеризует распределение энергии в поле излучения. В зависимости от того, на каких частотах устройство излучает наиболее интенсивно, излучатели электромагнитных сигналов подразделяют на низкочастотные, высокочастотные и оптические. Низкочастотными излучателями электромагнитных колебаний в основном являются звукоусилительные устройства различного функционального назначения и конструктивного исполнения. В ближней зоне этих устройств наиболее мощным выступает магнитное поле информативного сигнала. Такое поле усилительных систем достаточно просто обнаруживается и принимается посредством магнитной антенны и селективного усилителя звуковых частот. К группе высокочастотных излучателей относятся ВЧ-автогенераторы, модуляторы ВЧ-колебаний и устройства, генерирующие паразитные высокочастотные колебания по различным причинам и в различных условиях. Источниками сигнала выступают ВЧ-генераторы радиоприемников, телевизоров, измерительных генераторов, мониторы ЭВМ, модуляторы ВЧ колебаний. Довольно опасным источником высокочастотных колебаний могут быть усилители и другие активные элементы технических средств в режиме паразитной генерации за счет нежелательной положительной обратной связи. В качестве высокочастотного излучателя рассматривается любое устройство, содержащее элементы с нелинейными характеристиками (диоды, транзисторы, микросхемы), порождающими нежелательные составляющие высокочастотного характера. Спектр излучения обычно не поддается аналитическому расчету, т. к. его форма зависит от многих факторов; прежде всего это следующие: • рабочие частоты устройства, их гармоники и комбинационные частоты; • расположение и длина проводников; • расположение и конструкция реактивных элементов (конденсаторов и индуктивных катушек); 75 • тип корпуса, наличие в нем щелей, отверстий и т. п. При анализе спектра следует разделять информативное ПЭМИ и неинформативное ПЭМИ, а также реальные возможности восстановления информации из принятого ПЭМИ. Наиболее опасными являются следующие виды излучений и наводок: • электромагнитные излучения элементов ТСОИ (носителем информации является электрический ток, напряжение, частота или фаза которого изменяются по закону информационного сигнала); • электромагнитные излучения на частотах работы высокочастотных генераторов ТСОИ и ВТСС (в результате внешних воздействий информационного сигнала на элементах генераторов наводятся электрические сигналы, которые могут вызвать непреднамеренную модуляцию собственных высокочастотных колебаний генераторов и излучение в окружающее пространство [14]); • электромагнитные излучения на частотах самовозбуждения усилителей низкой частоты ТСПИ (самовозбуждение возможно за счет случайных преобразований отрицательных обратных связей в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов, причем сигнал на частотах самовозбуждения, как правило, оказывается промодулированным информационным сигналом); • наводки электромагнитных излучений ТСОИ (возникают при излучении элементами ТСОИ информационных сигналов, а также при наличии гальванической связи соединительных линий ТСОИ и посторонних проводников или линий ВТСС); • просачивание информационных сигналов в цепи электропитания (возможно при наличии магнитной связи между выходным трансформатором усилителя и трансформатором электропитания, а также за счет неравномерной нагрузки на выпрямитель, что приводит к изменению потребляемого тока по закону изменения информационного сигнала); • просачивание информационных сигналов в цепи заземления (образуется за счет гальванической связи с землей различных проводников, выходящих за пределы контролируемой зоны, в том числе нулевого провода сети электропитания, экранов, металлических труб систем отопления и водоснабжения, металлической арматуры и т. п.); • съем информации с использованием закладных устройств, представляющих собой минипередатчики, устанавливаемые в ТСОИ, излучения которых модулируются информационным сигналом и принимаются за пределами контролируемой зоны. 76 Параметрический канал утечки информации формируется путем «высокочастотного облучения» ТСОИ, при взаимодействии электромагнитного поля которого с элементами ТСОИ происходит переизлучение электромагнитного поля, промодулированного информационным сигналом. Взаимные влияния сигналов проявляются в линиях связи (табл. 5.1). Существуют реальные условия наводок с одного провода на другой, параллельный ему провод любой длины. В соответствии с явлением взаимной индукции ЭДС индукции наводится во всех проводниках, находящихся вблизи других проводников, ток в которых изменяется с течением времени, при этом ЭДС взаимной индукции пропорциональна скорости изменения тока. Таблица 5.1 Влияния в цепях связи и стандартные меры защиты Тип линии Преобладающее влияние Меры защиты Воздушные линии связи Систематическое влияние1 , возрастающее с увеличением частоты сигнала Скрещивание цепей, оптимальное расположение цепей Коаксиальный кабель Систематическое влияние через третьи цепи (с повышением частоты влияние убывает вследствие поверхностного эффекта) Экранирование и ограничение диапазона рабочих частот снизу Симметричный кабель Систематическое и случайное2 влияния, возрастающие с частотой Оптимизация шагов скрутки и конструкций кабеля, пространственное разделение цепей, экранирование Оптический кабель Систематическое и случайное влияния (от частоты не зависят) Экранирование оптических волокон, пространственное разделение отдельных волокон 1 Систематическое влияние – взаимные наводки, возникающие по всей длины линии 2 Случайное влияние – влияние, возникающее вследствие случайных причин и не поддающееся точной оценке. 77 Особое внимание следует обратить на перехват информации при ее передаче по каналам связи. Это вызвано тем, что в данном случае обеспечивается свободный несанкционированный доступ к передаваемым сигналам, особенно в случае использования радиоканала. В зависимости от вида канала связи технические каналы перехвата информации можно разделить на электромагнитные, электрические и индукционные. Электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться естественным образом с использованием стандартных технических средств. Электромагнитный канал перехвата информации широко применяется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым телефонам или по радиорелейным и спутниковым линиям связи. Электрический канал перехвата информации, передаваемой по кабельным линиям связи, предполагает контактное подключение к этим линиям. Электрический канал наиболее часто используется для перехвата телефонных разговоров, при этом перехватываемая информация может быть записана на диктофон или передана по радиоканалу. Подобные устройства, подключаемые к телефонным линиям связи и содержащие радиопередатчики для ретрансляции перехваченной информации, обычно называются телефонными закладками. Однако непосредственное электрическое подключение аппаратуры перехвата является компрометирующим признаком. Поэтому чаще используется индукционный канал перехвата, не требующий контактного подключения к каналам связи. Современные индукционные датчики, по сообщениям открытой печати, способны снимать информацию с кабелей, защищенных не только изоляцией, но и двойной броней из стальной ленты и стальной проволоки, которые плотно обвивают кабель. Единственным гарантированным методом защиты информации в этом случае является криптографическая защита. Для перекрытия электромагнитных каналов утечки информации используются пассивные и активные методы. К пассивным относятся экранирование элементов аппаратуры, устройств и линий связи, фильтрация сигналов в цепях питания и заземления. Активный метод – радиотехническое зашумление, используемое для закрытия (маскировки) побочных электромагнитных излучений и наводок. При этом спектр и энергия шумового сигнала подбираются таким образом, чтобы гарантировать невозможность выделения информативного сигнала.

## **Способы защиты информации**

### **Правовые**

Защита информации от утечки по техническим каналам осуществляется на основе конституций и законов, а также защита обеспечивается наличием авторских свидетельств, патентов, товарных знаков.

В России существует стандарт, который устанавливает классификацию и перечень факторов, воздействующих на защищаемую информацию, в интересах обоснования требований защиты информации на объекте информатизации. Настоящий стандарт распространяется на требования по организации защиты информации при создании и эксплуатации объектов информатизации, используемых в различных областях деятельности (обороны, экономики, науки и других областях). Требование соблюдения законов Российской Федерации, в частности «Об информации, информационных технологиях и о защите информации», «О государственной тайне», «О коммерческой тайне» и других законодательных актов Российской Федерации:

«Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам», утверждённого Постановлением Правительства РФ от 15.09.93 № 912-51, «Положения о лицензировании деятельности предприятий, организаций и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны», утвержденного Постановлением Правительства РФ от 15 апреля 1995 г. № 333, «Положения о государственном лицензировании деятельности в области защиты информации», утвержденного Постановлением Правительства РФ от 27 апреля 1994 г. № 10, «Положения о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации», утверждённого Постановлением Правительства РФ от 27 мая 2002 г. № 348, с изменениями и дополнениями от 3 октября 2002 г. № 731, «Положения о сертификации средств защиты информации», утверждённого Постановлением Правительства РФ от 26 июня 1995 г. № 608[]](https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D0%BD%D0%B0%D0%BB%D1%8B_%D1%83%D1%82%D0%B5%D1%87%D0%BA%D0%B8_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8#cite_note-16), Постановлений Правительства Российской Федерации «О лицензировании деятельности по технической защите конфиденциальной информации» (от 30 апреля 2002 г. № 290, с изменениями и дополнениями от 23 сентября 2002 г. № 689 и от 6 февраля 2003 г. № 64), «О лицензировании отдельных видов деятельности» (от 11 февраля 2002 г. № 135), а также «Положения по аттестации объектов информатизации по требованиям безопасности информации», утвержденного Председателем Гостехкомиссии России 25 ноября 1994 г., и других нормативных документов.

### **Организационные**

Обеспечивается совокупностью положений о Службе безопасности и планами работы этой службы. Планы мероприятий службы безопасности охватывают широкий круг вопросов, в частности:

а) на ранней стадии при проектировании помещений и строительстве Служба безопасности рассматривает следующие вопросы: выделение помещений для совещаний и переговоров (в таком помещении делается специальные перекрытия и каналы воздушной вентиляции, отдельные комнаты экранируют и так далее); удобство контроля помещений, людей, транспорта; создание производственных зон по типу конфиденциальности работ с самостоятельным дополнительным допуском;

б) служба безопасности участвует в подборе персонала с проверкой их качеств на основании личных бесед (изучение трудовой книжки, получения информации с других мест работы; затем принимаемый на работу ознакомляется с правилами работы с конфиденциальной информацией и порядком ответственности);

в) служба безопасности готовит положения и осуществляет: организацию пропускного режима; организацию охраны помещений и территорий; организацию хранения и использования документов, порядок учета, хранения, уничтожения документов, плановые проверки.

### **Инженерно-технические**

Защита включает в себя: аппаратные средства защиты; программные средства защиты — это использование специальных программ в системах, средствах и сетях обработки данных; математические способы защиты — применение математических и криптографических методов в целях защиты конфиденциальной информации (без знания ключа невозможно узнать и дешифровать украденную информацию)

**Рекомендации по проведению контрольно-поисковых работ с использованием изделия ST 033 "ПИРАНЬЯ"**



Эффективность применения изделия ST 033 "Пиранья" для проведения контрольно-поисковых работ определяется: степенью подготовленностью оператора к использованию изделия; полнотой и качеством подготовительных мероприятий; соответствием порядка действий оператора общим правилам и апробированным на практике приемам.  
Оператор должен иметь устойчивые навыки подготовки, проверки и управления изделием в предусмотренных режи мах, а также навыки анализа результатов слухового и визуального (по осциллограммам и спектрограммам) контроля параметров потенциально опасных сигналов.

Подготовительные мероприятия, обычно, проводят в два этапа. Первым из них является этап предварительной подготовки, а вторым - этап непосредственной подготовки.

Предварительный этап состоит, прежде всего, в заблаговременном детальном изучении объекта предстоящей контрольно-поисковой работы. При этом изучаются условия расположения объекта (характер наружной территории, наличие и предназначение смежных, выше и ниже расположенных помещений), а также его конструктивные особенности (размеры, высота потолков, материал и технология возведения стен и перегородок). Кроме того, важное на этом этапе, значение имеют оформление интерьера помещения (состав типаж и размещение мебели) и насыщенность техническими средствами (ПЭВМ, ксероксы, факсы, телефонные аппараты, бытовая техника и т. п.). Считается целесообразным полученные данные в том или ином виде протоколировать (вплоть до фотографирования). На этом этапе следует выявить наличие и трассы прохождения проводных и других потенциально опасных коммуникаций. Безусловно необходимой считается их паспортизация или, по крайней мере, наличие выполненных в масштабе схем сети электропитания, абонентской сети телефонной связи, систем пожарной и охранной сигнализации, трасс тепло- и водоснабжения, вентиляции. Данные, полученные в ходе предварительного этапа, служат основой для подготовки объекта и изделия ST 033 "Пиранья" непосредственно к началу работ. Порядок проведения непосредственной подготовки во многом зависит от целей и конкретных задач контрольно-поисковых работ, от степени предполагаемого задействования режимов и возможностей изделия. Поэтому содержание непосредственных подготовительных мероприятий, как и основные правила (приемы) выполнения операций контроля, удобнее всего рассматривать применительно к каждому виду контрольно-поисковых работ и режиму использования изделия.

Вместе с тем, существует общее, проверенное практикой, ПРАВИЛО. Оно состоит в том, что во всех случаях необходимо ИСКЛЮЧИТЬ ПРИСУТСТВИЕ НА КОНТРОЛИРУЕМОМ ОБЪЕКТЕ (В ПРОВЕРЯЕМОМ ПОМЕЩЕНИИ) ЛИЦ, НЕ ИМЕЮЩИХ ОТНОШЕНИЯ К ПОДГОТОВКЕ И ПРОВЕДЕНИЮ ПРОВЕРКИ.

1 ИСПОЛЬЗОВАНИЕ ИЗДЕЛИЯ ДЛЯ ВЫЯВЛЕНИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ В РАДИОЧАСТОТНОМ ДИАПАЗОНЕ Эти каналы могут быть созданы искусственно (преднамеренно), за счет использования заинтересованными органами и организациями специальных технических средств (радиомикрофоны, телефонные радиоретрансляторы, несанкционированно включенные радиостанции, радиомаяки и т. п.). Они могут возникнуть и естественно, за счет побочных электромагнитных излучений (ПЭМИ) технических средств обработки информации (ПЭВМ, телексы, факсы и т.п.). В любом случае возникает необходимость классификации сигналов в радиочастотном диапазоне по совокупности критериев.

1.1. ОДИН ИЗ ПРАКТИЧЕСКИХ ПОДХОДОВ К КЛАССИФИКАЦИИ РАДИОСИГНАЛОВ С точки зрения решения задач контроля защиты информации и использования при этом изделия ST 033 "Пиранья", все радиосигналы, попадающие в его рабочий диапазон, можно достаточно объективно подразделить на ОПАСНЫЕ и НЕОПАСНЫЕ. Полезной для практики является также классификация радиосигналов по наиболее вероятному месту их возникновения (ВНУТРЕННИЕ и ВНЕШНИЕ), относительно проверяемого объекта (помещения). ОПАСНЫЕ радиосигналы могут быть созданы как внутренними, так и внешними источниками. Более того, на практике встречается довольно большое число их самых разнообразных сочетаний. Обычно к числу чисто ВНУТРЕННИХ ОПАСНЫХ радиосигналов относят: сигналы "радиозакладок" (радиомикрофоны, телефонные радиотрансляторы и т.п.). сигналы радиомаяков; сигналы несанкционированно включенных в помещении радиостанций и радиотелефонов; побочные электромагнитные излучения ПЭВМ и других технических средств обработки информации. К категории ОПАСНЫХ, в сочетании "ВНУТРЕНИЕ-ВНЕШНИЕ", принято относить радиосигналы, источниками которых могут быть: радиомикрофоны с выносным акустическим микрофоном; телефонные радиоретрансляторы, установленные на линии связи за пределами помещения (но вблизи него); радиостетоскопы, установленные с наружной стороны ограждающих помещение поверхностей; вынесенные передатчики скрытых видеокамер; устройства внешнего высокочастотного облучения. Чисто ВНЕШНИЕ источники радиоизлучения, как правило, прямой ОПАСНОСТИ, с точки зрения утечки информации, не представляют. К их числу можно отнести широковещательные радиостанции, станции телевизионного вещания, средства радиосвязи и т.п. В качестве источников ВНУТРЕННИХ НЕОПАСНЫХ радиосигналов могут рассматриваться, прежде всего, электроприборы, оргтехника, бытовые средства, а также их блоки питания. Учитывая многообразие источников потенциально опасных сигналов при работе с изделием ST 033 "Пиранья" применяют два основных метода их поиска и локализации.

1.2. МЕТОДЫ ПОИСКА И ЛОКАЛИЗАЦИИ ИСТОЧНИКОВ ОПАСНЫХ РАДИОСИГНАЛОВ В практике вообще, и при работе с изделием ST 033 "Пиранья" в частности, используют раздельно или в сочетании два основных метода поиска и локализации источников опасных радиосигналов. Ими являются так называемые "Амплитудный метод" и метод "Акустической завязки". "Амплитудный метод" основан на резком возрастании уровня принимаемого сигнала при приближении приемной антенны изделия к месту расположения его источника. Радиус зоны обнаружения источника зависит от мощности излучаемого им сигнала, направленности его антенны и уровня фона электрического поля в точке расположения приемной антенны изделия. После фиксации факта обнаружения потенциально опасного радиосигнала следует двигаться в направлении возрастания его уровня. Контроль за уровнем принимаемого сигнала необходимо осуществлять по показаниям индикаторов уровня на экране дисплея изделия и по частоте щелчков звуковой сигнализации в режиме "TONE". Метод "Акустической завязки" основан на возникновении положительной акустической обратной связи между микрофоном "радиозакладки" и динамиком изделия ST 033 "Пиранья". Обязательно включение звуковой сигнализации изделия в режим "AUD" для вывода на динамик демодулированного сигнала. Эффект "акустической завязки" возникает только в отношении "радиозакладки", в которой применены обычные виды модуляции - амплитудная и частотная (узкополосная или широкополосная). Причем в случае частотной модуляции эффект основан на наличии "паразитной" амплитудной модуляции в частотномодулированном сигнале (в случае качественно выполненной "радиозакладки" эффект "акустозавязки" будет достаточно слабым, вплоть до полного отсутствия). Признаком возникновения "акустозавязки" является появление характерного "писка", тон и интенсивность которого изменяются при приближении динамика изделия к микрофону "радиозакладки". Следует учитывать, что наличие характерного звука при использовании данного метода демаскирует проведение работ. Поэтому в случае применения "радиозакладок" с дистанционным управлением они могут быть выключены на время проверки. Рациональный выбор того или другого метода во многом зависит от особенностей, присущих потенциально опасным радиосигналам и их источникам. 1.3. ОСОБЕННОСТИ ПОТЕНЦИАЛЬНО ОПАСНЫХ РАДИОСИГНАЛОВ И ИХ ИСТОЧНИКОВ Как уже отмечалось, источниками потенциально опасных радиосигналов являются радиомикрофоны, телефонные радиоретрансляторы, радиостетоскопы, скрытые видеокамеры с радиоканалом передачи информации, радиозакладки в ПЭВМ, средства пространственного высокочастотного облучения, несанкционированно включенные средства связи (радиостанции, радиотелефоны, телефоны с радиоудлинителями). В силу большого разнообразия вариантов конструктивного и схемного исполнения радиомикрофонов именно для них характерен и широкий спектр особенностей радиоизлучение.

1.3.1. РАДИОМИКРОФОНЫ Широкое распространение имеют радиомикрофоны с параметрической стабилизацией частоты передатчика. Основная особенность - большие пределы изменения несущей частоты (до нескольких мегагерц). Поэтому для локализации радиомикрофонов такого типа наиболее целесообразно использование метода "акустозавязки". Достаточно широко применяются радиомикрофоны с кварцевой стабилизацией частоты и узкополосной частотной модуляцией. Основные их особенности заключаются в небольших пределах изменения несущей частоты (до десятка килогерц) и слабом звуковом сигнале на выходе амплитудного детектора приемника изделия. Последнее определяет значительно меньшие размеры зоны возникновения "акустозавязки". Поэтому для поиска и локализации такого типа источников наиболее целесообразно использование амплитудного метода. В качестве высокопрофессиональных средств негласного добывания информации применяются радиомикрофоны с вынесенным передатчиком. Их основная особенность - разнос мест установки микрофона и собственно радиопередатчика (вплоть до выноса в другое помещение). В этом случае необходимо сочетание метода "акустозавязки" и амплитудного метода. Причем для локализации микрофона необходимо использовать метод "акустозавязки", а радиопередатчика (в проверяемом помещении или за его пределами) - амплитудный метод. Высокопрофессиональными средствами являются и радиомикрофоны с закрытым или маскированным радиоканалом. Их основная особенность в том, что принятый и демодулированный сигнал не несет в себе информации об акустическом фоне помещения. Это определяется использованием для закрытия (маскирования) радиоканала методов инверсии спектра, цифровых методов передачи и сложных видов модуляции. Следовательно, в основе их обнаружения и локализации должен лежать амплитудный метод с дополнением его анализом осциллограмм и спектрограмм в режимах "OSC" и "SA", соответственно. У радиомикрофонов, предназначенных для установки в автомобилях и других транспортных средствах, выделяют две основных особенности - повышенную мощность радиопередатчика и более чистый, без признаков внешнего фона, демодулированный сигнал (в силу звукоизолирующих свойств корпуса автомобиля). Другие особенности могут проявляться в зависимости от используемых способов стабилизации несущей частоты и применяемых видов модуляции. Поэтому методы поиска и локализации таких радиомикрофонов полностью аналогичны рассмотренным выше.

1.3.2. ТЕЛЕФОННЫЕ РАДИОРЕТРАНСЛЯТОРЫ Несмотря на многообразие вариантов исполнения телефонных радиоретрансляторов, отчётливо выделяются две их группы по способу подключения к элементам телефонной линии - с гальваническим контактом и без него.



При этом гальваническое подключение может осуществляться как последовательно (в разрыв одного из проводов телефонной линии), так и параллельно (одновременно к двум проводам телефонной линии). Телефонные радиоретрансляторы последовательного включения отличаются главной особенностью - появлением в эфире модулированного сигнала только при поднятой трубке телефонного аппарата. При этом явно прослушиваются сигналы АТС ("вызов", "занято"), щелчки набора номера, разговор абонентов после установления соединения. Такой радиоретранслятор принципиально может быть установлен, практически, на любом участке телефонной линии (корпус аппарата, его трубка, распределительные коробки и щиты, собственно провода абонентской линии). Локализацию телефонных ретрансляторов данного типа наиболее целесообразно осуществлять амплитудным методом. Это обусловлено тем, что телефонные аппараты, используемые в настоящее время, имеют достаточно чувствительные микрофоны и, часто, режим громкоговорящей связи. Применение метода "акустозавязки" может привести к ложным выводам о наличии установленного телефонного радиоретранслятора. Телефонные радиоретрансляторы параллельного включения могут иметь две разновидности. Первая из них предусматривает реализацию только функции ретранслятора. При этом в режиме поднятой трубки на радиочастоте прослушиваются сигналы АТС ("вызов", "занято"), щелчки набора номера и разговор абонентов. При положенной трубке модуляция радиосигнала отсутствует, может отсутствовать и сама несущая частота. Такой радиоретранслятор может быть принципиально установлен на любом участке телефонной линии. Для локализации закладок такого типа предпочтителен амплитудный метод с их активизацией путём поднятия трубки телефонного аппарата. Во второй разновидности часто совмещают функции телефонного радиоретранслятора и радиомикрофона, питающегося от телефонной линии и обеспечивающего контроль акустики помещения в режиме положенной трубки. Такие закладки устанавливаются на элементах телефонной линии в пределах интересующего помещения. Для их локализации при положенной трубке используется метод "акустозавязки" с применением тестового звукового сигнала. В режиме поднятой трубки для локализации таких закладок предпочтителен амплитудный метод. Необходимо иметь в виду, что радиоретрансляторы гальванического подключения, как правило, не имеют собственных антенн, а используют вместо них провода телефонных линий. В этом случае их локализация может быть осуществлена только амплитудным методом за счёт выявления распределения максимумов уровня высокочастотного электромагнитного поля вдоль телефонной линии. Максимумы чередуются через половину длины волны, а ближайший, по отношению к передатчику, удалён от него на расстояние четверти длины волны. Длина волны определяется в соответствии со значением частоты, "захваченной" частотомером изделия. Например, при частоте излучения 300МГц длина волны составляет 1 метр. Следовательно максимумы излучения для данного случая будут чередоваться через 0,5 метра, а места наиболее вероятной установки такого рода радиоретрансляторов будут находиться на расстоянии 25 сантиметров от точек максимума. Телефонные радиоретрансляторы не гальванического включения (индуктивного съёма информации) могут быть установлены на любом участке телефонной линии, как правило, вне интересующего помещения на абонентской проводке без нарушения изоляции. Они формируют модулированный радиосигнал только при поднятии трубки телефонного аппарата. При этом прослушиваются сигналы АТС ("вызов", "занято"), щелчки набора номера, разговор абонентов после установления соединения. Их локализация осуществляется амплитудным методом по мере обследования телефонной линии на всём её доступном протяжении.

1.3.3. ДРУГИЕ ИСТОЧНИКИ ПОТЕНЦИАЛЬНО ОПАСНЫХ РАДИОИЗЛУЧЕНИЙ Здесь следует рассмотреть, прежде всего, радиостетоскопы, скрытые видеокамеры с радиоканалом передачи информации, радиозакладки в ПЭВМ, радиомаяки, средства пространственного высокочастотного облучения, несанкционированно включенные средства связи (радиостанции, радиотелефоны, телефоны с радиоудлинителями).



Основная особенность радиостетоскопов состоит в том, что они устанавливаются только с внешней стороны поверхностей, ограждающих контролируемое помещение, или на выходящих за его пределы трубах систем отопления, водопровода и других коммуникациях. Для обнаружения их сигналов можно использовать режим "AUD" и классификацию "на слух", а для локализации источников радиоизлучения - амплитудный метод с перемещением изделия в смежные, выше и ниже расположенные помещения. Скрытые видеокамеры с радиоканалом передачи информации отличаются тем, что сигнал, излучаемый в радиодиапазоне, по структуре схож с сигналом канала яркости передатчиков телевизионного вещания. Этот сигнал, по оговоренной выше классификации, является ВНУТРЕННИМ (относительно проверяемого помещения). Обнаружение такого сигнала и локализацию его источника наиболее целесообразно осуществлять амплитудным методом, дополняя этот метод прослушиванием изменения тона продетектированного сигнала в режиме "AUD" и анализом изменения структуры сигнала в режимах "OSC" и "SA". Радиозакладки в ПЭВМ предназначены для передачи изображения монитора и цифровых сигналов системного блока и других элементов физической архитектуры компьютера. Основная их особенность заключается в том, что сигнал, передающий изображение монитора, по структуре похож на сигнал передатчика скрытой видеокамеры, а в других случаях содержит все признаки цифровой передачи. Основой для их обнаружения и локализации служит амплитудный метод, дополняемый анализом изображений в режимах "OSC" и "SA". Радиомаяки отличаются тем, что их радиоизлучение не имеет модуляции акустическим фоном помещения (объекта), является непрерывным или отчетливо выраженным периодическим. Возможна модуляция тоном. Их обнаружение может осуществляться амплитудным методом в сочетании с прослушиванием сигнала в режиме "AUD", а локализация - только амплитудным методом. Средства пространственного высокочастотного облучения являются ВНЕШНИМИ и используются для добывания информации из помещений путем ориентации на него (преимущественно через оконные проемы) мощного остронаправленного луча электромагнитного излучения высокой частоты и приема переизлученного (уже промодулированного) сигнала на частотах высших гармоник. Основные особенности, обеспечивающие возможность их (средств) обнаружения и локализации заключаются в том, что зондирующий сигнал является стабильным по частоте, его модуляция отсутствует, уровень неравномерен (более высокий в районе окон, существенно более низкий в коридоре и других помещениях). Кроме того, переизлученный сигнал по частоте соответствует высшим гармоникам зондирующего сигнала и имеет модуляцию акустическим фоном помещения. Поэтому обнаружение таких средств осуществляется амплитудным методом в сочетании с прослушиванием сигнала в режиме "AUD", а локализация направления облучения - только амплитудным методом. Основной особенностью несанкционированно включенных на передачу радиостанций, радиотелефонов и телефонов с радиоудлинителем является значительно меньшая, чем у радиомикрофонов чувствительность встроенного микрофона. Кроме того, во многих из них (особенно в радиотелефонах) используются сложные виды модуляции. Это приводит к тому, что в принятом и продетектированном радиосигнале либо не прослушивается акустический фон помещения, либо "акустозавязка" возникает в непосредственной близости к таким средствам. Для их поиска и локализации следует ориентироваться на амплитудный метод.

1.4 ОСНОВНЫЕ ПРАВИЛА ПОДГОТОВКИ И ПРОВЕДЕНИЯ КОНТРОЛЬНО-ПОИСКОВЫХ РАБОТ Начинаются работы с подготовки контролируемого помещения (объекта) и самого изделия ST 033 "Пиранья". Начальный этап подготовки помещения заключается в создании таких условий, при которых обеспечивается минимально возможный уровень фона электрического поля. Это достигается отключением потенциальных источников повышения фона, которыми принято считать средства оргтехники, ПЭВМ, преобразователи и блоки питания, базовые станции беспроводных телефонов, люминесцентные осветительные лампы и другие электронные устройства и электроприборы. Целесообразно также закрыть окна и двери, опустить (задвинуть) шторы или жалюзи.

ОСОБО СЛЕДУЕТ ОБРАТИТЬ ВНИМАНИЕ НА ТО, ЧТОБЫ БЫЛИ ВЫКЛЮЧЕНЫ РАДИОТЕЛЕФОНЫ И ДРУГИЕ РАДИОПЕРЕДАЮЩИЕ СРЕДСТВА, А ТАКЖЕ СРЕДСТВА АКТИВНОЙ РАДИОТЕХНИЧЕСКОЙ ЗАЩИТЫ, ЕСЛИ ИМИ ОБОРУДОВАНО ПРОВЕРЯЕМОЕ ПОМЕЩЕНИЕ ИЛИ СМЕЖНЫЕ С НИМ. НЕ ДОПУСКАЕТСЯ ОДНОВРЕМЕННАЯ РАБОТА ИЗДЕЛИЯ ST 033 "ПИРАНЬЯ" С НЕЛИНЕЙНЫМИ ЛОКАТОРАМИ.

Если объектом проверки является автомобиль, то необходимо правильно выбрать, с точки зрения уменьшения уровня электромагнитного фона, место проведения работ. Так, вблизи него не должны находиться высоковольтные линии электропередач, трансформаторные подстанции, излучающие средства связи, теле- и радиовещания, а также крупные отражающие (переизлучающие) поверхности - металлические ограждения, стены домов, гаражи, другие автомобили. Поиск потенциально опасных радиосигналов и их источников обычно проводят последовательно, поочерёдно проверяя наличие: автономных радиомикрофонов и телефонных радиоретрансляторов; камуфлированных радиомикрофонов, питающихся от электросети; радиостетоскопов; скрытых видеокамер с радиоканалом; пространственного высокочастотного облучения; радиозакладок в ПЭВМ. Для создания акустического фона и для активизации радиозакладок с акустопуском следует подготовить и разместить в контролируемом помещении тестовый источник звука. В качестве такого источника можно использовать магнитофон с хорошо известной музыкальной или речевой фонограммой. Не рекомендуется использовать в этих целях радиоприемник или телевизор, так как создаваемый ими звуковой сигнал, переизлучаемый "радиозакладкой", может совпасть с радиосигналом самой вещательной станции. Выбор громкости тестового звукового сигнала определяется как размерами помещения, так и чувствительностью микрофона "радиозакладки". Обычно такие микрофоны уверенно воспринимают звук средней громкости с расстояния порядка 10 метров. Подготовка самого изделия ST 033 "Пиранья" (после проверки его работоспособности в данном режиме) заключается в установке "нулевого" порога детектора, что является, фактически, определяющим для успешного проведения работ. Занижение порога обязательно приведет к частым ложным срабатываниям индикации, а его завышение - к вероятному пропуску сигнала "радиозакладки". И то, и другое значительно усложняет работу оператора, увеличивает время и снижает достоверность результатов проверки. Поэтому для установки "нулевого" порога необходимо обязательно придерживаться нескольких простейших правил. Нельзя проводить установку порога в проверяемом помещении, так как при функционировании в нем уже размещенной "радиозакладки", уровень ее радиоизлучения будет определен изделием как "нулевой". Во время настройки порога недопустимо использование радиостанций, радиотелефонов и других радиоизлучающих средств. Не приближать антенну изделия к включенным ПЭВМ и другим средствам оргтехники, как источникам ПЭМИ в диапазоне работы изделия. Не допускать контакта антенны изделия с металлическими предметами и проводами, как источниками переизлученных высокочастотных сигналов. Поэтому настройку изделия следует производить в одном из ближайших к проверяемому помещений, в котором, предположительно, уровень фона существенно не отличается, а установка "радиозакладок" либо невозможна, либо нецелесообразна. В качестве таких помещений обычно рассматривают помещения другого предназначения, но расположенные на том же этаже и с оконными проемами, выходящими на ту же сторону здания. Если объектом проверки является автомобиль или другое транспортное средство, то, обеспечив правильный выбор места работ, настройку "нулевого" порога следует проводить не ближе 10-20 метров от него. После установки "нулевого" порога изделие перемещают в контролируемое помещение (к контролируемому объекту) БЕЗ ВЫКЛЮЧЕНИЯ ПИТАНИЯ. Ибо каждое последующее его включение приводит к автоматической установке порога уже применительно к новым условиям электромагнитной обстановки. Выполнив изложенные выше правила и ограничения, можно считать проверяемое помещение (объект) и изделие ST 033 "Пиранья" подготовленными к проведению контрольно-поисковых работ Поиск автономных радиомикрофонов и телефонных радиоретрансляторов целесообразно осуществлять, отключив от розеток электросети шнуры питания всех санкционированных потребителей и выключить осветительные приборы с лампами накаливания. С учетом того, что радиочастотный тракт изделия ST 033 "Пиранья" выполнен по совмещенной схеме детектора-частотомера, для его применения пригодны те же приемы и методы, как и для автономных детекторов поля, интерсепторов и радиочастотомеров. В целом они заключаются в следующем. Если не накладываются ограничения на скрытность проведения работ, то наилучший эффект дает сочетание амплитудного метода и метода "акустозавязки". При проведении скрытного поиска необходимо ориентироваться на амплитудный метод с прослушиванием детектированных сигналов через головные телефоны. Особое внимание обращается на радиоизлучения в диапазоне 60-640МГц, наиболее типичном для использования радиомикрофонами и телефонными радиоретрансляторами. Поиск осуществляется путем планомерного обхода помещения (объекта) с движением вдоль стен и обследованием мебели и других расположенных в нем предметов. Ввиду достаточно большой чувствительности высокочастотной антенны поиск целесообразно начинать с применением телескопической антенны. При обходе антенну необходимо ориентировать в разных плоскостях, совершая плавные, медленные повороты основного блока и добиваясь максимального уровня сигнала. Антенну изделия целесообразно держать на расстоянии не более 20-25 см от обследуемых поверхностей и предметов. При отсутствии ограничений на использование метода "акустозавязки" динамик встроенного громкоговорителя изделия следует ориентировать в сторону обследуемых поверхностей и предметов.

При приближении антенны изделия ST 033 "Пиранья" к месту размещения "радиозакладки" напряженность электромагнитного поля возрастает, соответственно повышается и уровень сигнала на его входе. С превышением уровнем сигнала установленного "нулевого" порога, в зависимости от вида сигнала, увеличивается количество окрашенных секторов одной из строк индикаторов уровня и, начиная с четвертого (отсчет от нулевой отметки), возрастает частота щелчков звуковой сигнализации в режиме "TONE", а при включении режима "AUD" и динамика громкоговорителя возникает "акустозавязка". В случае нахождения источника с частотномодулированным сигналом будет увеличиваться количество окрашенных секторов верхнего индикатора уровня сигнала. При достаточном приближении к источнику радиочастотомер осуществляет "захват" частоты и показывает в последней строке экрана ее значение по результатам нескольких измерений. Путем уменьшения громкости кнопкой "-", изменения границ динамического диапазона кнопкой "SET", увеличения вручную порога срабатывания детектора, постоянного наблюдения за показаниями частотомера сужается зона обследования и, тем самым, локализуется место установки "радиозакладки" с погрешностью в пределах 10-15 см. Дополнительные возможности, прежде всего по классификации радиоизлучений, дает периодическое включение режима "AUD" и прослушивание демодулированного сигнала. Однако необходимо помнить, что эффект "акустозавязки" и отчетливое прослушивание демодулированного сигнала наблюдаются не всегда. Например, если закладки имеют маскированный радиоканал. Поэтому в основе их поиска лежит использование амплитудного метода в чистом виде. Дополняющим здесь может быть простой прием. Если выключить источник тестовой фонограммы и создать в проверяемом помещении короткий резкий звук (сильный хлопок, удар по крышке стола или металлическому предмету), то можно зафиксировать характерные изменения демодулированного сигнала "на слух" в режиме "AUD", изменения осциллограммы в режиме "OSC" и спектрограммы в режиме "SA". В случае применения "радиозакладки" с цифровыми методами модуляции индикация повышения уровня будет происходить на нижнем индикаторе. Индикация частоты принимаего сигнала в данном случае будет случайной. В случае применения в качестве "радиозакладки" телефонов стандарта DECT или GSM, помимо индикации повышения уровня сигнала в нижней строке, на индикаторе появится надпись DECT или GSM. Аналогично поиску радиомикрофонов осуществляется поиск телефонных радиоретрансляторов. При этом для их активизации необходимо снять трубки всех телефонных аппаратов. Собственно поиск проводится в два этапа. Сначала на наличие закладных устройств проверяются сами телефонные аппараты. Установленный в аппарате радиоретранслятор проявляется точно так же как и радиомикрофон. При приближении антенны изделия к такому телефонному аппарату реагируют средства звуковой (в режиме "TONE") индикации, индикатор уровня сигнала и частотомер. При переключении в режим "AUD" в динамике или в головных телефонах прослушивается либо непрерывный, либо прерывистый тональный сигнал телефонной станции. В ряде случаев при приближении микрофона телефонной трубки к динамику изделия ST 033 "Пиранья" может возникнуть эффект "акустозавязки". Не рекомендуется проверять телефонные аппараты в режиме громкоговорящей связи (если он предусмотрен), так как в этом случае может возникнуть ложная "акустозавязка" между микрофоном и динамиком самого аппарата. Далее поиск телефонных радиоретрансляторов осуществляется путем обхода помещения вдоль абонентской телефонной линии и выявления на ней мест с возрастанием (максимумом) уровня радиосигнала. При обходе антенну изделия необходимо ориентировать в разных плоскостях на минимально возможном расстоянии от линии. Практически всегда существует необходимость проверки линии вплоть до основного распределительного щита.

Особое внимание следует обращать на распределительные коробки и места, где линия проложена скрытой проводкой. Установленные на линии телефонные радиоретрансляторы локализуются, в основном, амплитудным методом, дополняемым проверкой на возникновение "акустозавязки". Поиск камуфлированных радиомикрофонов, питающихся от электросети, и локализация места их установки осуществляется теми же методами, которые были охарактеризованы выше. Для их активизации необходимо включить тестовый источник звука. Поочередно включить имеющиеся осветительные изделия с лампами накаливания и подключить к розеткам электросети шнуры питания санкционированных потребителей. Последовательно провести обследование каждого из вновь подключенных средств. Поиск радиостетоскопов имеет определённые особенности, обусловленные способами их применения (установка вне контролируемого помещения). Поэтому для обнаружения сигналов радиостетоскопов необходимо обследовать все реально доступные внешние поверхности ограждающих помещение конструкций. Поскольку средой распространения виброакустических колебаний могут являться трубы отопления и водоснабжения, то проверке подлежат и эти коммуникации. В подавляющем большинстве радиостетоскопы используют открытый радиоканал. Это дает возможность анализа принятого сигнала "на слух" в режиме "AUD". При проверке ограждающих помещение конструкций антенну изделия следует располагать на минимально возможном расстоянии от обследуемых поверхностей, так как радиус зоны обнаружения сигнала от радиостетоскопа обычно меньше, чем от радиомикрофонов. При проверке трубопроводных коммуникаций необходимо выполнять эти же рекомендации, но не допускать контакта антенны с металлическими поверхностями. Локализация радиостетоскопов осуществляется амплитудным методом в смежных помещениях, дополняемым, при необходимости, использованием режимов "OSC" и "SA".

Поиск скрытых видеокамер с радиоканалом передачи изображения (часто и звука) сопряжен с некоторыми трудностями, которые определяются сходством сигнала видеопередатчика с сигналом яркости передатчиков телевизионного вещания и работой значительного количества этих устройств в диапазоне телестанций (от 60 до 500МГц). Поэтому в ходе проведения работ при обнаружении такого сигнала первой является задача его распознавания по критерию "внешний-внутренний". Для распознавания необходимо закрыть окна шторами или жалюзи, оставив включенным внутреннее освещение. Произвести несколько раз включение и выключение искусственного освещения. При включенном режиме "AUD" должны прослушиваться отчетливые изменения тона продетектированного сигнала. Для повышения надежности распознавания включить режим "OSC" и убедиться в изменении структуры сигнала по осциллограмме при включении и выключении освещения. Вид осциллограммы радиосигнала передачи видеоинформации при различных значениях параметров горизонтальной развёртки показан на рисунках 7 и 8.

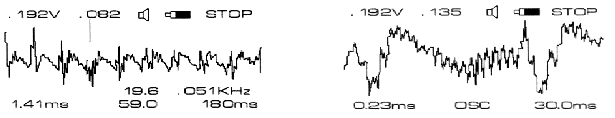


                                                   Рис.7                                                                       Рис.8

Радиосигнал передачи видеоинформации, период развертки 180 мс.

Радиосигнал передачи видеоинформации, период развертки 30 мс. Если результаты такой проверки положительны, то сигнал уверенно можно отнести к категории внутренних, создаваемых передатчиком видеокамеры, так как изменение освещенности помещения на параметры сигнала телевизионного вещания не влияет. Принципиально передатчики видеокамер могут работать на частотах до 2300МГц. Обнаружение сигнала (похожего на сигнал яркости) на частотах вне диапазона телевизионного вещания практически однозначно свидетельствует о работе передатчика скрытой видеокамеры. Локализация таких средств осуществляется амплитудным методом. Применительно к пространственному высокочастотному облучению основной является задача выявления факта создания этого искусственного канала добывания информации. Обычно она решается в два этапа. На первом этапе выявляется факт облучения помещения высокочастотным сигналом. На втором этапе отслеживается отклик на зондирующий высокочастотный сигнал. При этом необходимо ориентироваться на следующие моменты. Остронаправленный луч электромагнитной энергии может быть сформирован только на очень высоких частотах (800-900МГц и выше). Особенности распространения радиоволн этого диапазона (необходимость "прямой видимости" между источником излучения и облучаемыми предметами) определяют в качестве основных путей их проникновения в контролируемое помещение, прежде всего, оконные проемы. Переизлучающими объектами могут быть обычные для данного помещения технические средства, обладающие так называемым микрофонным эффектом (паразитные акустоэлектрические преобразователи). К ним обычно относят динамики бытовых громкоговорителей, акустические системы даже выключенной аудиоаппаратуры, телефонные аппараты с электрическим звонком и т.п. Переизлученный на частотах высших (чаще всего второй или третьей) гармоник сигнал локализуется в непосредственной близости от облучаемых предметов и имеет модуляцию акустическим фоном помещения. Исходя из этого, может быть использован следующий порядок работы. Для выявления факта высокочастотного облучения поочередно обследовать потенциально опасные оконные проемы. Для этого поднести антенну к внутреннему стеклу на расстояние 5-10 см, зафиксировать уровень и частоту наиболее мощного сигнала. Включить режим "AUD" и "на слух" определить наличие и особенности демодулированного сигнала. По графическому индикатору оценить стабильность частоты излучения. Перейти в любое из соседних помещений (ориентированных окнами в ту же сторону) и повторить проверку в районе каждого из его оконных проемов. Высокочастотное облучение вполне вероятно, если: частота принимаемого сигнала лежит (или очень близка) в пределах указанного диапазона; стабильность частоты высокая; модуляция сигнала отсутствует; в соседних, по отношению к проверяемому, помещениях уровень принимаемого сигнала существенно меньше. Для выявления источников переизлучения необходимо тщательно обследовать каждый из потенциально опасных предметов, размещая антенну изделия в непосредственной близости к нему. Основанием для принятия конечного решения об облучении и о наличии в помещении переизлучающих предметов являются показания индикатора уровня изделия ST 033 "Пиранья" и его частотомера, а также результаты прослушивания в режиме "AUD". При этом в качестве основных признаков обычно рассматривают фиксацию номинала частоты, кратного максимум третьей гармонике облучающего сигнала, и идентификацию звукового сигнала в режиме "AUD" с акустическим фоном помещения. Проверку ПЭВМ на наличие в них "радиозакладок" целесообразно проводить в последнюю очередь. Это обусловлено тем, что во включенном состоянии они создают достаточно интенсивные побочные радиоизлучения в диапазоне до 1000МГц и выше, то есть являются источниками повышения электромагнитного фона, который может "маскировать" излучения ранее рассмотренных радиозакладных устройств. При этом необходимо иметь в виду, что "радиозакладки" могут передавать как сигналы, соответствующие изображению на экране монитора, так и сигналы, несущие цифровую информацию, обрабатываемую элементами системного блока. И те, и другие сигналы имеют достаточно отчетливые внешние признаки, проявляющиеся на их осциллограммах в режиме "OSC". Первые по структуре схожи с сигналом передатчиков видеокамер, а вторые представляют собой четко обозначенную импульсную последовательность. Для обнаружения сигналов "радиозакладок" необходимо перемещать антенну изделия ST 033 "Пиранья" вокруг монитора и системного блока, фиксируя уровень принимаемого сигнала и показания частотомера. Наличию в ПЭВМ "радиозакладки" и ее работе на передачу соответствуют резкое возрастание уровня принимаемого сигнала и относительно высокая стабильность частоты. В этом случае следует зафиксировать положение антенны, которому соответствует максимальный уровень, включить режим "OSC" и визуально оценить вид сигнала. Для исключения ошибочных выводов сравнить его с осциллограммой побочных электромагнитных излучений монитора ПЭВМ, вид которой показан на рисунке 9.



Рис.9

ПЭМИ монитора ПЭВМ Определение места установки "радиозакладки" осуществляется, кроме того, путем последовательного включения и выключения монитора и системного блока.

ПРИМЕЧАНИЕ: Методика поиска и локализации несанкционированно включенных на передачу радиостанций, радиотелефонов, телефонов с радиоудлинителями и радиомаяков полностью аналогична методике поиска и локализации радиомикрофонов. Причем в подавляющем большинстве случаев следует ориентироваться на амплитудный метод с периодическим прослушиванием демодулированного сигнала в режиме "AUD".

2. ИСПОЛЬЗОВАНИЕ ИЗДЕЛИЯ ДЛЯ ВЫЯВЛЕНИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ ПО ПРОВОДНЫМ ЛИНИЯМ РАЗЛИЧНОГО НАЗНАЧЕНИЯ

Здесь рассматриваются приёмы выявления искусственно созданных каналов утечки информации по проводным линиям, в основе которых лежит использование специальных технических средств. Основными видами проводных линий, для анализа которых предназначено изделие ST 033 "Пиранья", являются линии электросети (высокопотенциальные линии), а также абонентские телефонные линии и линии систем пожарной и охранной сигнализации (низкопотенциальные линии). В целом приёмы и методы, применяемые для проверки проводных линий названных видов, одинаковы. Подключение к ним осуществляется с использованием единого, универсального адаптера. Анализу методом сканирования подвергается общий диапазон от 0 до 15МГц. Вывод результатов сканирования производится в виде изображения панорамы с однотипным представлением (отображением) измеренных параметров. Функции органов управления изделием одинаковы (вне зависимости от вида проверяемой линии). Общие (для всех линий) положения методики работы состоят в следующем. Проведение подготовки контролируемого помещения заключается в проверке соответствия количества и назначения реально существующих в нём проводных линий ранее изготовленным (представленным) схемам их прокладки. Подготовка самого изделия ST 033 "Пиранья" (после проверки его работоспособности в данном режиме) фактически состоит только в выборе наиболее удобных наконечников к щупам, применительно к типу и особенностям имеющихся проводных линий. Наибольшее внимание следует уделять диапазону 40-2500кГц, как наиболее типичному для использования закладками, питающимися от напряжения проводных линий и передающих перехваченную информацию по их проводам. Значительно реже встречаются закладные устройства с частотами около 7МГц и выше. Для обеспечения гарантированной надёжности не пропуска сигналов закладок по частоте верхняя граница диапазона сканирования в изделие ST 033 "Пиранья" определена на уровне 15МГц. Рекомендуется следующий порядок действий оператора. Включить изделие. Дождаться начала сканирования в диапазоне до 10.450МГц и после завершения 2-3-х циклов установить верхнюю границу диапазона на уровне 15МГц. Внимательно изучив наиболее характерные особенности изображения панорамы определить наличие частотных составляющих, превышающих уровень общего фона. При необходимости разбить диапазон на отдельные интервалы и просканировать их подробно, останавливаясь, прежде всего, на частотах наиболее интенсивных составляющих. Границы интервалов задаются последовательным нажатием кнопок "SET", "4", кнопок с цифровой маркировкой и кнопки "ENTER" (либо альтернативнй вариант с заданием центральной частоты и ширины полосы). Установить нижний порог индикации уровня сигнала порядка 10-15%. Для этого нажать кнопку "SET", кнопкой "3" вывести надпись "3 ->THRESHOLD level", нажать кнопку "ENTER" и кнопками "5" и "6" добиться установки этого порога индикации. В последующем, в зависимости от характера изображения панорамы, выбрать наиболее удобный для анализа уровень порога. Запуск и остановка сканирования осуществляется нажатием кнопки "RUN/STOP". После прохода нескольких циклов сканирования можно обоснованно установить порог "автостопа" для чего нажать кнопку "SET", выбрать кнопкой "3" режим "SQUELCH LEVEL", подтвердить выбор кнопкой "ENTER" и, манипулируя кнопками "5" и "6", поставить курсор на необходимый уровень. После остановки на частоте того или иного сигнала следует произвести точную настройку кнопками "3" и "4", одновременно анализируя сигнал "на слух" поочерёдным включением детекторов "AM" и "FM" кнопкой "ENTER". Для анализа слабых сигналов можно выбрать кнопками "SET", "5" и "ENTER" более удобный амплитудный диапазон (0,1-1мВ). При необходимости дополнить возможности анализа сигналов в проводных линиях переключением изделия в режимы "OSC" и "SA", так как изображения осциллограмм и спектрограмм сигналов, выводимые на экран дисплея, дают более детальную характеристику параметров. В этом можно убедиться сравнением изображений панорамы и осциллограммы одного и того же цифрового сигнала передачи речевой информации (см. рис.10 и рис.11).

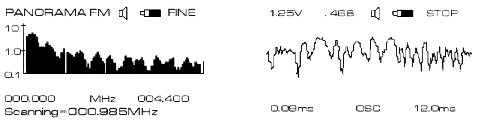


Рис.10 Панорама цифрового сигнала передачи речевой информации в проводной линии.

Рис.11 Осциллограмма цифрового сигнала передачи речевой информации в проводной линии (тот же сигнал).

ПРИМЕЧАНИЕ. Если помещение включено в план регулярных периодических проверок, то целесообразно сохранить в энергонезависимой памяти панораму (осциллограмму, спектрограмму) необходимых частотных интервалов. Для сохранения нажать кнопку "SAVE" и "ENTER". Для вызова из памяти нужной панорамы (осциллограммы, спектрограммы) нажимать кнопку "LOAD". Вместе с тем, необходимо учитывать и некоторые особенности, определяемые спецификой линий каждого вида. Проверку наличия в электросети специальных технических средств, принимающих акустические сигналы из помещения, питающихся от сети и передающих информацию на высокой частоте по её проводам, целесообразно начинать с сетевых розеток. Для уменьшения уровня фона следует отключить (с видимым отсоединением от розеток) все электроприборы и аппаратуру, размещённую в контролируемом помещении. Подключить изделие к сети, используя для этого любую из розеток (как правило энергообеспечение помещения осуществляется от одной фазы или, по крайней мере, от одного распределительного щитка). Провести анализ изображения панорамы. Если обнаружен сигнал, содержащий признаки модуляции акустикой помещения, то для локализации его источника может быть использован метод "акустозавязки", при поочерёдном подключении ко всем розеткам в проверяемом помещении. Аналогичную проверку провести на элементах линий, питающих электроосветительные приборы. После проверки силовых линий и линий, питающих осветительные приборы, необходимо проверить тройники, удлинители и другие электропотребляющие средства путём их поочерёдного подключения к электросети. Проверка проводных линий систем пожарной и охранной сигнализации, а также линий неизвестного предназначения аналогична проверке линий электросети, так как аналогичны сами технические средства, используемые на этих коммуникациях. При проверке абонентских телефонных линий, помимо поиска описанных выше специальных технических средств, необходимо решать задачу выявления факта использования линии для добывания акустической информации из помещения за счет линейного высокочастотного навязывания. Признаком факта линейного высокочастотного навязывания является наличие в линии немодулированного стабильного зондирующего сигнала на частотах не ниже 150 кГц. При этом порядок подключения изделия и процедура анализа не отличается от изложенного применительно к проверке линий электросети.

3. ИСПОЛЬЗОВАНИЕ ИЗДЕЛИЯ ДЛЯ ВЫЯВЛЕНИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ В ИНФРАКРАСНОМ ДИАПАЗОНЕ

Принципиально следует рассматривать два вида таких каналов утечки информации. Один из них создается за счет применения специальных технических средств с передачей перехваченной информации в инфракрасном диапазоне. Другой канал основан на облучении стекол оконных проемов направленным лучом источника инфракрасных излучений и приеме отраженного сигнала, промодулированного акустикой помещения. Для выявления обоих каналов утечки необходимо провести одинаковые подготовительные мероприятия. Прежде всего следует правильно выбрать время проведения проверки, а именно такое, когда в окна контролируемого помещения не попадают прямые солнечные лучи. В самом помещении необходимо выключить лампы накаливания и источники интенсивного теплового излучения. Целесообразно также выключить, если он имеется, цветной телевизор, так как датчик изделия может реагировать на "теплые" тона изображения. Специфика инфракрасных закладок предопределяет необходимость обеспечения "прямой видимости" между передатчиком закладки и приемником инфракрасных излучений. Поэтому в помещении путь прохождения излучения передатчика наружу может проходить только через оконные проемы. С учетом этих особенностей, поиск опасных сигналов следует начинать от окон помещения, передвигаясь в глубь его. Поскольку у передатчика может быть достаточно узкая диаграмма направленности, а угол зрения датчика изделия составляет 300, необходимо плавно изменять пространственную ориентацию датчика. Признаком наличия инфракрасного излучения является появление окрашенных сегментов шкалы индикатора уровня и щелчков звуковой индикации в режиме "TONE" после окрашивания 4-го элемента шкалы. Анализ обнаруженных сигналов может производиться "на слух" в режиме "AUD", а также визуально с использованием встроенных осциллографа и анализатора спектра. Локализация источников инфракрасного излучения наиболее точно осуществляется сочетанием амплитудного метода и метода "акустозавязки". При этом порядок действий такой же как и при работе в режиме высокочастотного детектора-частотомера. Для выявления внешних потенциально опасных инфракрасных излучений необходимо обследовать каждый оконный проем. При этом датчик ориентируется в сторону окна. Плавно изменяя его пространственное положение, провести обследование всей площади оконного проема. Поскольку зондирующий сигнал не имеет модуляции, то его наличие может быть оценено только по показаниям индикатора уровня и тональной индикации в режиме "TONE". 4. ИСПОЛЬЗОВАНИЕ ИЗДЕЛИЯ ДЛЯ ВЫЯВЛЕНИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ ПО НИЗКОЧАСТОТНЫМ МАГНИТНЫМ ПОЛЯМ Для таких каналов характерно то, что они возникают при использовании по целевому предназначению санкционированных средств (ПЭВМ, переговорных устройств, систем звукоусиления, магнитофонов, телефонов и т.д.). Поэтому одной из основных задач следует считать исследование таких средств на наличие, интенсивность и дальность низкочастотного магнитного поля. Сопутствующими могут считаться задачи поиска скрытой (несанкционированно проложенной) проводки и обнаружения работающих диктофонов. Перед проведением работ целесообразно выключить в помещении люминесцентные светильники, а антенну изделия, при необходимости, включить в дифференциальном режиме (переключатель на корпусе антенны поставить в положение "к белой точке"). Потенциальные источники опасных низкочастотных магнитных полей следует проверять раздельно, включая их в работу поочередно. При исследовании технических средств необходимо оценить дальность распространения магнитных полей и особенности их спектра. Для этого первоначально разместить магнитную антенну в непосредственной близости к исследуемому объекту. Зафиксировать по осциллограмме относительный уровень поля. Удаляясь от исследуемого средства и изменяя пространственную ориентацию антенны, оценить дальность уверенного приема низкочастотного сигнала. Применительно к усилителям звуковой частоты, имеющим выходной трансформатор, следует оценить дальность уверенного (разборчивого) приёма речевого (тестового) сигнала. Такая оценка может послужить основой для правильного выбора мест установки соответствующих средств по отношению к наружной стороне помещения и варианта их совместного расположения в помещении. При необходимости включить режим "SA", проанализировать спектрограмму и записать ее в энергонезависимую память. Для поиска скрытой проводки необходимо последовательно обойти все стены помещения, располагая магнитную антенну в непосредственной близости к ним. Зафиксировать область возрастания уровня поля и путем перемещения антенны по горизонтали и вертикали определить прохождение трассы скрытой проводки. Возможность обнаружения работающих диктофонов определяется как уровнем магнитного поля, создаваемого их двигателями, так и уровнем магнитного фона помещения. Для решения этой задачи обычно применяют специализированные средства с предварительной тщательной подготовкой помещения. Поэтому не всегда может быть достигнут положительный результат только при использовании изделия ST 033 "Пиранья", особенно на расстоянии между диктофоном и магнитной антенной 30 см и более.

5. ИСПОЛЬЗОВАНИЕ ИЗДЕЛИЯ ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ ВИБРОАКУСТИЧЕСКОЙ ЗАЩИТЫ И ЗВУКОИЗОЛЯЦИИ ПОМЕЩЕНИЙ

Объединение этих направлений использования изделия определяется общностью источников возникновения каналов утечки информации (речевой сигнал в акустическом диапазоне), сходством приёмов контроля и практической идентичностью задействования возможностей ST 033 "Пиранья". Во-первых, и в том, и в другом случае при подготовке помещения необходимо выключить приборы и средства, создающие дополнительный акустический фон. Во-вторых, в обоих случаях следует использовать тестовые, а лучше всего калиброванные, источники звукового сигнала. В-третьих, в смежных, по отношению к проверяемому, помещениях должен быть обеспечен минимально возможный уровень акустического фона. В-четвёртых, применяют практически одинаковые методы анализа сигналов ("на слух", по осциллограммам и спектрограммам). Оценка эффективности виброакустической защиты помещения обычно проводится в два этапа. На первом этапе защита, если она имеется, должна быть выключена и произведена проверка собственно виброакустических свойств ограждающих помещение поверхностей. Для этого необходимо виброакустический датчик прикреплять в различных местах проверяемых поверхностей (стен, дверей, окон, по возможности пола и потолка) с внешней, по отношению к контролируемому помещению, стороны. Включить источник тестового звукового сигнала. Он может размещаться либо в обычном месте ведения конфиденциальных разговоров, либо на определённом расстоянии от обследуемой поверхности (например, как показано на рисунке 12).

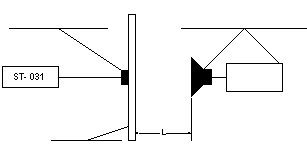


Рис.12. Вариант схемы оценки виброакустических свойств и виброакустической защиты помещений.

Уровень звука обычно устанавливают соответствующим громкой речи (74дБ). Для калиброванных источников звука расстояние "L" выбирают в пределах 1,0-2,0м. Сначала на качественном уровне (путём прямого прослушивания) оцениваются виброакустические свойства обследуемых поверхностей, а затем, переходом в режим "SA", количественно оцениваются амплитуды частотных составляющих тестового сигнала. На втором этапе, если это предусмотрено, оценивается эффективность системы виброакустической защиты. Для этого на каждой поверхности как качественно "на слух", так и количественно по спектрограмме определяется соотношения уровней тестового и маскирующего сигнала, а также выявляются "не прикрытые" составляющие спектра. Это служит объективной основой коррекции амплитудно-частотной характеристики источников маскирующего сигнала. Согласно общепринятым правилам разборчивость речевых сигналов гарантированно не восстанавливается, если маскирующий шум (помеха) в 4-5 раз (16дБ) превышает их уровень. Полное исключение признаков речи достигается при 8-ми кратном превышении уровня сигнала помехой, создаваемой системой активной защиты. Оценку звукоизоляции помещений также целесообразно проводить в два этапа. На первом этапе, используя тестовый источник сигнала с уровнем звука, соответствующим громкой речи, установить соответствие между этим уровнем и показаниями изделия ST 033 в режимах осциллографа и анализатора спектра. Для этого (см. рисунок 13) разместить акустический излучатель источника звука и микрофон изделия ST 033 на некотором фиксированном расстоянии. Обычно его выбирают в пределах 1,0-2,0м.

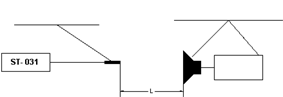


Рис.13. Вариант схемы калибровки индикаторов уровня звукового сигнала изделия ST 033.

На втором этапе оцениваются звукоизоляционные свойства ограждающих помещение поверхностей (стен, дверей, окон, а если возможно, то пола и потолка), эффективность системы активной защиты (зашумления), а также возможность утечки речевой акустической информации через элементы вентиляции, различного рода ниши, сквозные отверстия и т.п. Для оценки звукоизоляционных свойств стен, дверей (пола, потолка) тестовый источник звука может быть расположен либо в обычном месте ведения конфиденциальных разговоров, либо на расстоянии от обследуемой поверхности. Например, в варианте показанном на рисунке 14.

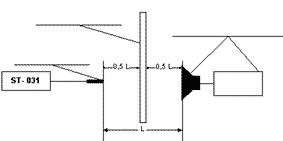


Рис.14. Вариант оценки звукоизоляции помещений.

Размещая микрофон в различных местах смежных (выше и ниже расположенных) помещений качественно "на слух" и количественно по спектрограмме определить дальность перехвата речевой информации из данного помещения и оценить снижение уровня звукового сигнала за счёт свойств ограждающих поверхностей, а также наличие наименее ослабленных составляющих спектра. Последнее даёт возможность принять обоснованное решение о необходимости дополнительной защиты, в том числе и активной, и выбор характеристик средств защиты. Если помещение расположено выше первого этажа, возникают определённые трудности в проверке звукоизоляции оконных конструкций. В этом случае достаточный для качественной оценки эффект даёт следующий, часто используемый приём. Тестовый источник звука размещается по любому из ранее рассмотренных вариантов. Открывается форточка, фрамуга или другая часть окна, в зависимости от особенностей оконных переплётов. Микрофон вывешивается наружу и в этом положении фиксируется уровень принимаемого им тестового сигнала из помещения. Затем открытая часть окна осторожно (чтобы не повредить кабель микрофона), но, по возможности, плотно прикрывается. Качественно "на слух" и количественно по осциллограмме или спектрограмме оцениваются звукоизоляционные свойства оконных конструкций. Поскольку воздуховоды систем вентиляции принято рассматривать в качестве наиболее опасных каналов утечки речевой акустической информации, то они подлежат обязательной проверке. Для этого микрофон прибора ST 033 необходимо ввести в выходное (входное) отверстие воздуховода каждого из смежных помещений, а возможно и некоторых других. Качественно "на слух" оценить прохождение и разборчивость сигнала от тестового источника, а по показаниям прибора ST 033 в режиме осциллографа или анализатора спектра его ослабление при прохождении по воздуховоду до места размещения микрофона. При этом правильная оценка ослабления может быть получена только в том случае, если имеется детальная схема системы вентиляции. Её наличие даёт возможность учесть ослабление, вносимое различными элементами конструкции воздуховодов.

Так, ослабление речевого сигнала обычно составляет:

* 0,15дБ/м - в прямых металлических воздуховодах;
* 0,2-0,3дБ/м - в прямых не металлических воздуховодах;
* 1,0-3,0дБ/м - при изменении сечения воздуховод;
* 3,0-7,0дБ/м - на один изгиб воздуховод.

Результаты проверки служат объективной основой для решения о необходимости дополнительной защиты, для выбора мер и средств её обеспечения.