МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

Ю.Ф. Каторин
А.В. Разумовский
А.И. Спивак

ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

Учебное пособие

Санкт-Петербург

2012

Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.

Учебное пособие посвящено теме борьбы с промышленным шпионажем. Авторы в простой и доступной форме излагают основные способы съёма конфиденциальной информации с помощью технических средств и принципы построения средств и систем защиты. Пособие предназначено для формирования у студентов знаний по основам инженерно-технической защиты информации, а также развития в процессе обучения системного мышления, необходимого для решения задач инженерно-технической защиты информации.

В полном объёме излагаемый материал рассчитан для подготовки студентов технических университетов по направлению: 090900 – «Информационная безопасность» и 090103 – «Организация и технология защиты информации».

Рекомендовано к печати учёным советом факультета КТиУ от 18 декабря 2012 г., протокол №10.

В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена программа его развития на 2009–2018 годы. В 2011 году Университет получил наименование «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

Оглавление

ВВЕДЕНИЕ

Понятие *промышленный шпионаж* возникло вместе с появлением промышленности и является неотъемлемой частью отношений в странах, где наряду с государственной существуют и другие формы собственности.

Сущность промышленного шпионажа – это стремление к овладению секретами конкурентов с целью получения максимальной коммерческой выгоды. Он заключается в получении любой информации о новейших научно-технических разработках (ноу-хау), коммерческих планах, состоянии дел и т. п. Ведется всеми доступными средствами, включая применение специальных технических средств и подкуп должностных лиц.

Однако, несмотря на то, что промышленный шпионаж в прямой постановке не затрагивает интересы государства, он является незаконным видом деятельности, так как покушается на конституционные права граждан. Государство стоит на защите этих прав, а значит, их нарушение ведет к уголовной ответственности.

Основная задача, которую авторы учебного пособия ставили перед собой, состоит в том, чтобы *защитить информационные системы и их пользователей от недобросовестных конкурентов*. Поскольку нельзя «победить противника», ничего не зная о нем и его средствах, то первая часть пособия посвящена именно рассмотрению методов и средств негласного получения информации.

За многовековой период своего развития человечество накопило огромную массу знаний о способах и средствах ведения разведки противоборствующей (конкурирующей) стороны. Понятно, что в основном это опыт военного характера, но он используется и для «мирной» реализации на ниве промышленного шпионажа.

Рассмотрим основные способы ведения разведывательных (шпионских) действий. Все они, независимо от того, кто и против кого их предпринимает, могут быть представлены в виде трех основных групп:

- на основе открытых источников;
- путем использования субъектов – носителей информации;
- через технические каналы.

К использованию *открытых источников* относятся способы добывания информации, реализуемые путем анализа газет, книг, научных и технических изданий, официальных отчетов и особенно рекламных материалов. Подобным образом работают большинство разведок мира. Понятно, что основная работа при этом ложится на специально подготовленных аналитиков, которые пропускают через себя горы материалов, отсеивая и накапливая необхо-

димую информацию. Главными направлениями получения открытого доступа к конфиденциальной информации здесь являются:

- доклады на конференциях, симпозиумах и других собраниях;
- вопросы, осторожно задаваемые специалистами;
- попытки пригласить на работу сотрудников конкурирующей фирмы и заполнение ими при этом специальных вопросников;
- прием на работу, обычно с резким увеличением оклада, служащего конкурирующей фирмы (своего рода законный подкуп);
- изучение выставочных образцов;
- притворные переговоры с конкурентами о приобретении лицензии или совместной деятельности и другие.

Все эти методы давно опробованы на Западе. По мере становления служб безопасности крупных коммерческих организаций и создания при них серьезных аналитических отделов, при условии привлечения специалистов из разведки, легальные источники сбора информации и в России займут подобающее им место в системе сбора данных.

Напомним главное правило – всегда нужно помнить о свойстве информации постепенно накапливаться. Поэтому, когда вы даете внешне безобидную рекламу или интервью, посылаете отчет или делаете доклад, всегда сопоставляйте их содержание с ранее «опубликованными» материалами; в сочетании с ними ваши откровения могут иметь совсем другое значение.

И, последнее замечание, хотя собирать открытую информацию легко, но она недостаточно достоверна, так как не менее легко дать по этому каналу и дезинформацию.

Использование субъектов – носителей информации принадлежит к другой группе способов промышленного шпионажа. Дело в том, что в ряду источников конфиденциальной информации люди занимают особое место, ибо способны выступать не только обладателями неких сведений, но и субъектами злонамеренных действий. В отличие от технического устройства их можно подкупить, шантажировать или просто обмануть, но при этом люди являются не просто обладателями и распространителями информации в пределах своих функциональных обязанностей, их возможности гораздо шире. Так, любой специалист, кроме того, что он является носителем информации, может ее анализировать, обобщать и делать выводы, то есть получать требуемые сведения по совокупности косвенных данных.

При определенных условиях люди способны скрывать, воровать, продавать информацию и совершать иные криминальные действия вплоть до вступления в устойчивые преступные связи со злоумышленниками. Правда, процесс выявления кандидата в агенты является достаточно сложным. Вначале проводится оценка и разработка кандидата, то есть изучение его личных

качеств и способностей, а также изыскание способов его наиболее эффективной вербовки и использования. Далее производится сама вербовка путём - шантажа, подкупа, идейных соображений, личного неприятия руководителя компании и т. д.

Очень часто агенту неизвестно, на кого он работает, либо ему дается неверная информация. Позднее, когда приобретут силу финансовые или другие средства контроля, завербованному, часто к его ужасу, раскрывают истинное имя хозяина. Впрочем, как показал богатый опыт спецслужб, более эффективной работы от агента можно добиться путем убеждения, а не угроз, и умные хозяева стремятся развивать дружеские отношения с ним.

Обнаружение скрытого агента – очень сложная и трудоемкая задача, требующая специальных навыков оперативной работы. Останавливаться на этих вопросах мы не будем, поскольку все материалы по методам ведения оперативной работы являются сугубо секретными, да и данная тематика выходит за рамки нашей книги и нашей квалификации. Отметим только, что при правильной организации деятельности фирмы большинство агентов (особенно обслуживающий персонал) не может обладать всей полнотой информации. В этом случае их используют для легального проникновения в помещения с целью установки подслушивающих устройств и исследования содержимого мусорных корзин.

Для некоторого затруднения деятельности таких агентов необходимо, прежде всего, определить строгий порядок и выделить специальные оборудованные помещения для ведения деловых бесед, чтобы исключить даже кратковременное «случайное» присутствие посторонних, в том числе и из своих сотрудников. Организовать максимально жесткий учет и строго регламентировать порядок работы с деловыми документами. Узаконить круг лиц, допускаемых к тем или иным внутрифирменным секретам, запретить сотрудникам вести служебные переговоры с домашних телефонов. При посторонних нельзя называть фамилию, имя, отчество собеседника. Назначая место встречи, надо переходить на условности и т. д. Но эти меры будут недостаточными, если нельзя исключить применение против вас технических средств несанкционированного съема информации.

Общая характеристика методов несанкционированного получения конфиденциальной информации *через технические каналы* и перечень используемых при этом средств приведены в табл. 1.

Как видно из таблицы, некоторые физические явления имеют место в разных действиях, т.е. на практике при съеме информации с объекта, эти явления зачастую смешиваются, это важно учитывать при защите объекта.

Таблица 1.

Действие	Физическое явление	Способ (средство) съема информации
1. Разговор нескольких лиц	Акустический сигнал	Подслушивание, в том числе случайное Диктофоны Закладные устройства с передачей информации по: имеющимся коммуникациям (трубам, цепям сигнализации, сетям 220 В, телефонным линиям...); специально проложенным проводам; радио- или ИК-каналу Направленный микрофон
	Виброакустический сигнал	Стетоскоп - Вибродатчик с передачей информации по: радиоканалу; проводам; коммуникациям; ИК-каналу Оптический лазерный микрофон
	Гидроакустический сигнал	Гидроакустический датчик
	Акустоэлектрический сигнал	Радиоприемник спецназначения
	Движение губ	Визуально, в том числе оптическими приборами Камера, в том числе с передачей по проводам и радиоканалу
2. Разговор по телефону	Акустический сигнал	Аналогично п. 1
	Электрический сигнал в линии	Параллельный телефон, прямое подключение, подключение через электромагнитный датчик, телефонная радиозакладка
	Побочные электромагнитные излучения (ПЭМИ) и наводки	Специальные радиотехнические устройства
3. Разговор по радиотелефону	Акустический сигнал Электромагнитные волны	Аппаратура п. 1 Специальные радиоприемные устройства

4. Документ на бумажном носителе	Наличие	Визуально, в том числе с помощью оптических средств; Фотографирование, в том числе с дистанционной передачей снимка; Копирование
5. Размножение документа на бумажном носителе	Следы на нижнем листе, копировальной бумаге или красящей ленте	Кража, визуально
	Шумы принтера	Спецаппаратура акустического контроля
	ПЭМИ от ЭВМ	Специальные радиотехнические устройства
6. Почтовые отправления	Наличие	Прочтение: со вскрытием, без вскрытия
7. Документ на небумажном носителе	Носитель	Копирование, вскрытие, несанкционированное использование ЭВМ
8. Изготовление документа на небумажном носителе	Изображение на дисплее	Визуально, в том числе с помощью оптических средств Фотографирование Видео- или телевизионные закладные устройства
	ПЭМИ	Специальные радиотехнические устройства
	Электрические сигналы в сетях	Аппаратные закладки
9. Передача документов на небумажном носителе.	Электрические сигналы	Несанкционированное подключение к информационной системе, имитация пользователя

Обеспечение информационной безопасности в России является одной из приоритетных государственных задач. Под *информационной безопасно-*

стью понимают состояние защищенности собственно информации и её носителей (человека, органов, систем и средств, обеспечивающих получение, обработку, хранение, передачу и использование информации) от различного вида угроз. Источники этих угроз могут быть *преднамеренными* (т.е. имеющими цель незаконного получения информации) и *непреднамеренными* (такую цель не преследующими).

Обеспечить безопасность информации можно различными методами и средствами как организационного, так и инженерного характера. Комплекс организационных мер, программных, технических и других методов и средств обеспечения безопасности информации образует систему защиты информации. При этом следует иметь в виду, что защите подлежит информация, содержащая сведения, отнесенные к государственной тайне, и другие конфиденциальные сведения.

В данном учебном пособие представлены материалы, посвященные рассмотрению технических каналов утечки информации, возникающих при работе технических средств обработки информации, технических мер и средств защиты, предотвращающих возможность перехвата информации с использованием этих каналов.

Защита информации рассматриваться как *Государственная политика информационной безопасности*. В настоящее время в Российской Федерации сформулирована *Концепция информационной безопасности* как составной части национальной безопасности России. В рамках проекта этой Концепции изложены основные положения государственной политики обеспечения информационной безопасности, имеющие большое значение для построения как государственной, так и ведомственных систем защиты информации и заключающиеся в следующем:

1) Государство формирует Федеральную программу информационной безопасности, объединяющую усилия государственных организаций и коммерческих структур в создании единой системы информационной безопасности России;

2) Государство формирует нормативно-правовую базу, регламентирующую права, обязанности и ответственность всех субъектов, действующих в информационной сфере;

3) Ограничение доступа к информации есть исключение из общего принципа открытости информации, и осуществляется только на основе законодательства;

4) Ответственность за сохранность, засекречивание и рассекречивание информации персонифицируется;

5) Доступ к какой-либо информации, а также вводимые ограничения доступа осуществляются с учетом определяемых законом прав собственности на эту информацию;

6) Юридические и физические лица, собирающие, накапливающие и обрабатывающие персональные данные и конфиденциальную информацию, несут ответственность перед законом за их сохранность и использование;

7) Государство осуществляет контроль за созданием и использованием средств защиты информации посредством их обязательной сертификации и лицензирования деятельности предприятий и организаций в области защиты информации;

8) Государство проводит протекционистскую политику, поддерживающую деятельность отечественных производителей средств информатизации и защиты информации, и осуществляет меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;

9) Государство стремится к отказу от зарубежных информационных технологий для информатизации органов государственной власти и управления по мере создания конкурентоспособных отечественных информационных технологий и средств информатизации;

10) Государство законными средствами обеспечивает защиту общества от ложной, искаженной и недостоверной информации, поступающей через средства массовой информации;

11) Государство способствует предоставлению гражданам доступа к мировым информационным ресурсам, глобальным информационным сетям;

12) Государство, прилагая усилия для противодействия информационной экспансии других стран, поддерживает интернационализацию глобальных информационных сетей и систем.

На основе приведенных выше положений государственной политики обеспечения информационной безопасности должны проводиться все мероприятия по защите информации в различных сферах деятельности государства. Это предполагает, в свою очередь, разработку соответствующего научно-технического и организационно-правового обеспечения защиты информации.

Научно-техническое обеспечение защиты информации должно быть направлено на достижение необходимого уровня защищенности информационных технологий, систем и средств информатизации и связи и заключается в проведении фундаментальных и прикладных исследований, создании защищенных технологий, средств и систем, а также создании средств и систем контроля состояния защиты информации.

Организационно-правовое обеспечение защиты информации должно представлять собой высокоупорядоченную совокупность организационных

решений, законов, нормативов и правил, регламентирующих как общую организацию работ по защите информации в масштабах государства и ведомства, так и создание и функционирование систем защиты информации на конкретных объектах.

Контроль состояния защиты информации (ЗИ) осуществляется с целью своевременного выявления и предотвращения утечки информации по техническим каналам, несанкционированного доступа к ней, преднамеренных программно-технических воздействий на информацию и оценки защиты ее от промышленного шпионажа, в том числе и иностранных технических разведок (ИТР).

Контроль заключается также в проверке выполнения актов законодательства Российской Федерации по вопросам ЗИ, решений Гостехкомиссии России, а также в оценке обоснованности и эффективности принятых мер защиты для обеспечения выполнения утвержденных требований и норм по ЗИ.

Угрозы безопасности информации реализуются через опасные воздействия со стороны источников угроз на определенные информационные объекты: информационные ресурсы, информационные системы и технологии, средства обеспечения автоматизированных информационных систем и технологий. При этом в зависимости от цели воздействия различают виды угроз.

1. Уничтожение. При уничтожении информационных объектов или их элементов они утрачиваются, т.е. либо переходят в руки посторонних лиц (например, при хищении), либо уничтожаются или разрушаются, например, в результате стихийного бедствия или вооруженного конфликта, неграмотных действий законных пользователей, преднамеренного введения в программное обеспечение определенного типа вирусов и т.п.

2. Утечка. При утечке информационные объекты не утрачиваются, однако становятся доступными посторонним лицам (например, случайное или преднамеренное подслушивание конфиденциального разговора, перехват излучений РЭС техническими средствами разведки, незаконное копирование информации в компьютерных системах, анализ и обобщение множества источников открытой информации и т.п.).

3. Искажение. Результатом искажения является несанкционированное изменение содержания, (структуры) информационного объекта (например, ввод ложной информации в систему обработки, изменение элементов программного обеспечения, изменение содержания банка данных и т.п.).

4. Блокирование. В результате блокирования информационный объект не утрачивается, но становится недоступным для его собственника, владельца или пользователя (потребителя) в результате физического или логического блокирования этого элемента.

Каждая из рассмотренных угроз при ее реализации может привести к серьёзным последствиям с точки зрения безопасности информации.

Работа систем информатизации и связи, а также ведение переговоров по закрытым вопросам сопровождаются возникновением акустических и электромагнитных полей, и (или) электрических сигналов, распространяющихся в различных средах (в воздухе, в токопроводящих конструкциях и т.д.). Поэтому существуют определенные предпосылки для образования каналов утечки информации (или технических каналов утечки информации) при работе различных технических средств и систем. Необходимым условием образования таких каналов является наличие опасного сигнала (т.е. сигнала, содержащего закрытую информацию) в тех полях, электрических и других сигналах, которые порождаются работой технических средств. Обнаружение, прием и анализ носителей опасного сигнала техническими средствами разведки позволяют несанкционированно получить закрытую информацию, обрабатываемую техническими средствами систем информатизации и связи.

В общем случае под техническим каналом утечки информации будем понимать совокупность *источника опасного сигнала*, *среды распространения носителя опасного сигнала* и *средства разведки*.

Возможность образования технических каналов утечки информации в системах и средствах информатизации и связи обусловлена следующими причинами:

- наличием информационных радио-, оптических и электрических сигналов в различных технических средствах передачи и обработки информации;
- наличием нежелательных электромагнитных излучений систем и средств информатизации и связи;
- образованием наводок электромагнитных излучений на различные токоведущие цепи и конструкции;
- применением специальных воздействий на элементы технических средств;
- применением различных закладных устройств;
- возникновением и распространением в окружающей среде акустических колебаний при обсуждении вопросов, содержащих секретные сведения;
- наличием случайных электроакустических преобразователей в отдельных элементах технических средств.

1. СРЕДСТВА ПЕРЕХВАТА АУДИОИНФОРМАЦИИ

1.1. Общие сведения о закладных устройствах

Один из эффективных путей негласного получения коммерческой информации основан на применении так называемых закладных устройств (ЗУ), скрытно устанавливаемых в местах возможного нахождения объектов наблюдения (конкурентов) либо подключаемых к используемым ими каналам связи. В настоящее время создано огромное количество типов таких устройств, различающихся принципом функционирования, способом передачи информации, дальностью действия, а также размером и внешним оформлением.

Самые миниатюрные ЗУ имеют вес всего в 1,5 г и линейные размеры – 2-5 миллиметров. Дальность передачи информации с таких устройств едва превышает 10 м. Более мощные устройства имеют размеры до нескольких сантиметров и позволяют осуществить передачу перехватываемой информации на дальность от нескольких сот до тысячи и более метров. Обычно ЗУ скрытно устанавливаются в элементах конструкций зданий и интерьера, крепятся под одеждой или камуфлируются под личные вещи.

Для того чтобы систематизировать представление о таких устройствах, целесообразно ввести пять признаков их классификации:

- по каналу передачи информации;
- по способу восприятия информации;
- по наличию устройства управления;
- по внешнему виду;
- по используемому источнику питания.

Рассмотрим отдельно каждый из классификационных признаков. В зависимости от *канала передачи информации* различают следующие типы ЗУ:

- радиозакладки;
- инфракрасные закладки;
- закладки с передачей информации по токоведущим линиям;
- закладки с записью на магнитофон.

В *радиозакладках* для передачи информации используется энергия электромагнитных волн, не влияющих на органы чувств человека, способных распространяться на значительные расстояния, преодолевая естественные и искусственные препятствия. Благодаря этим двум свойствам радиозакладные устройства позволяют с помощью специальной приемной аппаратуры вести скрытное наблюдение за интересующим объектом практически из любой удаленной точки.

С технической точки зрения, закладки могут работать практически в любом диапазоне радиоволн. Однако из конструктивных соображений наиболее используемые частоты – от 100 до 1000 МГц.

В *инфракрасных закладках* для передачи информации также используется энергия электромагнитных волн, но не радиодиапазона, а невидимой части оптической области спектра – инфракрасного диапазона. Благодаря малой длине такие волны распространяются узким пучком в заданном направлении, и их трудно обнаружить даже с помощью специальной аппаратуры. Дальность передачи информации от инфракрасных ЗУ достигает 500 м.

Однако высокая скрытность таких устройств существенно усложняет их применение. Так, инфракрасная закладка должна постоянно находиться в зоне прямой видимости приемника оптического излучения, а случайно попавший на линию визирования предмет, человек или автомобиль, а также изменившиеся погодные условия могут привести к существенному ухудшению качества или даже пропаданию сигнала в аппаратуре регистрации. Естественно, что такие ЗУ совершенно не применимы на мобильных объектах. В силу перечисленных недостатков инфракрасные закладки редко используются в практике промышленного шпионажа.

Закладки с передачей информации по токоведущим линиям используют свойство электрических сигналов распространяться на значительные расстояния по проводникам. Такие ЗУ обладают существенными достоинствами: высокой скрытностью передачи информации, большой дальностью действия, отсутствием необходимости в дополнительных источниках питания. Кроме того, они хорошо камуфлируются под элементы электрических цепей и токоприемники (розетки, тройники, электрические удлинители, настольные лампы и т. д.). В качестве токопроводящих линий используются либо специально проложенные провода, либо кабели электрических и телефонных сетей. В силу перечисленных обстоятельств ЗУ такого типа часто применяются недобросовестными конкурентами для получения сведений конфиденциального характера.

В случаях, когда отсутствует необходимость получения оперативной информации в реальном масштабе времени, а также имеется возможность скрытного извлечения и замены кассеты или магнитной ленты, закладка может оснащаться *магнитофоном* вместо устройства передачи по одному из рассмотренных каналов. Такой способ, как правило, применяется только в тех случаях, когда есть потенциальная угроза обнаружения объектом наблюдения канала передачи информации (например, с помощью специальной аппаратуры контроля).

В зависимости от *способа восприятия информации* различают три типа закладных устройств:

- микрофонного типа;
- вибрационного типа;
- с подключением к коммуникационным линиям.

Принцип действия ЗУ *микрофонного типа* основан на преобразовании акустических атмосферных колебаний в электрические сигналы и передаче их потребителю одним из вышеперечисленных способов.

Закладные устройства *вибрационного типа* (стетоскопы) перехватывают акустические колебания твердых сред (вибрации), возникающие вследствие давления атмосферных акустических волн на среды (см. рис. 1). В качестве чувствительных элементов в таких устройствах обычно используются пьезомикрофоны, электронные микрофоны или датчики акселерометрического типа. Они наиболее эффективны при фиксации на тонких «площадных» поверхностях (межкомнатных перегородках, стеклах, дверях и т. п.).

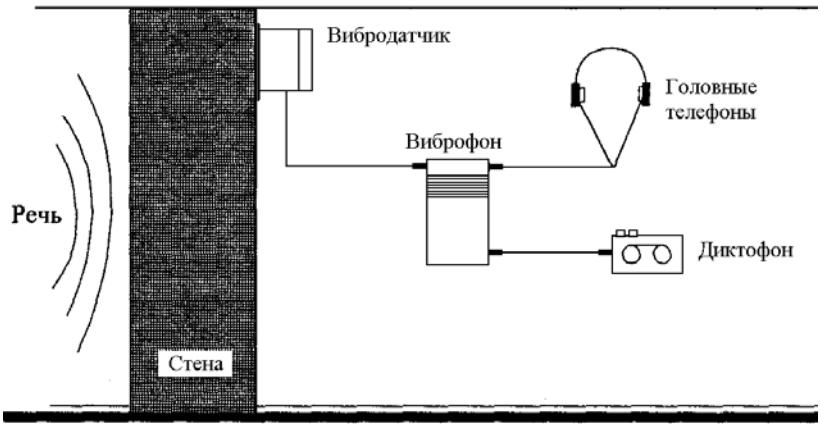

Рис. 1. Стетоскоп с передачей информации по специально проложенным проводным линиям

Для передачи информации потребителю, как правило, используется радиоканал, поэтому такие ЗУ обычно называют радиостетоскопами (рис. 2).

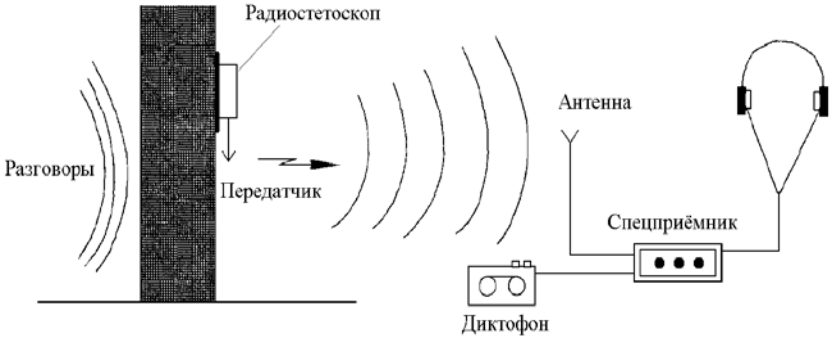

Рис. 2. Радиостетоскоп с передачей информации по радиоканалу

Закладные устройства *с подключением к коммуникационным линиям* предназначены для негласного перехвата информации, циркулирующей в телефонных или волоконно-оптических линиях. Такие ЗУ позволяют скрытно получать информацию о содержании телефонных переговоров, а также текстовых сообщений (телеграфных, факсимильных, электронной почты и т. д.). Для передачи информации с подключаемых ЗУ часто используется радиоканал. Такие ЗУ называют радиозакладными (РЗУ).

По способу подключения к телефонным линиям радиозакладки делят на две группы: РЗУ с непосредственным подключением, и РЗУ с индукционным подключением (см. рис. 3).

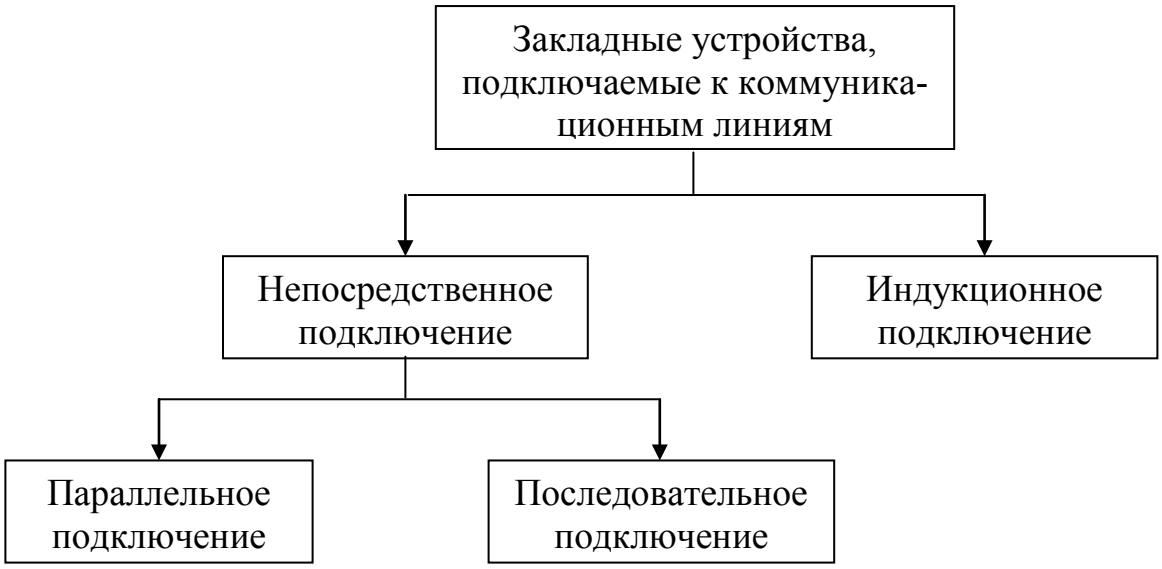

Рис. 3. Классификация ЗУ по способу подключения
к токопроводящим коммуникационным линиям

Первая группа – *радиозакладки с непосредственным подключением*.

Они подключаются либо одновременно к обоим проводам параллельно абоненту (параллельное подключение – рис. 4.*а*), либо в разрыв одного из проводов (последовательное подключение – рис. 4.*б*).

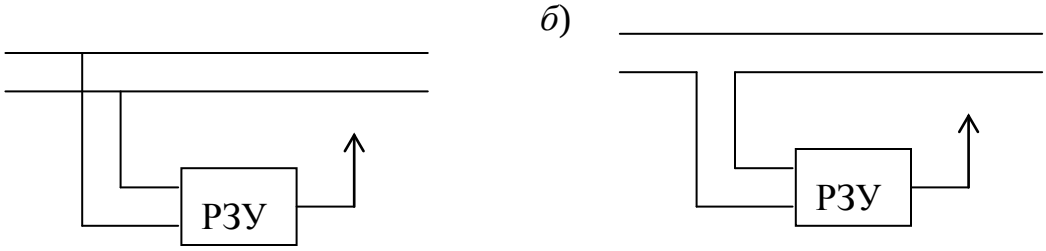

Рис. 4. Непосредственное подключение РЗУ:
а – параллельное, *б* – последовательное

Такие способы позволяют получить высокий уровень сигнала (его хорошее качество) на входе радиозакладки, а также появляется возможность обеспечить ее питание от линии. Однако закладки с непосредственным подключением могут быть легко обнаружены в связи с изменением параметров линии.

Этого недостатка в значительной степени лишены устройства второй группы – *радиозакладки с индукционным подключением* (см. рис. 5).

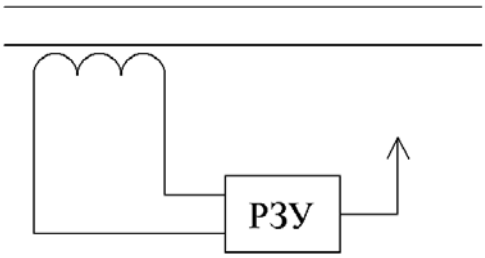

Рис. 5. Индукционное подключение РЗУ

В таких закладках чувствительным элементом выступает специальным образом построенная антенна, устанавливаемая вплотную к проводам телефонной линии. Электромагнитное поле, окружающее телефонные провода, наводит в антенне токи, содержащие информацию о характере сообщения. Эти токи усиливаются, преобразуются и далее полученная информация передается на пункт регистрации.

Закладные устройства для снятия информации с волоконно-оптических линий принципиально отличаются от рассмотренных выше только способом снятия информации. Для этих целей применяются специальные устройства сжатия волоконных линий, вызывающие интерференционные процессы на поверхности оптического волокна, которые и считываются фотоприемником.

По *наличию устройства управления* закладные устройства условно разделяют на три группы:

- с непрерывным излучением;
- с дистанционным управлением;
- с автоматическим включением при появлении сигнала.

ЗУ *с непрерывным излучением* наиболее просты в изготовлении, дешевы и предназначены для получения информации в течение ограниченного промежутка времени. Работа на излучение таких ЗУ начинается с момента подключения питания. Если источник питания автономный, то, как правило, время работы такого ЗУ не превышает 1–2 часа из-за большого потребления энергии на передачу сигнала. Время работы ЗУ, питающихся от линий (силовых или телефонных), практически неограничено.

Однако общим существенным недостатком для всех ЗУ с непрерывным излучением является возможность их обнаружения по излучению.

Существенно увеличить время непрерывной работы устройств с автономным питанием и повысить скрытность позволяет применение *дистанционного управления* ЗУ. Оно позволяет переводить устройство в режим излучения только в тех случаях, когда объект наблюдения ведет переговоры либо передает информацию по каналам связи.

Время излучения может быть дополнительно сокращено, если закладка содержит устройство накопления и сжатия сигнала.

Другим способом увеличения времени работы закладки является использование *устройств автоматического включения передатчика при появлении сигнала* (акустического либо электрического в линии).

Устройства включения от голоса называются *акустоматами*. Иногда их называют системами VAS или VOX. Закладка, оборудованная таким устройством, в обычном (дежурном) режиме работает как акустический приемник, потребляя незначительный ток. При появлении сигнала, например в начале разговора объекта наблюдения с кем-либо, подается напряжение на передатчик, и тот переходит в режим излучения. При пропадании акустического сигнала (прекращении разговора) через определенное время, обычно несколько секунд, передатчик выключается и закладка переходит в режим дежурного приема. Применение акустомата позволяет в несколько раз увеличить время работы закладного устройства. Однако их использование приводит к потере первых слов при каждом включении.

По *используемому источнику питания,* как было отмечено выше, ЗУ делятся на два вида:

- с собственным источником;
- с питанием от внешнего источника.

К *первому виду* относятся любые ЗУ, имеющие встроенный аккумулятор (батарейку).

Ко *второму* – ЗУ с передачей информации по токоведущим линиям и ЗУ с непосредственным подключением к коммуникационным линиям. Время работы таких устройств практически неограниченно.

По *внешнему виду* различают ЗУ: в обычном исполнении; в закамуфлированном виде.

В *обычном исполнении* устройства имеют, как правило, металлический корпус (окрашенный или нет) и форму параллелепипеда. Они достаточно универсальны и применяются в различных условиях обстановки.

Такие ЗУ маскируются одеждой, предметами интерьера (корзиной для бумаг, пластиковой коробкой, книгами, картиной и т. п.) либо местными предметами, пропускающими акустические и (или) электромагнитные коле-

бания (травой, смятым бумажным либо пластиковым пакетом, куском доски, фанеры и т. п.).

В *закамуфлированном виде* ЗУ применяются только в соответствии с конкретной обстановкой. Так, например, в виде силовой или телефонной розетки только в том случае, если другие неиспользуемые розетки в помещении имеют такой же внешний вид, в виде личных вещей (часов, зажигалки, заколки), если они соответствуют общему имиджу применяющего их человека.

1.2. Радиозакладки

Наиболее широкое применение в практике промышленного шпионажа нашли устройства с радиоканалом передачи перехватываемой информации, так называемые, радиозакладные устройства (РЗУ), или просто радиозакладки. Повышенный интерес к использованию РЗУ связан с их исключительно широкими возможностями по наблюдению за мобильными объектами, находящимися на значительном расстоянии.

Радиозакладные устройства как радиотехнические средства обладают рядом специфических особенностей, не свойственных другим ЗУ. В соответствии с этими особенностями для классификации радиозакладок могут быть использованы следующие классификационные признаки: принцип формирования сигнала, способ закрытия передаваемой информации и дальность действия.

В соответствии с *принципом формирования сигнала* РЗУ могут быть активные, полуактивные и пассивные.

Активные РЗУ

Активные РЗУ наиболее распространены. В общем виде они могут быть представлены структурной схемой, изображенной на рис. 6.

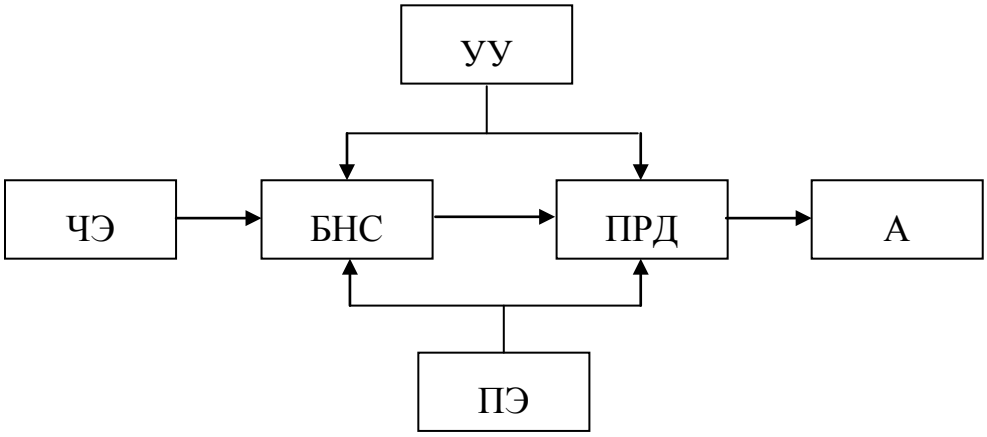

Рис. 6. Типовая структурная схема активного РЗУ

На рис. 6 приняты обозначения: УУ- устройство управления (например, *акустомат* или приемник сигналов от блока дистанционного управления); ЧЭ - чувствительный элемент (микрофон, вибродатчик или специальная антенна для перехвата электромагнитных полей коммуникационных линий и т. п.); БНС - блок накопления и сжатия информации, предназначенный для уменьшения времени работы РЭУ на излучение (до нескольких секунд за сеанс передачи); ПРД - передатчик, работающий на частотах, лежащих в диапазоне 100 - 1000 МГц; А - антенна (как правило, встроенная либо в виде отрезка изолированного провода длиной $L = \lambda/4$, где λ - длина волны излучения); ПЭ - питающий элемент (может отсутствовать, если РЭУ подключено к линии, находящейся под напряжением). Описание внешнего вида и основных характеристик некоторых активных РЗУ приведены в табл. 2.

Таблица 2.

Вид исполнения Индекс	Частота, МГц Вид модуляции	Вых. мощн., мВт Дальность действ., м	Габариты, мм Масса, г	Тип антенны Питание, В	Примечание, время работы, ч
Обычный РК1195-SS	427 Узкополосная частотная (±5 кГц)	1-100	20×55×5		Дистанционное управление. Акустомат (VOX). Цифровой сигнал с кодировкой
Обычный РК540-SS	427 Узкополосная частотная (±5 кГц)	20	65×50×30	Гибкая 9	Кварцевая стабилизация частоты. Кодирование сигнала
Обычный РК1970-SS	427 Двойная модуляция		80×50×20	Гибкая 9; 220	
Обычный РК1970	427 Широкополосная частотная	10 100	70×47×9	Гибкая 6-10	Цифровой скремблированный сигнал

Обычный РК2050	1.3 ГГц Частотная	10		Гибкая 220/110	Цифровой сигнал

Продолжение таблицы 2.

Обычный STG 4007	395.41 Узкополосная частотная	15 150	66×27×14 52 г	Гибкая 9	Акустомат 10
Обычный РК1380-S	115-200 Узкополосная частотная (±5 кГц)	40	33×33×20	Гибкая 9	Кварцевая стабилизация частоты. Кодирование сигнала (инверсия спектра)
Обычный SIM-PR-9000T	350-450 Широкополосная частотная (5 МГц)	100	70×39×5 51	Встроенная 6-10	Двухканальный режим работы Цифровое кодирование сигнала
Вид исполнения Индекс	Частота, МГц Вид модуляции	Вых. мощн., мВт Дальность действ., м	Габариты, мм Масса, г	Тип антенны Питание, В	Примечание, время работы
Деревянный брусок «Брусок – ЛЗБ ДУ»	Частотная	 300		Встроенная	Дистанционное управление. Кварц, стабил. частоты. Кодирование сигнала (сложная инверсия спектра). 25 суток

Лист упаковочного гофрокартона «Картонка ДУ»	300 Узкополосная частотная	0.5-20 50-250	6×10-70 $см^2$		Дистанционное управление (500 м на f=140-170мГц). Кварц, стабилизация частоты 50-400 ч; 3-12 мес. в дежурном режиме
Папка для документов «Папка ДУ»	300 Узкополосная частотная	0.5-50 50-500			Дистанционное управление (500 м на f=140-170мГц). Кварц, стабилизация частоты 20-500 ч; 3-12 мес. в дежурном режиме
Авторучка «Авторучка»	300 Широкополосная частотная	 100	135×10.5	Встроенная 2 элемента V393	Кварцевая стабилизация частоты 6 ч

Продолжение таблицы 2.

Вид исполнения Индекс	Частота, МГц Вид модуляции	Вых. мощн., мВт Дальность действ., м	Габариты, мм Масса, г	Тип антенны Питание, В	Примечание, время работы
Наручные часы РК1025-SS	427 Узкополосная частотная		∅25×4 40	 1,5	Кварцевая стабилизация частоты. Встроенный переключатель «вкл./выкл.». 6 ч

Кожаный ремень КС-1392	427 Широкополосная частотная	300 1-6×10^3	300	8×1,5	Кварцевая стабилизация частоты 8 ч
Зажигалка «Cricket»	447-459 Широкополосная частотная	100	77×22×13	Спиральная 2×1,5	Дальность перехвата разговора 10 м 25 ч
Калькулятор «Калькулятор-475»	470-475 Широкополосная частотная	50	140×9	Внутренняя 3,2	Схемотехническая стабилизация частоты 48 ч
Пачка сигар «РМ-пачка сигар»	630-640 Частотная	1		3	50

Полуактивные РЗУ

Полуактивные РЗУ характеризуются существенно большим временем функционирования от автономного источника питания: до 4000 часов. Положительный эффект достигается за счет комплексного использования энергии внешнего специально сформированного мощного зондирующего сигнала и энергии собственного питающего элемента. При этом энергия собственного аккумулятора тратится лишь на модуляцию принимаемого высокочастотного сигнала и его усиление.

Так как такие радиозакладки могут работать только при наличии внешнего зондирующего электромагнитного поля, то они получили название «аудиотранспондеры» («аудиоответчики») от английского «audiotransponder».

Структурная схема полуактивного РЗУ показана на рис. 7, где приняты следующие обозначения: ПрмА и ПрдА приёмная и передающая антенны, соответственно; М – модулятор; У – усилитель; ЧЭ - чувствительный элемент; ПЭ - питающий элемент.

Примером аудиотранспондеров могут служить радиозакладки SIM-ATP-16 и SIM-ATP-40, описанные ниже.

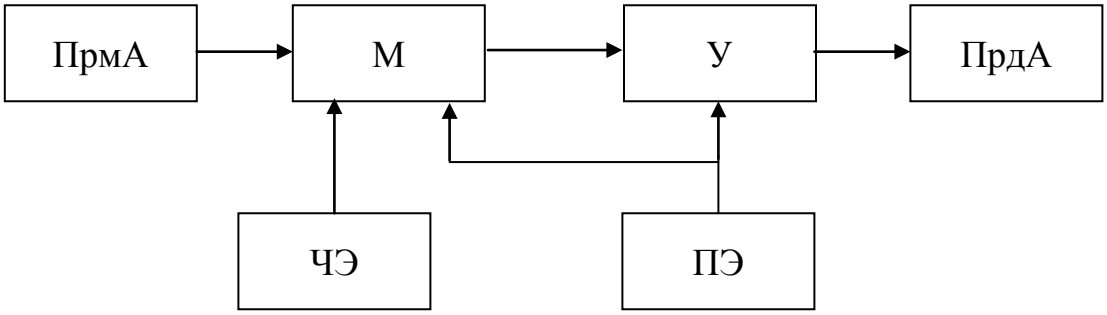

Рис. 7. Типовая структурная схема полуактивного РЗУ

SIM-ATP-16 – аудиотранспондер, имеющий размеры 90×90×4 мм, выглядит подобно дискете 3,5". Его легко можно спрятать в интерьере комнаты. Устройство упаковано в фольгу и может храниться более двух лет. Для приведения в рабочее состояние фольга должна быть снята и на расстоянии не более 10 м (в соседней комнате или автомобиле) должен быть установлен генератор синусоидального сигнала мощностью 10 Вт с частотой излучения 160 МГц. Время работы: 2000-4000 ч.

Схемой РЗУ предусмотрено, что переизлученный сигнал сдвинут относительно зондирующего на +12 кГц. Это обеспечивает развязку приемного и передающего каналов и маскировку полезного маломощного сигнала сильным зондирующим. Информационный сигнал может быть принят специальным приемником на удалении до 500 м. Для приема и переизлучения сигналов используется плоская кольцевая антенна.

Однако мощный зондирующий сигнал является демаскирующим признаком применения полуактивного ЗУ, что для руководителя службы безопасности должно послужить толчком к проведению соответствующих мероприятий по защите информации.

SIM-ATP-40 – отличается от SIM-ATP-16 тем, что имеет габариты 130×75×250 мм и работает в диапазоне 800-950 МГц. Необходимая мощность облучающего сигнала лежит в пределах от 0,1 до 20 мВт. Дальность активации системы передатчиком – 10 м. Время работы транспондера от внутренней батареи напряжением 3 В – до 4 месяцев. Для облучения и приема переизлученного сигнала используются направленные директорные антенны. Потери на переизлучение составляют около 8 дБ.

Пассивные РЗУ

Принцип действия *пассивных* РЗУ был разработан еще в середине 40-х годов. Одна из таких радиозакладок в течение многих лет проработала в посольстве США в Москве, спрятанная в гипсовый герб Соединенных Штатов, установленный над рабочим столом в кабинете посла. Выявлена она была

с большим трудом и только после того, как ЦРУ стало точно известно, что утечка информации происходит именно из этого кабинета.

Однако пассивные РЗУ в настоящее время не нашли достаточно широкого применения. Это связано с необходимостью использования столь высоких уровней излучаемой мощности передатчиков, что обслуживающий персонал вынужден работать с применением защитных средств (например, свинцовых фартуков). В этом плане полуактивные РЗУ обладают существенным преимуществом.

Примером серийно выпускаемой пассивной закладки может служить пассивная радиозакладка **SIPE MM1**, выполненная в виде стержня длиной около 30 см и диаметром 2,5 см. Дальность действия - до 100 м. Поставляется в комплекте, состоящем из закладки, источника облучения с питанием от электросети и приемного устройства.

Принцип применения пассивных и полуактивных радиозакладок иллюстрируется на рис. 8, где номерами обозначены: 1 - передатчик (ПРД), 2 - приемник (ПРМ), настроенные на частоту работы закладного устройства; 3 – полуактивная, либо пассивная радиозакладка; 4 - источник акустического сигнала.

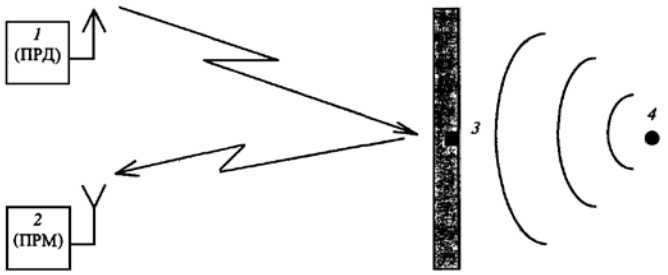

Рис. 8. Схема применения полуактивной (или пассивной) радиозакладок

Способы закрытия информации

По *способу закрытия информации,* передаваемой в радиоканале, РЗУ делятся на три вида:

- без закрытия информации;
- с использованием сложных видов модуляции;
- с кодированием информации.

Наиболее простым видом ЗУ являются радиозакладки *без закрытия информации*. Однако их применение ограничено возможностью перехвата информации любым лицом, имеющим приемник, работающий на частоте РЗУ.

К радиозакладкам *с использованием сложных видов модуляции* относятся устройства с двойной модуляцией сигнала – на поднесущей и основной частоте излучения, например, РК1970-SS (см. табл. 2). Частота поднесущей выбирается много больше 20 кГц. Поэтому прием информации возможен только на специальный приемник с двойным детектированием, что существенно повышает ее скрытность. Попытка прослушивания сигнала обычным приемником ни к чему не приведет, так как выходной сигнал будет превышать верхний частотный уровень чувствительности человеческого уха.

К более эффективным способам закрытия информации относится использование сложных шумоподобных сигналов и различных способов *кодирования информации*.

Так, например, шумоподобные сигналы с фазовой манипуляцией используются в радиозакладках **РК1970** и **SIM-PR-9000T**, а аналоговое скремблирование (наиболее часто применяемый способ шифрования) – в радиозакладках **РК2010S** (простая инверсия спектра), а в устройствах «**Брусок-ЛЗБ ДУ**», **РК1380-SS** или **РК540-SS** (сложная инверсия спектра).

Более сложный способ шифрования речевой информации – кодирование ее в цифровом виде. Такой способ закрытия применен, например, в радиозакладках **РК1195-SS**, **РК2050**, **SIM-PR-9000T** и **РК1970** (см. табл. 2).

Мощность передатчика

В зависимости от мощности передатчика РЗУ делятся на три вида – малой, средней и большой дальности действия.

Радиозакладные устройства *малой дальности* способны передавать информацию на расстояние, не превышающее несколько десятков метров, поэтому без ретранслятора (приемно-передающего блока) они, как правило, не используются. РЗУ *средней дальности* позволяют вести уверенный прием информации на удалении несколько сот метров, а радиозакладки *большой дальности* способны работать с радиоприемными устройствами, расположенными на удалении 1000 м и более.

В качестве иллюстрации можно привести характеристики некоторых типов серийно выпускаемых закладных устройств:

РК580-S – передатчик с кварцевой стабилизацией частоты, закамуфлированный под поясной ремень. Вес – 250 г. Мощность излучения – 50 мВт, рабочая частота – 139 МГц, дальность передачи радиосигнала – 700 м. Источник питания – батарея с напряжением 6 В. Рекомендуемые приемники для работы с данным радиомикрофоном: **РК830-SS**, **РК1015-SS.**

РК525-S – передатчик с кварцевой стабилизацией частоты, закамуфлированный в головном уборе. Вес – 150 г. Рабочая частота –139 МГц. Источник питания – батарея с напряжением 6 В.

РК585-S – передатчик с кварцевой стабилизацией частоты, закамуфлированный под авторучку диаметром 11 мм и длиной 135 мм. Вес – 30 г. Рабочая частота – 139 МГц. Дальность перехвата акустических сигналов – 5 м, дальность передачи радиосигналов – 300 м. Источник питания – 2 батареи с напряжением по 1,5 В. Рекомендуемые приемники для работы с данным радиомикрофоном: **РК830-SS**, **РК825-S, РК1015-SS.**

РК575-S – передатчик с кварцевой стабилизацией частоты, закамуфлированный под зажигалку диаметром 55 мм и длиной 73 мм. Вес – 95 г. Источник питания – батарея с напряжением 6 В. Рекомендуемые приемники для работы с данным радиомикрофоном: **РК830-SS**, **РК815-S, РК1015-SS.**

РК560-S – передатчик, закамуфлированный под электролампочку. Дальность перехвата акустических сигналов – 20 м, дальность передачи радиосигналов – 300 м. Питается от электросети переменного тока с напряжением 110/220 В. Не может быть использован в качестве источника света. Рекомендуемые приемники для работы с данным радиомикрофоном: **РК830-SS**, **РК825-S, РК1015-SS.**

РК570-S – передатчик, закамуфлированный под пепельницу. Габариты передатчика 125×12×30 мм, вес – 275 г. Дальность передачи радиосигналов – до 250 м. Источник питания – батарея с напряжением 9 В, время непрерывной работы – 50 часов. Дистанционное управление режимом излучения.

РК1025-S – передатчик, закамуфлированный под наручные часы. Представляет из себя диск диаметром 25 мм и толщиной 4 мм, вес 40 г. Питается от одного элемента 1,5 В, которого хватает на 6 часов непрерывной работы. Частоты излучений лежат в диапазонах 88-108; 130-150 МГц. Рекомендуемый приемник для работы с данным радиомикрофоном: **РК1015-SS.**

STG 4005 – радиомикрофон с «акустоматом», работает в диапазоне частот 130...150 МГц, вид модуляции – широкополосная частотная, выходная мощность – 6 мВт. Габариты – 45×30×15 мм, вес – 35 г, напряжение питания – 6 В, тип антенны – гибкая.

STG 4007 – радиомикрофон с «акустоматом», работает в диапазоне частот 395...415 МГц, вид модуляции – узкополосная частотная, выходная мощность – 15 мВт. Габариты – 66×27×14 мм, вес – 52 г, напряжение питания – 6 В, тип антенны – гибкая.

GTG 4215 – радиомикрофон с дистанционным управлением, работает в диапазоне частот 115-150 МГц, вид модуляции – широкополосная частотная, выходная мощность – 5 мВт. Габариты – 67×36×25 мм, вес – 70 г, напряжение питания – 110/220 В электросети переменного тока, антенна – провод электросети. Устройство дистанционного управления работает в диапазоне частот: 800-.1000 Гц. Выходная мощность – 50 мВт, команда – кодированная. Габариты –155×60×20 мм, вес – 70 г.

UXMC – радиомикрофон, закамуфлированный в виде портативного компьютера с сетевым или батарейным электропитанием. Может использоваться и как обычный компьютер, и как радиомикрофон для передачи перехватываемых речевых сигналов из контролируемого помещения на расстояние до 3000 м. Диапазон рабочих частот – 398-430 МГц с выделением шести фиксированных частот. Устройство поставляется в комплекте с миниатюрным приемником, оборудованным шумоподавителем и имеющим возможность подключения диктофона с длительностью записи 1,3 или 6 часов.

UX CARD – радиомикрофон, закамуфлированный в виде кредитной карточки. Работает в диапазоне частот 398-430 МГц. Имеет размеры кредитной карточки толщиной 4 мм. Он может быть скрыт между страницами книги, вставлен в один из настольных канцелярских приборов, размещен в кармане одежды или сумке. Время непрерывной работы прибора – 30 часов, дальность передачи – 200-300 м. Электропитание от встроенной литиевой батареи с напряжением 3 В.

UXP – радиомикрофон, закамуфлированный в корпус шариковой ручки типа Parker. При этом остается место для миниатюрного пишущего стержня. Дальность действия до 300 м. Ручку с встроенным устройством можно держать в кармане или пользоваться ею открыто, не вызывая подозрений у окружающих. Электропитание от двух элементов с напряжением 1,5 В, размещенных в корпусе авторучки.

UXC – радиомикрофон, закамуфлированный в виде карманного калькулятора. Работает в диапазоне частот 398...430 МГц, дальность передачи информации 300 – 1000 м. Устройство наделено всеми функциями обычного калькулятора, поэтому может быть размещено в непосредственной близости от прослушиваемого источника речевой информации.

Внешний вид некоторых радиозакладных устройств в обычном исполнении показан на рис. 9.

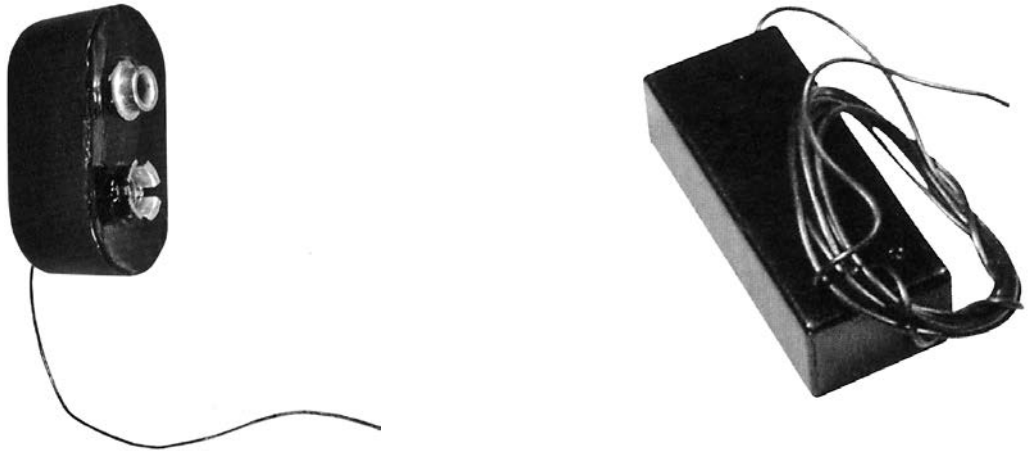

Рис. 9. Радиомикрофоны в обычном исполнении

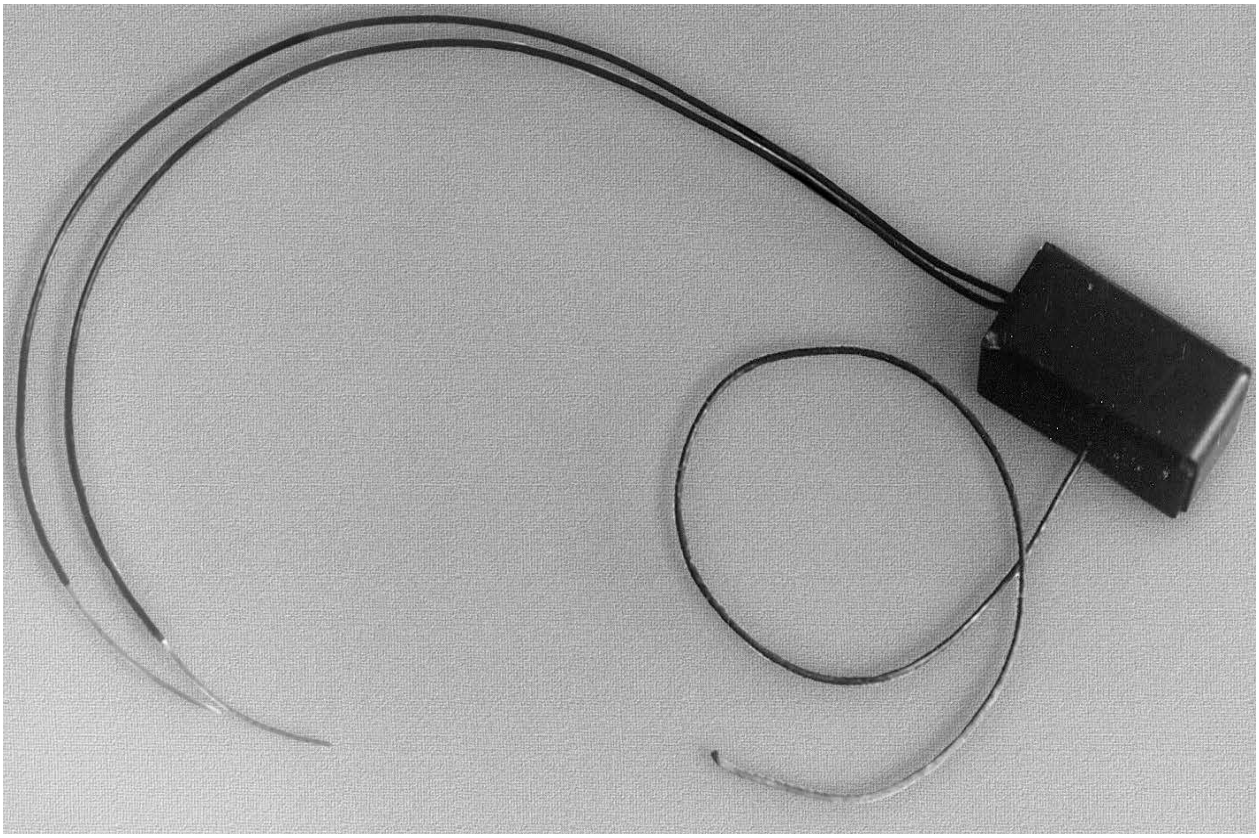

Рис. 10. Радиозакладное устройство в обычном исполнении, предназначенное для подключения к телефонным линиям связи

Внешний вид некоторых радиомикрофонов, в закамуфлированном под бытовые предметы виде, показан на рис. 11-18.

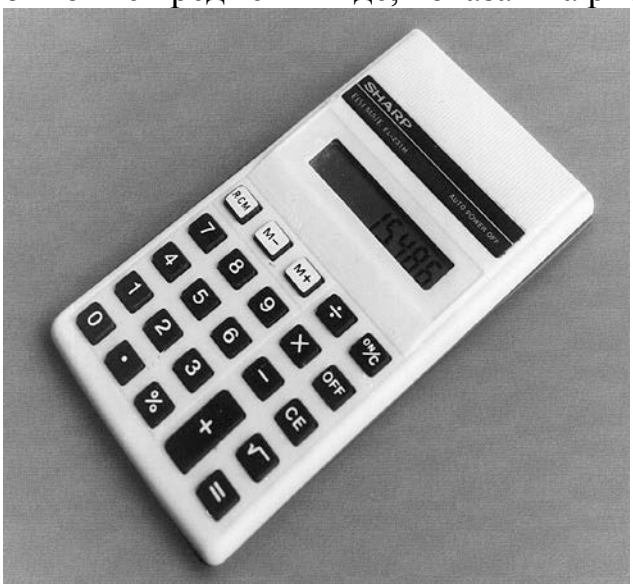

Рис. 11. Калькулятор

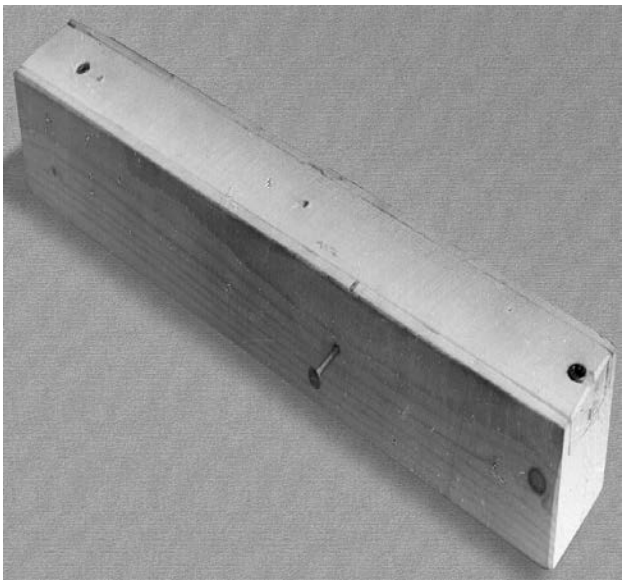

Рис. 12. Деревянный брусок

Рис. 13. Кожаный ремень

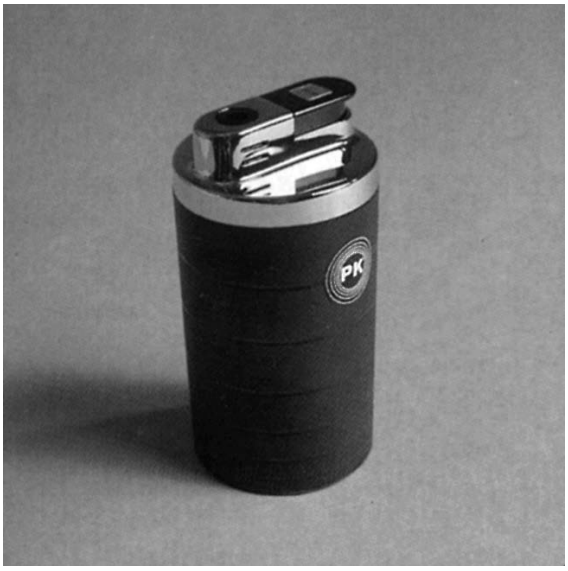

Рис. 14. Зажигалка

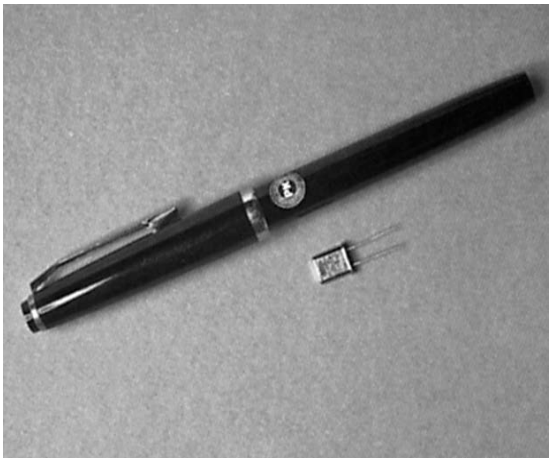

Рис. 15. Шариковая ручка типа Parker

Рис. 16. Пепельница

Рис. 17. Электрические лампочки

Рис. 18. Обруч

Схемы применения радиозакладных устройств

Схемы применения радиозакладных устройств с использованием ретрансляторов сигналов от закладных устройств к пунктам приёма и сбора информации приведены на рис. 19 и 20.

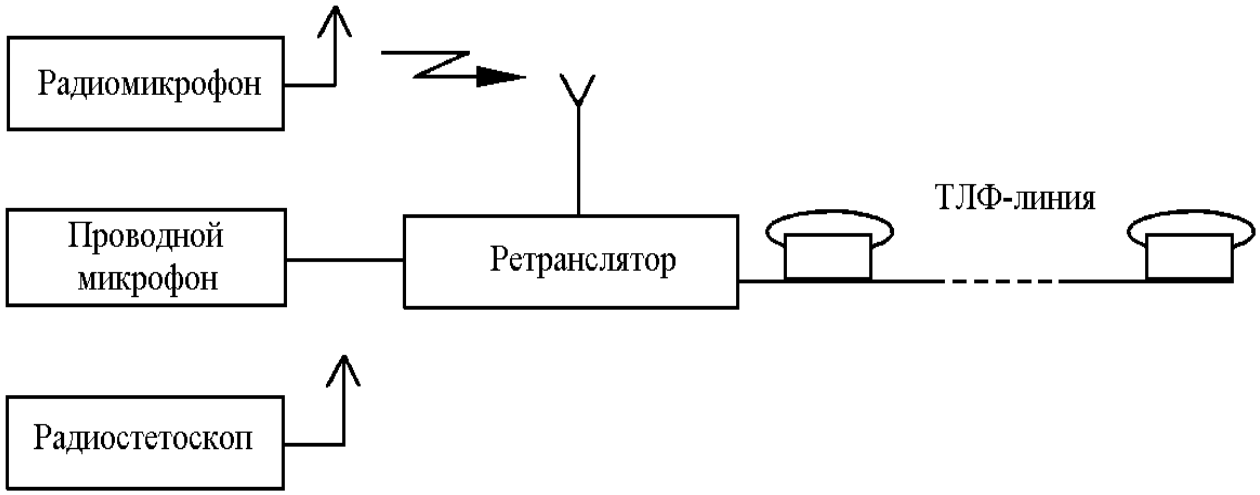

Рис. 19. Ретрансляция сигналов в телефонную линию

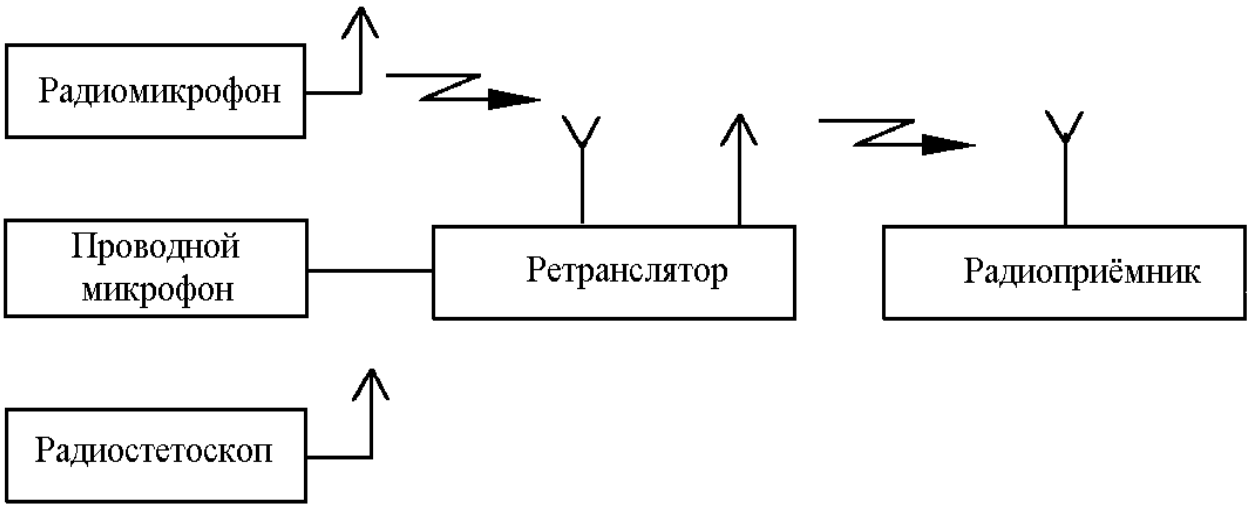

Рис. 20. Ретрансляция сигналов в УКВ радиоканал

На один приёмник можно принимать сигнал от нескольких радиозакладных устройств, в том числе и закамуфлированных либо под личные вещи либо под элементы электроцепей. Схемы применения закамуфлированных радиозакладных устройств приведены на рис. 21 и 22.

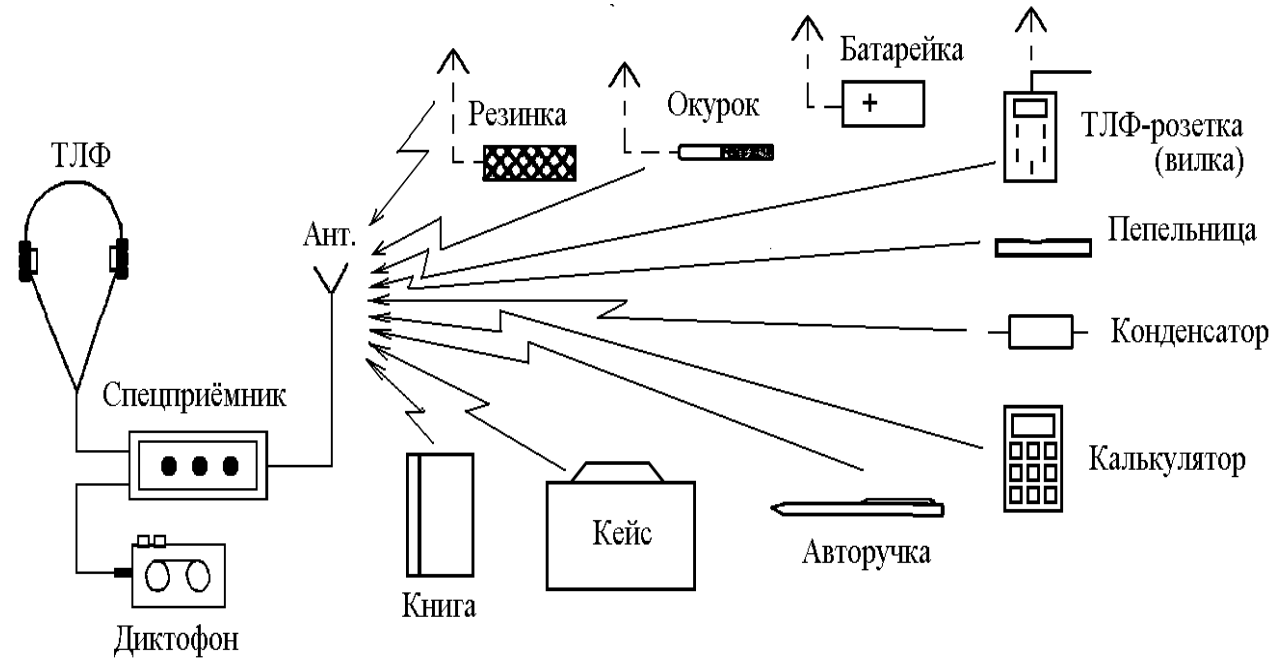

Рис. 21. Приём сигналов от радиозакладок, закамуфлированных под личные вещи сотрудников и некоторые предметы

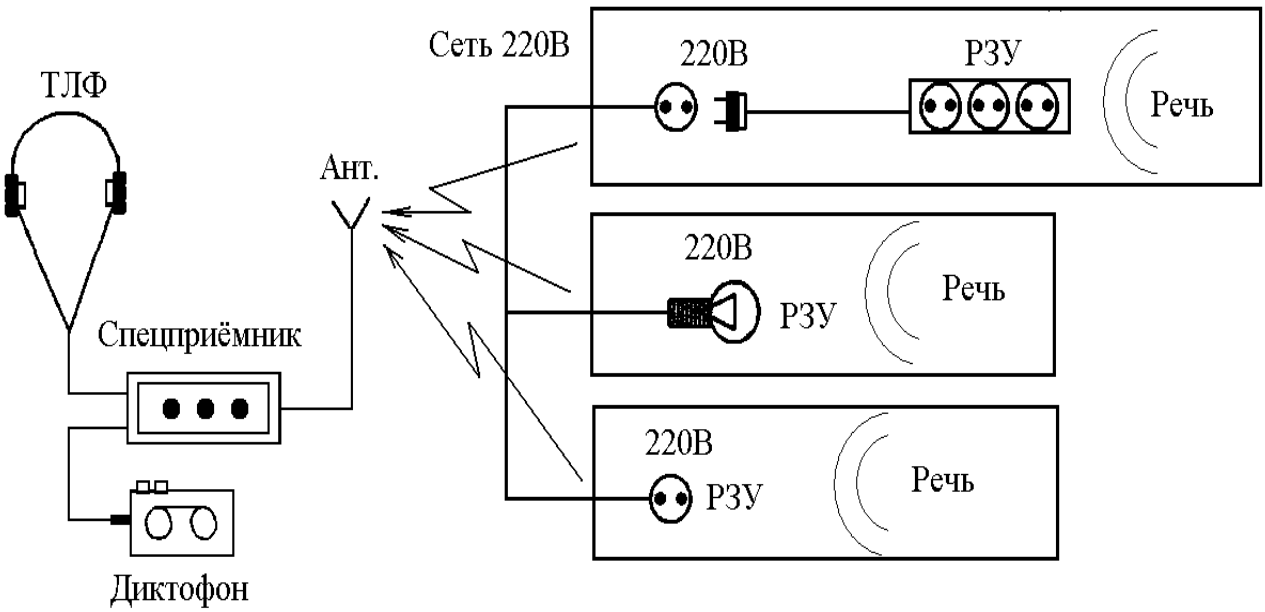

Рис. 22. Приём сигналов в контролируемых помещений, от нескольких радиозакладок которые закамуфлированы под элементы электросети 220В

Для того чтобы дать представление о принципах построения РЗУ, приведём ниже два простейших варианта принципиальных схем построения радиозакладных устройств (радиомикрофонов).

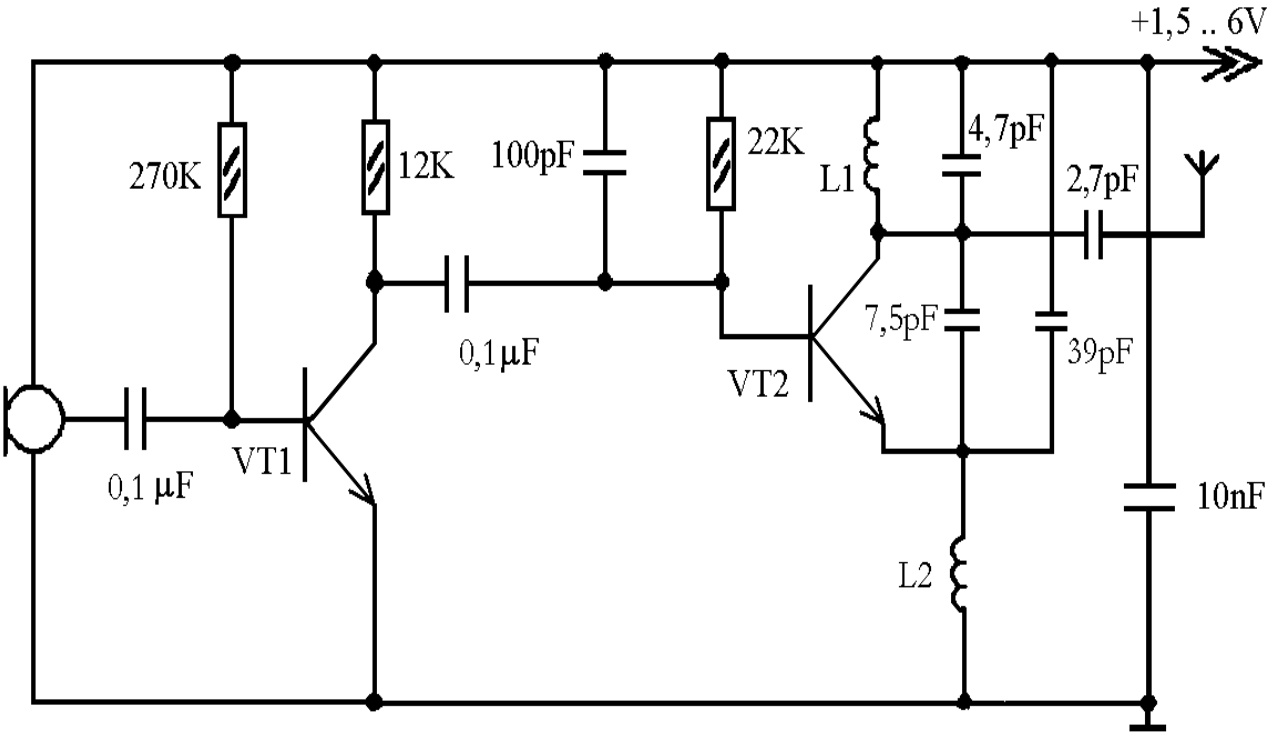

Рис. 24. Принципиальная схема простейшего радиопередающего устройства (радиомикрофона)

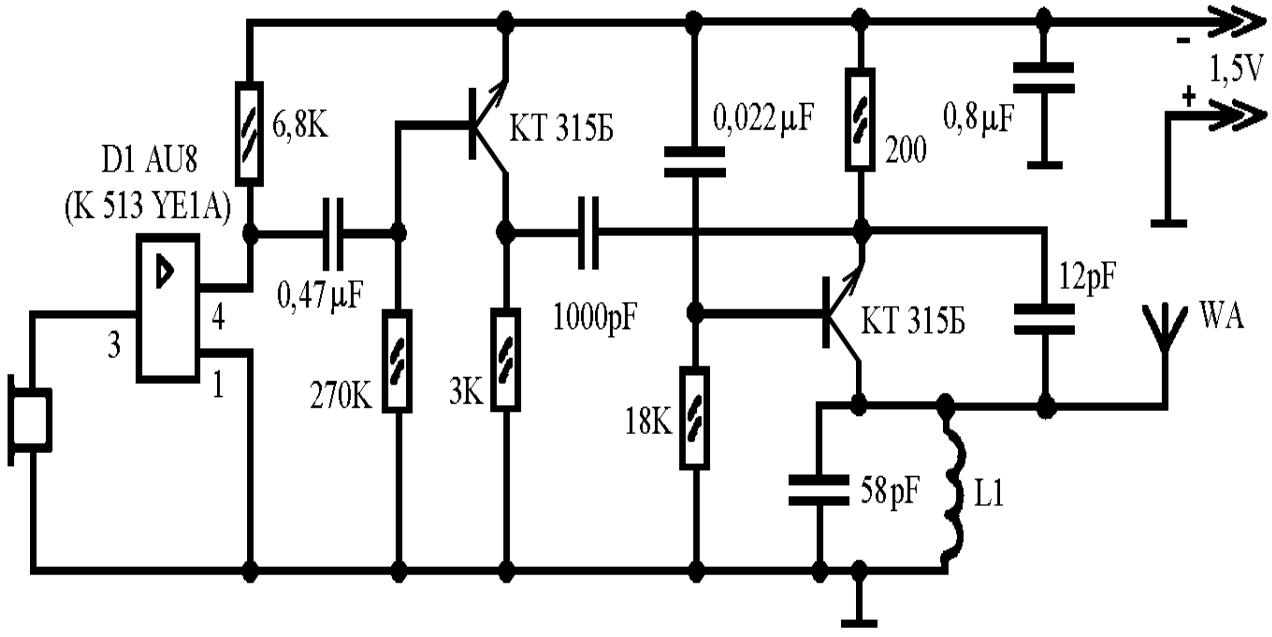

Рис. 25. Радиомикрофон, принципиальная схема (вариант 2)

1.3. Приемники излучения радиозакладных устройств

Для приема информации, передаваемой с радиозакладок, могут быть использованы различные виды радиоприемных устройств. Наиболее часто для этих целей используют:

- портативные сканерные приемники;
- специальные приемные устройства;
- приемники портативных радиостанций;
- бытовые радиоприемники.

Портативные сканерные приемники

Современные переносные малогабаритные (портативные) *сканерные* приемники имеют автономные аккумуляторные источники питания, свободно умещаются во внутреннем кармане пиджака, а их вес составляет 150-350 г.

Несмотря на малые габариты и вес такие приемники позволяют осуществлять прием сигналов в диапазоне 100 кГц -1300 МГц, а некоторые типы приемников – до 1900 МГц и даже до 2060 МГц («**HSC-050**»). Они обеспечивают прием сигналов с амплитудной, узкополосной и широкополосной частотной модуляцией, а их чувствительность лежит в пределах от 0,35 до 6 мкВ. Полоса пропускания в режиме приема узкополосных сигналов – 12.-15 кГц, а широкополосных (текстовых) – 150-180 кГц.

Портативные сканерные приемники имеют от 100 до 1000 каналов памяти и обеспечивают скорость сканирования до 30 каналов в секунду. Некоторые типы приемников, например **AP-2700** и **AR-8000**, могут управляться компьютером.

Специальные приемные устройства

Для приема информации от радиозакладок используют и *специальные приемные устройства*. Они выпускаются как в обычном, так и камуфлированном виде под предметы повседневного обихода или бытовые приемники. Некоторые специальные приемники оборудованы встроенными магнитофонами (например, **РК820-S**). В ряде случаев применяются специальные комплексы, как, например, **РК1015-SS**, способные одновременно принимать информацию по нескольким каналам и осуществлять ее запись на магнитофон или обеспечивать прослушивание на внутренние динамики. Чувствительность специальных приемных устройств не уступает чувствительности сканерных приемников и составляет величину менее 0,5 мкВ.

Иногда для приема сигналов с радиозакладок используют специальные сверхминиатюрные приемники. Например, такой приемник, работающий в УКВ-диапазоне, имеет вес около 1,5 г (с батарейкой) и размеры 17,5×11,5 мм,

позволяющие полностью установить его в слуховой проход. Для затруднения обнаружения приемника его окрашивают в телесный или темный цвет. Приемное устройство имеет кварцевую стабилизацию и может быть настроено на любую частоту в диапазоне 138...190 МГц. Чувствительность такого приемника не хуже 2 мкВ, а время непрерывной работы – 15-30 часов.

Примером специальных приемников для перехвата излучений радиозакладок, могут служить следующие устройства:

PK1015-SS – приемник, размещенный в атташе-кейсе. Габариты – 460×330×120 мм, вес – 5 кг. Источник питания – 8 элементов по 1,5 В. Диапазон рабочих частот – 130-150 МГц. Значение рабочей частоты выводится на жидкокристаллический дисплей. Имеет 3 канала кварцованных частот: А – 139,6 МГц, В – 139,8 МГц, С – 140,0 МГц. Чувствительность приемника не хуже 0,25 мкВ при отношении сигнал/шум на выходе РПУ 12 дБ. Время непрерывной работы – 2 часа. Предусмотрена автоматическая запись принимаемых сигналов на диктофон.

PK830-SS – приемник с габаритами, позволяющими размещать его в стандартной пачке сигарет: 85×54×20 мм, вес – 275 г. Источник питания – элемент с напряжением 9 В. Диапазон рабочих частот – 120...150 МГц. Имеет 3 канала кварцованных частот: А – 139,6 МГц, В – 139,8 МГц, С – 140,0 МГц. Чувствительность приемника не хуже 0,25 мкВ при отношении сигнал/шум на выходе РПУ 12 дБ.

UXR1 – двухканальный радиоприемник, работающий в диапазоне частот 398...430 МГц. Может одновременно принимать передачи от двух радиомикрофонов с попеременным переключением каналов. Габариты – 48×66×19 мм, электропитание – литиевая батарея напряжением 6 В, время непрерывной работы – 36–48 часов. Дальность приема сигналов – 150–1000 м.

UXR3 – высокочувствительный двухканальный радиоприемник диапазона частот 398...430 МГц, объединенный с аудиомагнитофоном. Предназначен для установки в транспортные средства. Электропитание – 12 В, дальность приема – до 2000 м.

UXR5 – четырехканальный радиоприемник – аудиомагнитофон, размещенный в портфеле типа «дипломат». Рабочий диапазон – УВЧ. Оснащен автоматическим управлением и миниатюрным компьютером для опознавания голосов, перехватываемых радиомикрофонами в контролируемых помещениях. В блок входит аудиомагнитофон с автоматическим реверсом, рассчитанный на непрерывную запись в течение 2 часов.

Внешний вид некоторых приемных устройств приведен на рис. 26 –30.

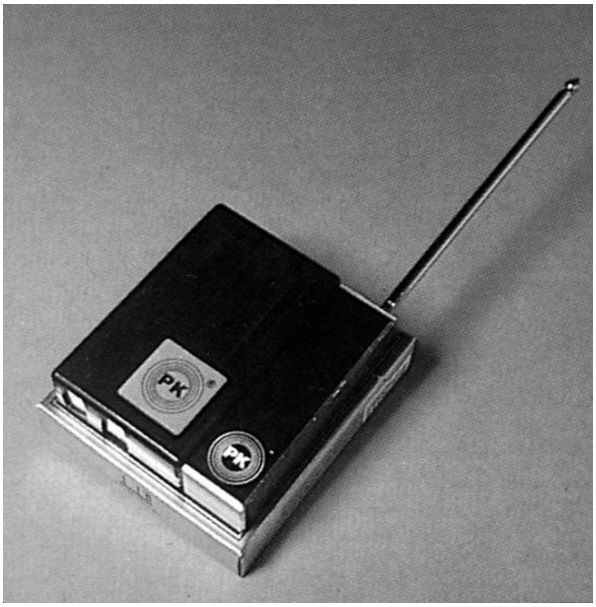

Рис. 26. Специальный приёмник (РК 25-SS)

Рис. 27. Сто канальный комплекс, размещённый в атташе кейсе

Рис. 28. Панорамный радиоприёмник (AR 8000)

Рис. 29. Стандартная магнитола Panasonic со встроенным конвертором

Приемники портативных радиостанций

Для приема излучений радиозакладок, работающих в диапазоне 134-174 МГц, 400-512 МГц могут использоваться *портативные радиостанции* (см. рис. 30). Они имеют высокую чувствительность (0,25-0,5 мкВ) и малые габариты.

Рис. 30. Портативные радиостанции

Основным достоинством применения таких приемников является возможность приема кодированных сигналов, так как современные радиостанции оборудуются встроенными скремблерами. Недостатком является то, что портативные радиостанции обеспечивают высокое качество приема сигналов только от радиозакладок, имеющих узкополосную частотную модуляцию и использующих кварцевую стабилизацию частоты.

Бытовые радиоприемники

Для приема информации, передаваемой с радиозакладок, которые работают в диапазоне 88...108 МГц, может быть использован любой бытовой радиоприемник, имеющий FM-диапазон (для отечественных приемников – диапазон УКВ-2). Единственным условием нормального приема является отсутствие (либо возможность отключения) системы автоматической подстройки частоты, в противном случае приемник будет перестраиваться от слабого сигнала радиозакладки на мощный сигнал ближайшей стационарной вещательной радиостанции.

1.4. Закладные устройства с передачей информации по проводным каналам

Техническая возможность применения токоведущих линий для передачи перехваченной акустической информации практически реализована в целом ряде ЗУ.

Передача информации от ЗУ по сети 220В

Наиболее широкое распространение получили закладки, использующие для передачи информации сеть 220 В. Как правило, подслушивающие устройства устанавливаются в стандартную розетку или любой другой постоянно подключенный к силовой сети электроприбор (тройник, удлинитель, блок питания радиотелефона, факс и т. п. устройства), расположенные в помещении, в котором ведутся переговоры интересующих лиц. Типовая схема такой закладки приведена на рис. 31.

Чувствительность внедренных микрофонов, как правило, обеспечивает надежную фиксацию голоса человека или группы лиц на удалении от ЗУ до 10 м.

Дальность передачи информации лежит в пределах от 300 до 1000 м. Она обеспечивается за счет применения выходного усилителя с мощностью 5-300 мВт и амплитудной или частотной модуляции несущей, специально сформированной в задающем генераторе закладного устройства.

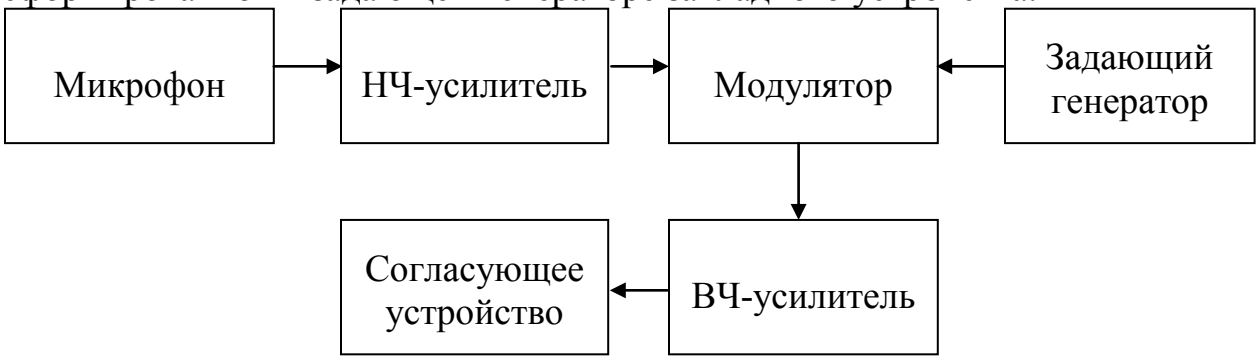

Рис. 31. Структурная схема закладного устройства

Несущая модулируется информационным сигналом, прошедшим предварительное усиление в низкочастотном (НЧ) усилителе, и через высокочастотный (ВЧ) усилитель и специальное согласующее устройство излучается в линию. Частота передаваемого сигнала лежит в диапазоне50...300 кГц. Выбор данного участка обусловлен тем, что, с одной стороны, на частотах ниже 50 кГц в сетях электропитания относительно высок уровень помех от бытовой техники, промышленного оборудования, лифтов и т. д. С другой – на частотах выше 300 кГц существенно затухание сигнала в линии, и кроме того, провода начинают работать как антенны, излучающие сигнал в окружающее пространство. Однако в некоторых случаях используются колебания с частотами, достигающими до 10 МГц. Питание ЗУ осуществляется от той же сети, 220 В.

Приемное устройство (см. рис. 32), расположенное вне пределов контролируемого помещения и подключенное к той же сети, перехватывает информационный сигнал и преобразует его в вид, удобный для прослушивания через головные телефоны, а также запись на магнитофон.

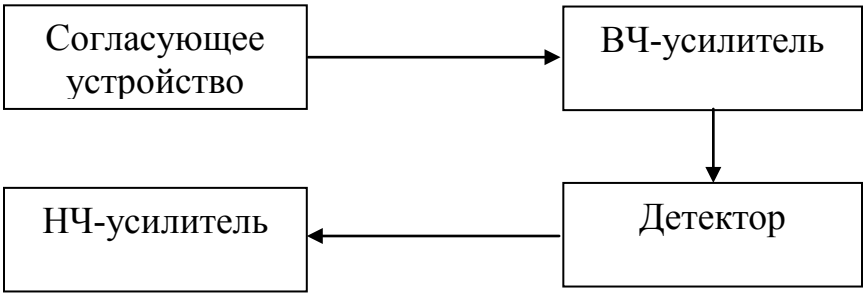

Рис. 32. Структурная схема приёмного устройства

Принимаемый сигнал поступает на ВЧ-усилитель через согласующее устройство, затем детектируется и через НЧ-усилитель подается на головные телефоны или магнитофон. *Чувствительность* такого устройства, как правило, лежит в пределах от 3 до 100 мкВ, а *питание* осуществляется от батареек (аккумуляторов).

Типовая схема организации негласного прослушивания переговоров с задействованием энергосети приведена на рис. 33.

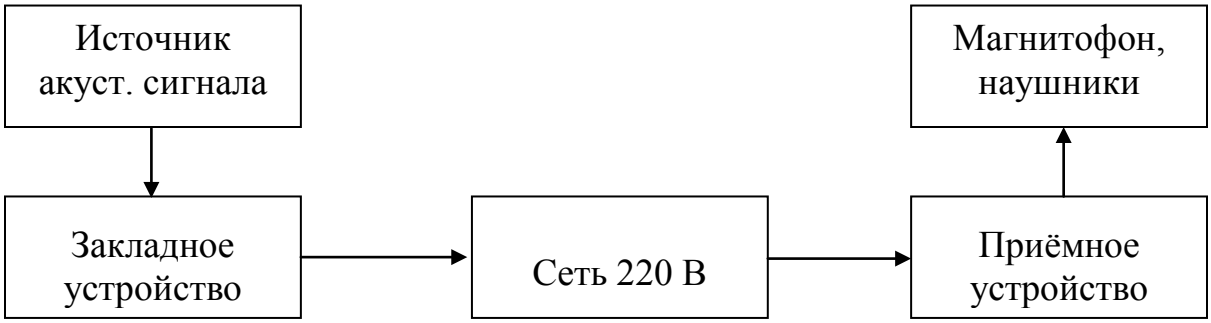

Рис. 33. Схема применения ЗУ с передачей информации по сети 220В

Многоканальные системы прослушивания

В некоторых случаях для одновременного прослушивания нескольких помещений, используются многоканальные системы (см. рис. 34).

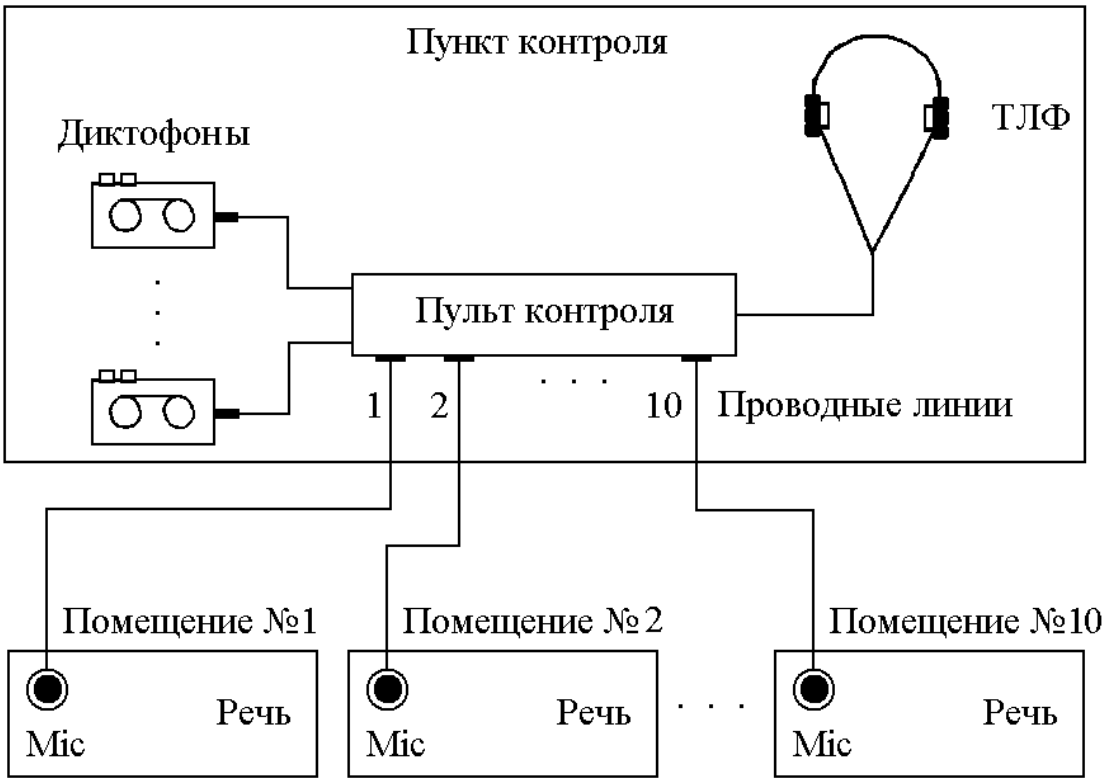

Рис. 34. Многоканальные ЗУ с передачей информации на пункт сбора и обработки по специально проложенным кабелям

Основной недостаток этой структуры состоит в том, что легко обнаружить такой пункт контроля.

Рассмотрим многоканальные ЗУ с передачей информации по сети 220 В, изображённые на рис. 35.

При этом закладные устройства (проводные микрофоны, сокращённо - Mic) работают на различных фиксированных частотах, а оператор выбирает на приемном устройстве канал, необходимый для прослушивания в каждый конкретный момент времени.

В целом устройства контроля акустической информации с передачей по сети 220 В обладают существенными преимуществами перед другими ЗУ. Во-первых, в этом случае практически невозможно точно выявить место установки приемного оборудования. Во-вторых, по сравнению с радиозакладками – повышенной скрытностью (поскольку невозможно ее обнаружение с помощью радиоприемных устройств). В-третьих, практически неограниченным временем непрерывной работы, так как не требуют периодической заме-

ны источников питания. По сравнению с обычными проводными микрофонами (см. рис. 34), использующими собственные проводники для передачи сигнала.

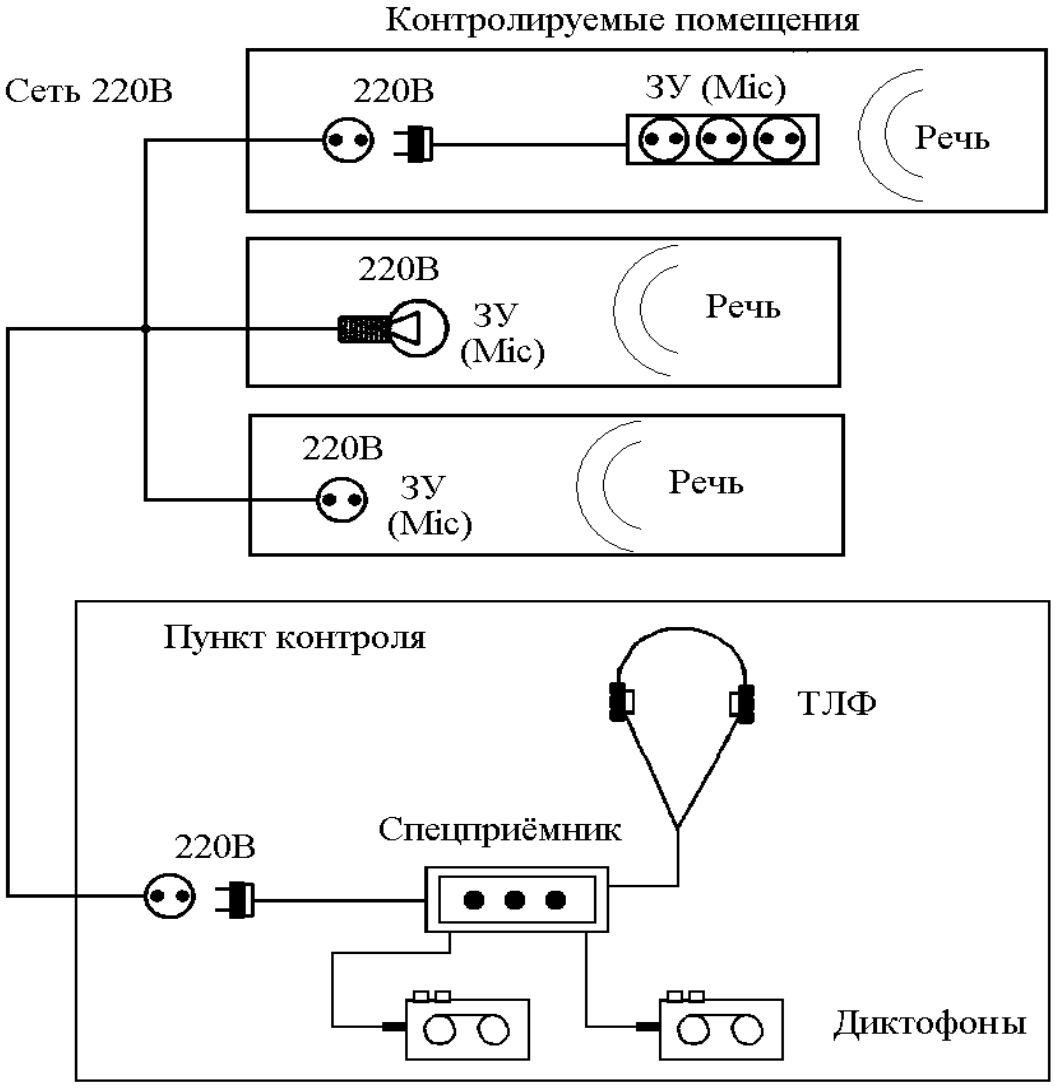

Рис. 35. Многоканальные ЗУ с передачей информации по сети 220 В

На первый взгляд, кажется, что второй вариант (см. рис. 35) лучше. Однако при использовании данной техники возникают следующие существенные проблемы.

Во-первых, работа возможна только в пределах одной фазы электропроводной сети.

Во-вторых, на качество перехватываемой информации влияют различные сетевые помехи.

В-третьих, прибор, в который внедрено ЗУ, может быть отключен от сети переменного тока.

Поэтому применение данной техники обычно сопровождается тщательным изучением схемы организации электроснабжения, наличия и типов потребителей электроэнергии, выбором камуфляжа.

Аналогично системам с передачей информации по сети 220 В функционирует и аппаратура акустического контроля с передачей информации по телефонной сети. В состав изделий входят те же блоки, используется тот же частотный диапазон. Отличительной особенностью является блок питания, предназначенный для преобразования напряжения телефонной линии к требуемому уровню. В связи с тем, что от телефонной линии нельзя потреблять более 2 мА, мощность передающих устройств не может превышать 10-15 мВт.

Однако существуют определенные ограничения на применение подобных устройств.

Во-первых, необходимо подключать приемную аппаратуру именно к той телефонной линии, на которой установлено устройство съема информации, что упрощает обнаружение пункта контроля (по сравнению с передачей по сети 220 В).

Во-вторых, устройство достаточно габаритное и его относительно трудно использовать скрытно, так как все возможные места установки (телефонный аппарат, розетки, распределительное оборудование и т. д.) легко проверить, в отличие от системы электропроводки.

Вышеперечисленные недостатки привели к тому, что данные устройства практически не используются.

Подобно телефонным, для установки закладок могут быть использованы и другие сети слаботочного оборудования (пожарной и охранной сигнализации, радиотрансляции и т. д.). Их недостатки аналогичны приведенным выше, в связи с этим и реальное применение крайне редко.

Примерами серийно выпускаемых закладок с передачей информации по токоведущим линиям могут служить следующие устройства:

UM104 – сетевая закладка, предназначенная для прослушивания служебных и жилых помещений путем передачи и приема акустической информации по сети переменного тока. Дальность передачи (по проводам) – не менее 30 м; словесная разборчивость (при отсутствии помех) – 90 %; электропитание закладки – сеть 220 В; питание приемника – 4 батареи «АА».

Закладка устанавливается вместо стандартной стенной розетки или встраивается в электробытовые приборы. При установке в нишу стенной розетки UM104 полностью выполняет все ее функции и допускает подключение электроприборов мощностью 1,5 кВт (см. рис. 36).

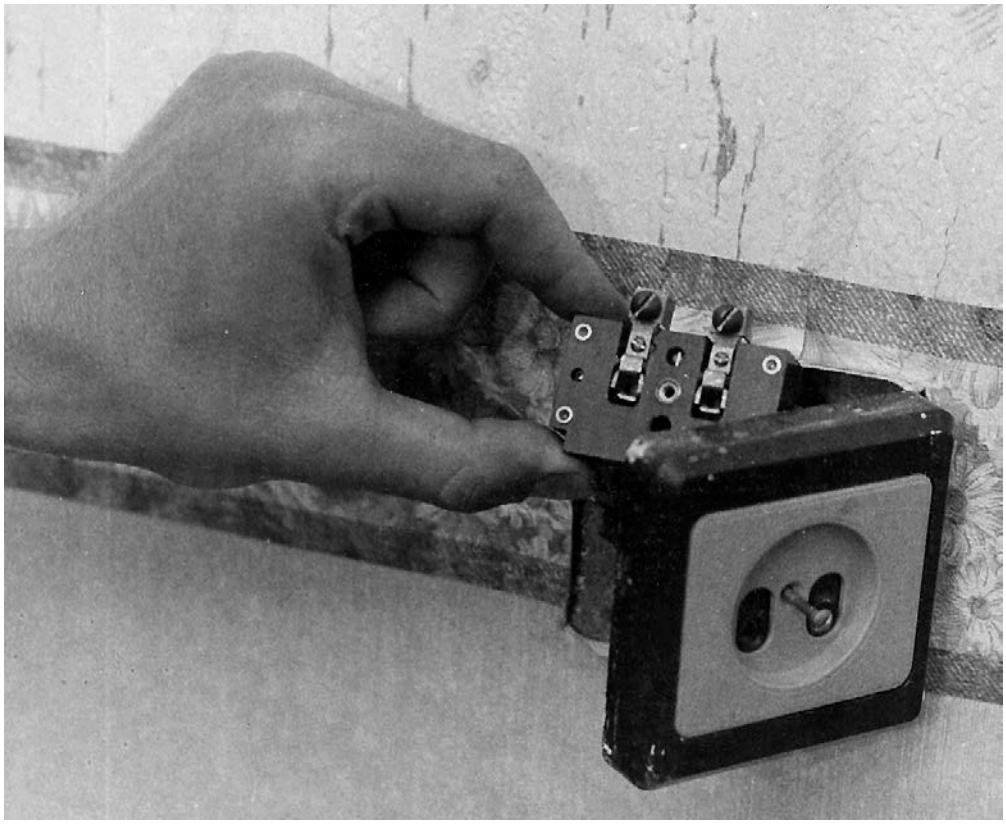

Рис. 36. Микрофон, закамуфлированный под электрическую розетку

Отличительной способностью спецприемника является подключение к силовой сети только одним проводом, что обеспечивает повышенную безопасность и удобство в эксплуатации. Выбор провода для подключения определяется небольшим экспериментом и по лучшему качеству прослушивания. Контроль переговоров разрабатываемых лиц ведется на головные телефоны.

IPS MCX – акустическая закладка с передачей информации по сети переменного тока. Скрытно устанавливается в одном из бытовых приборов (см. рис. 37). Диапазон используемых для передачи частот – до 120 кГц; рабочее напряжение 100-260 В переменного тока с частотой 50/60 Гц; диапазон передаваемого акустического сигнала – 300-3500 Гц; модуляция – узкополосная частотная; габариты – 33×67×21 мм.

Передаваемая информация принимается приемником, рассчитанным на обслуживание шести передатчиков. Он оборудован встроенным громкоговорителем и выходами на диктофон и головные телефоны. Для записи на магнитофон имеется линейный выход.

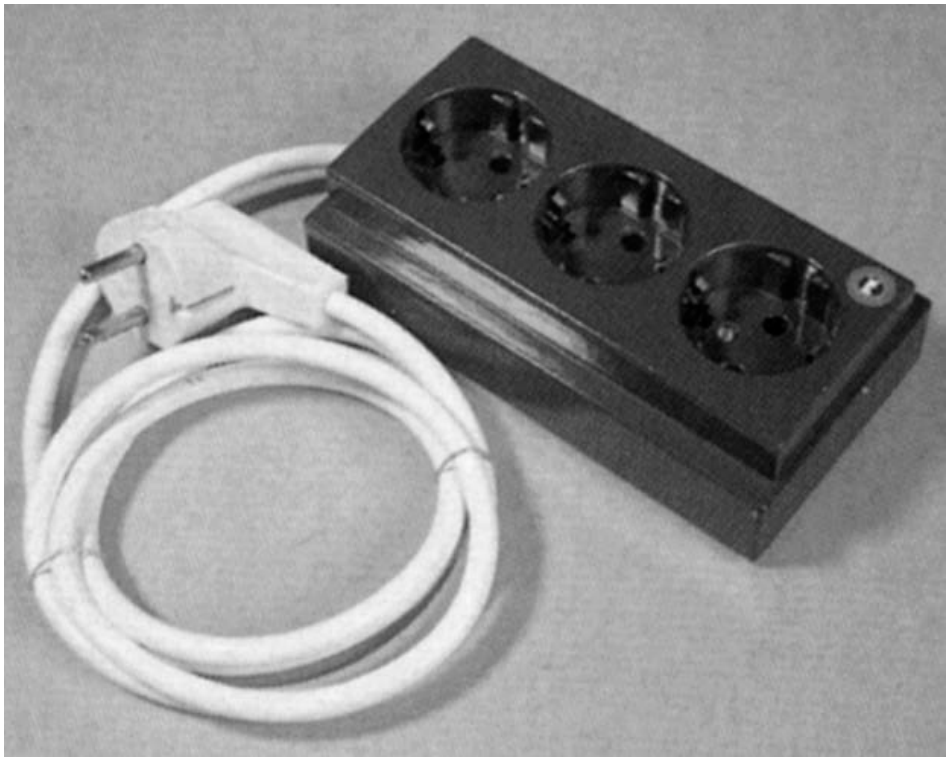

Рис. 37. Микрофон закамуфлированный под электрический тройник

РК170 – телефонная закладка с рабочей частотой около 100 кГц, вес – 180 г, габариты – 130×30×20 мм. Используется частная модуляция. В комплекте поставляется приемник (вес 750 г). Закладку производитель рекомендует устанавливать либо непосредственно в телефонном аппарате, либо в телефонной розетке.

2. НАПРАВЛЕННЫЕ МИКРОФОНЫ

В наиболее общем виде любой направленный микрофон можно представить как некоторый комплекс, состоящий из чувствительного элемента (собственно *микрофона*), осуществляющего акустико-электрическое преобразование, и механической системы (*акустической антенны*), обеспечивающей направленные свойства комплекса.

2.1. Микрофон

Микрофон (происходит от *греч*. micros – малый, и phone – звук) представляет собой электроакустический прибор для преобразования звуковых колебаний в электрические. В зависимости от принципа действия микрофоны делят на следующие типы: порошковые угольные; электродинамические; электростатические (конденсаторные и электретные); полупроводниковые; пьезоэлектрические; электромагнитные.

Порошковый угольный микрофон впервые был сконструирован русским изобретателем Махальским в 1878 году и позже, независимо от него, Голубицким в 1883-м. Принцип действия такого микрофона основан на том, что угольная или металлическая мембрана под действием звуковых волн колеблется, изменяя плотность и, следовательно, электрическое сопротивление угольного порошка, находящегося в капсюле и прилегающего к мембране. Вследствие неравномерного механического давления сила тока, протекающего через микрофон, изменяется в акустический сигнал. Однако в интересах съема информации микрофоны данного типа практически не используются из-за их низкой чувствительности и большой неравномерности амплитудно-частотной характеристики.

Электродинамический микрофон катушечного типа изобрели американские ученые Венте и Терас в 1931 году. В нем применена диафрагма из полистирольной пленки или алюминиевой фольги. Катушка, сделанная из тонкой проволоки, жестко связана с диафрагмой и постоянно находится в кольцевом зазоре магнитной системы. При колебаниях диафрагмы под действием звуковой волны витки катушки пересекают магнитные силовые линии и в обмотке наводится электродвижущая сила (ЭДС), создающая переменное напряжение на выходе микрофона. Вместо катушки может использоваться ленточка из очень тонкой (около 2 мкм) металлической фольги.

В *конденсаторном микрофоне,* изобретенном американским ученым Э. Венте в 1917 году, звуковые волны действуют на тонкую металлическую мембрану, изменяя расстояние и, следовательно, электрическую емкость между мембраной и металлическим неподвижным корпусом, которые представляют собой пластины электрического конденсатора. При подведении к пластинам постоянного напряжения изменение емкости вызывает появление тока

через конденсатор, сила которого изменяется в такт с колебаниями звуковых частот.

Электретный микрофон, изобретенный японским ученым Егути в начале 20-х годов XX века, по принципу действия и конструкции схож с конденсаторным. Только роль неподвижной обкладки конденсатора и источника постоянного напряжения в нем играет пластина из электрета. Недостатком такого микрофона является высокое выходное сопротивление, которое приводит к большим потерям сигнала, поэтому в корпус элемента, как правило, встраивают истоковый повторитель, что позволяет снизить выходное сопротивление до величины не более 3-4 кОм.

В *пьезоэлектрическом микрофоне,* впервые сконструированном советскими учеными Ржевкиным и Яковлевым в 1925 году, звуковые волны воздействуют на пластинку из вещества, обладающего пьезоэлектрическими свойствами (например, из сегнетовой соли), вызывая на ее поверхности появление электрических зарядов.

В *электромагнитном микрофоне* звуковые волны воздействуют на мембрану, жестко связанную со стальным якорем, находящимся в зазоре постоянного магнита. На небольшом расстоянии вокруг якоря намотана обмотка неподвижной катушки. В результате воздействия акустических волн на такую систему на выводах обмотки появляется ЭДС. Данные изделия так же, как и порошковые угольные микрофоны, не получили широкого распространения из-за большой неравномерности амплитудно-частотной характеристики.

Обобщенные характеристики перечисленных выше типов микрофонов приведены в табл. 3.

Чаще всего в направленных микрофонах применяются чувствительные элементы (микрофоны) электретного типа, так как они имеют наилучшие электроакустические характеристики: широкий частотный диапазон; малую неравномерность амплитудно-частотной характеристики; низкий уровень искажений, вызванных нелинейными и переходными процессами, а также высокую чувствительность и малый уровень собственных шумов.

Точность воспроизведения перехватываемых акустических сигналов (разборчивость речи) зависит не только от типа микрофона. Важное значение имеют и характеристики электронного блока, состоящего из микрофонного усилителя и головных телефонов. В большинстве же случаев, из экономических соображений, фирмы, поставляющие направленные микрофоны, комплектуют их дешевыми электронными блоками, соответствующими аппаратуре 3-го класса бытовой техники. Поэтому владельцы таких средств зачастую вынуждены сами подбирать акустический усилитель и головные телефоны с требуемыми параметрами.

Таблица 3.

Тип микрофона	Диапазон частотной характеристики, Гц	Неравномерность воспроизводимых частот, дБ	Осевая чувствительность на частоте 1кГц, мВм^2/н
Порошковые угольные	300-3 400	20	1000
Электродинамические	30-15 000	12	1
Конденсаторные	30-15 000	5	5
Электретные	20-18 000	2	1
Пьезоэлектрические	100-5 000	15	50
Электромагнитные	300-5 000	20	5

2.2. Акустические антенны

Акустические антенны являются именно теми основополагающими элементами, которые определяют облик и основные характеристики комплексов дистанционного перехвата речевой информации. Назначение их заключается в усилении звуков, приходящих по основному направлению, и существенном ослаблении всех остальных акустических сигналов. В настоящее время разработано несколько модификаций антенн, в соответствии с которыми решено классифицировать направленные микрофоны (см. рис. 38).

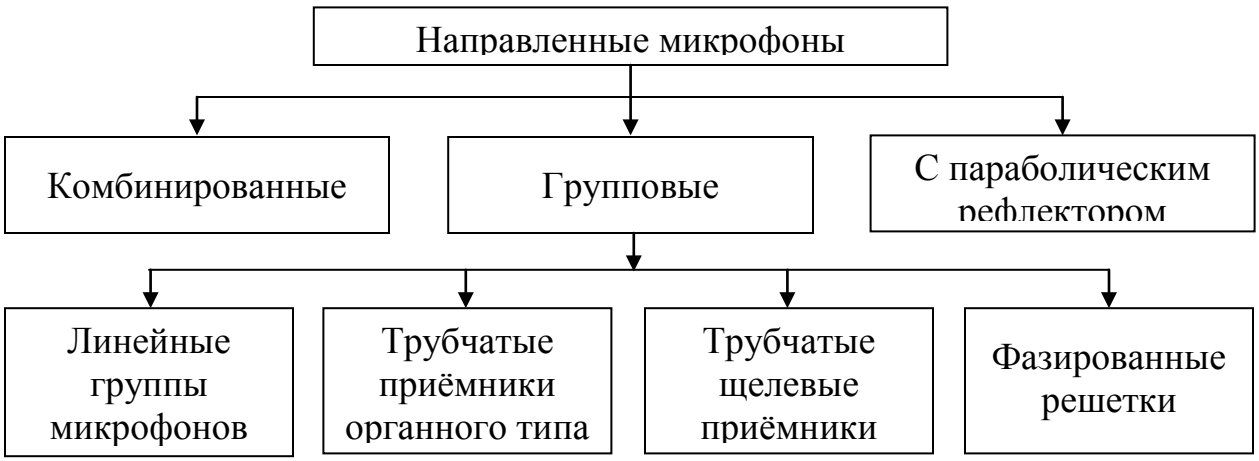

Рис. 38. Классификация направленных микрофонов

Для сравнительной оценки качества вышеперечисленных направленных микрофонов используют технические характеристики, основными из которых являются характеристика направленности и индекс направленности.

Характеристика, или диаграмма направленности – это чувствительность микрофона в зависимости от угла Θ между рабочей осью микрофона

и направлением на источник звука. Ее определяют или на ряде частот, или в пределах полосы частот. Обычно используют нормированную характеристику направленности R(Θ), то есть зависимость отношения чувствительности E_Θ измеренной под углом Θ, к осевой E_{OC} (максимальной) чувствительности.

$$R(\Theta) = E_\Theta / E_{OC} \qquad (2.1)$$

Большинство микрофонов имеет осевую симметрию, поэтому характеристика направленности для них одинакова во всех плоскостях, проходящих через ось микрофона. Графическое представление характеристик направленности часто дают в полярных координатах (см. рис. 39).

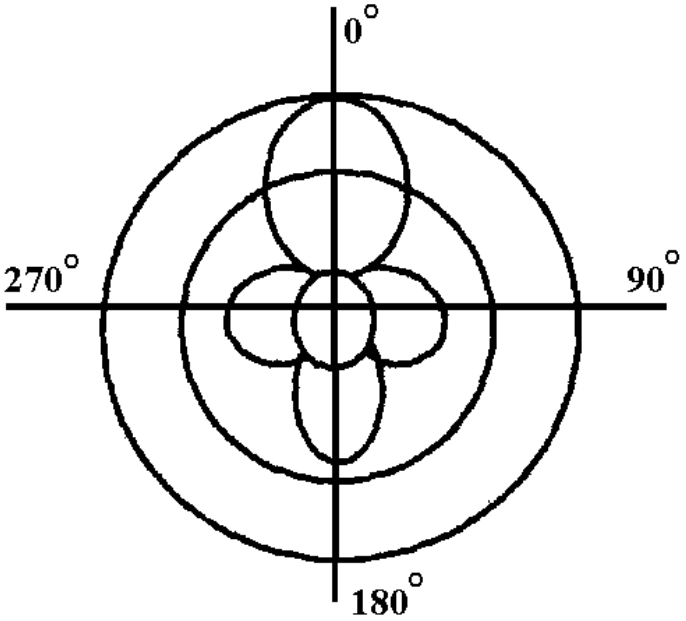

Рис. 39. Диаграмма направленности микрофона

Индекс направленности показывает выраженную в децибелах разницу уровней мощности сигналов на выходе микрофона от двух источников звука: одного (например, голоса человека), расположенного на оси, и другого – источника рассеянных звуковых волн (например, шума автотрассы), если оба создают в точке расположения микрофона одинаковое акустическое давление. Иными словами, индекс направленности показывает величину подавления (дискриминации) шума, приходящего с бокового направления, по отношению к сигналу, приходящему с направления, совпадающего с осью микрофона. Ненаправленный микрофон не подавляет шума, поэтому его индекс направленности равен нулю ($Q_{НМ}$ = 0 дБ).

Коэффициент направленного действия показывает выраженную в децибелах степень увеличения уровня сигнала на выходе микрофона при замене

ненаправленного микрофона направленным и постоянной величине акустического давления.

2.3. Комбинированные микрофоны

Комбинированные микрофоны являются простейшим видом направленных микрофонов, так как представляют из себя систему, состоящую из двух типов акустических приемников-микрофонов. Обычно это приемники давления и градиента давления, реагирующие соответственно на величину и изменение величины акустического сигнала.

Простейшая комбинация этих приемников, наиболее часто применяемая на практике, состоит из одного микрофона-приемника давления и одного микрофона-приемника градиента давления, располагаемых как можно ближе друг к другу (обычно один над другим) и так, чтобы их оси были параллельны. Изменяя параметры микрофонов, можно получать различные характеристики направленности и соответственно индексы направленности (рис. 40) всей системы.

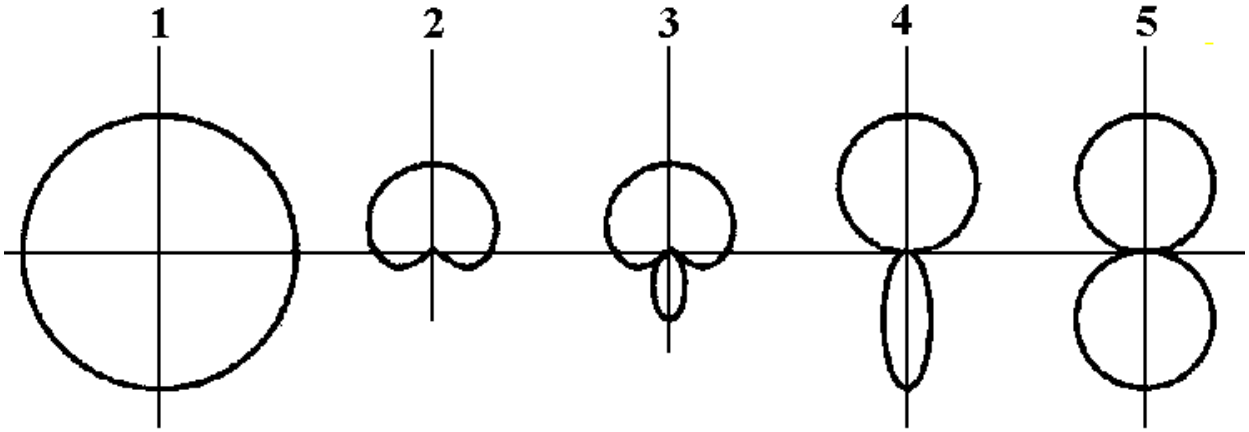

Рис. 40. Виды характеристик направленности
для комбинированных микрофонов

Виды характеристик направленности: 1 – окружность для приёмника давления; 2 – кардиоида для комбинированного приёмника с одинаковой чувствительностью приемников давления и градиента давления; 3 – суперкардиоида; 4 – гиперкардиоида; 5 – косинусоида (восьмерка) для одного приемника градиента давления. Наибольший индекс достигается для 4-го случая, когда диаграмма имеет вид гиперкардиоиды ($Q_{ГК}$ = 6 дБ).

2.4. Групповые микрофоны

К групповым акустическим приемникам относятся линейные группы, трубчатые микрофоны и фазированные решетки.

Линейная группа приемников

Линейная группа приемников (микрофонов) – это несколько микрофонов, обычно располагаемых в ряд по прямой горизонтальной линии так, чтобы их оси были параллельны друг другу (рис. 41), иногда микрофоны располагают по небольшой дуге. Электрические выходы акустических приемников последовательно соединяют в специальном смесителе.

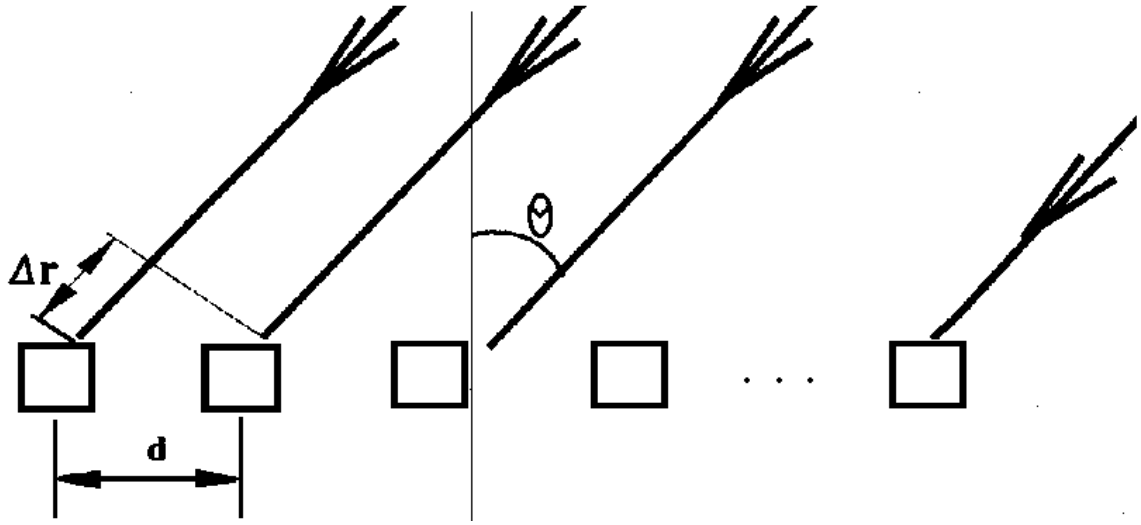

Рис. 41. Общий вид линейной группы микрофонов

Характеристика направленности такой линейной группы R(θ) из N приёмников определяется как произведение характеристики направленности одиночного приемника $R_1(\theta)$ на характеристику группы.

$$R(\theta) = R_1(\theta) \times \frac{\sin(N \cdot x)}{N \cdot \sin(x)},\ x = \frac{\pi \cdot d}{\lambda} \times \sin\theta, \qquad (2.2)$$

где d – расстояние между соседними приемниками.

Чем меньше отношение длины волны λ акустического сигнала к длине группы l = (N – 1)×d, тем уже будет основной лепесток диаграммы направленности и больше индекс направленности. Однако следует иметь в виду, что при чрезмерной длине группы (сравнимой с расстоянием от приемника до источника звука) будут сказываться интерференционные явления из-за большой разности хода звуковых волн от источника до входов отдельных микрофонов, входящих в состав группы.

Численное значение ширины основного лепестка определяется из соотношения

$$\theta_1 = \arcsin(\lambda / l). \qquad (2.3)$$

Пример. Для группового приемника, состоящего из шести ненаправленных микрофонов, расположенных по прямой линии с шагом d = 10 см (l = 50 см) и частотой принимаемого сигнала f = 1000 Гц (λ=33 см), ширина основного лепестка составляет величину $\theta_1 \approx 41°$. Расчет индекса направленности для этой группы дает величину 8 дБ.

Основной недостаток такого типа направленных микрофонов – это обеспечение направленных свойств только в плоскости, проходящей через оси микрофонов; в ортогональной плоскости характеристика такая же, как и у одиночного микрофона.

Трубчатый микрофон органного типа

Трубчатый микрофон органного типа так же использует свойства групповых антенн. Его вид схематично представлен на рис. 42.

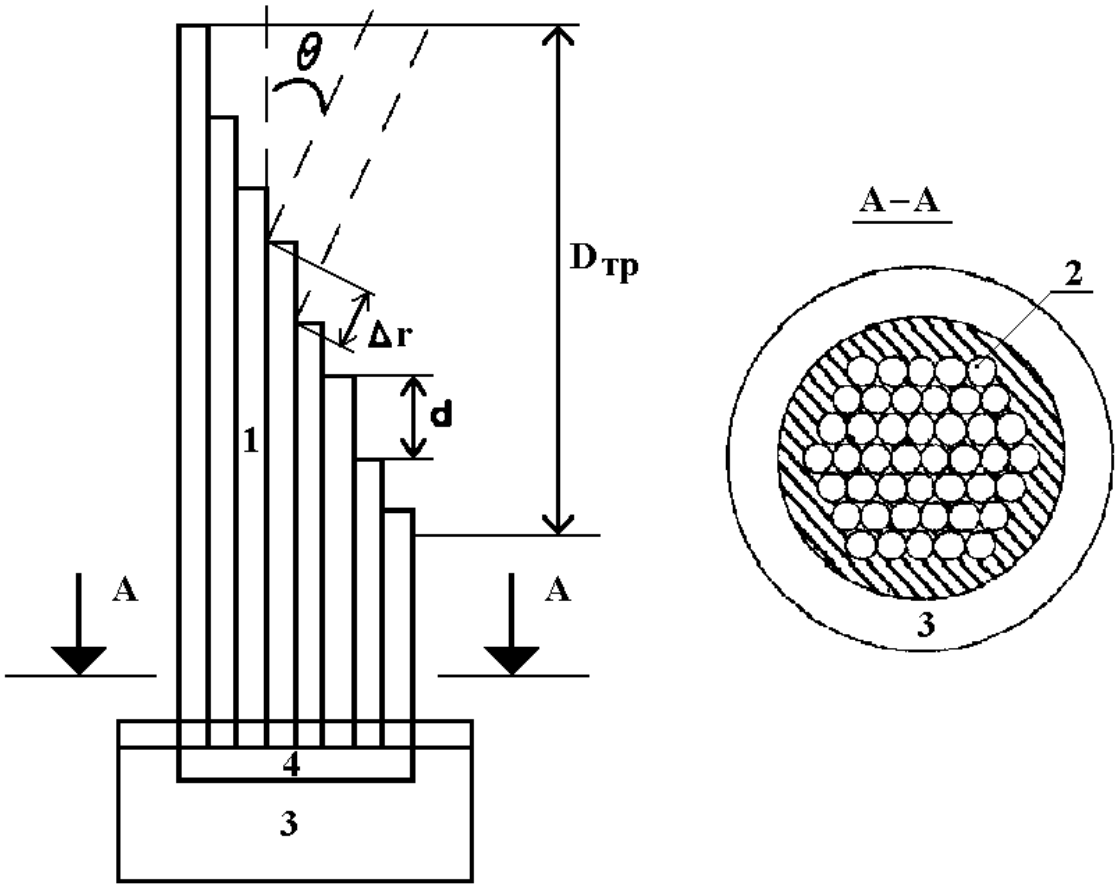

Рис. 42. Строение трубчатого микрофона органного типа

Такой микрофон имеет в своем составе несколько десятков тонких трубок 1 с длинами от нескольких сантиметров до метра и более. Эти трубки собирают в пучок – длинные по середине, короткие – по наружной поверхности. Концы трубок с одной стороны образуют плоский срез 2, входящий в

предкапсюльный объем 4. Сам микрофонный капсюль 3 выбирается, как правило, электродинамического или электромагнитного типа (приемника давления) в зависимости от требуемого частотного диапазона. Звуковые волны, приходящие к приемнику по осевому направлению, проходят в трубки и поступают в предкапсюльный объем в одинаковой фазе. Их амплитуды складываются арифметически

$$U_{\Sigma} = \sum_{i=1}^{N} U_i , \tag{2.4}$$

где N – количество трубок, а U_i – амплитуды звуковых волн.

Звуковые волны фонового шума, приходящие под углом θ к оси, оказываются сдвинутыми по фазе, так как трубки имеют разную длину, поэтому амплитуды этих волн складываются геометрически

$$U_{\Sigma} = U_i^2 + U_{i+1}^2 - 2U_i U_{i+1} \times \cos\Delta\varphi , \tag{2.5}$$

где $\Delta\varphi$ – величина разности фаз для любой пары звуковых волн, пришедших по трубкам, длины которых отличаются на величину d. Разности фаз можно найти по формуле

$$\Delta\varphi = \pi \cdot (d/\lambda) \times (1 - \cos\theta) . \tag{2.6}$$

Характеристика направленности R(θ) для такого направленного микрофона определяется из соотношения, аналогичного для линейной группы приемников (2.2):

$$R(\theta) = \frac{\sin(N \cdot x)}{N \cdot \sin(x)},\ x = \frac{\pi \cdot d_{min}}{\lambda} \times (1 - \cos\theta) , \tag{2.7}$$

где d_{min} – разница в длине между ближайшими по размеру трубками.

Приведенные соображения справедливы в случае, если в трубке не образуются резонансные колебания. С этой целью входные отверстия трубок либо их концы у капсюля закрывают при помощи пробок из пористого поглотителя.

Основным достоинством таких направленных микрофонов является высокий индекс направленности (до 8 дБ, при этом шумы, действующие с боковых направлений, ослабляются по отношению к сигналу почти в 10 раз).

Основной недостаток – большие геометрические размеры (максимальная длина трубок около 90 см). Поэтому на сегодняшний день подобные устройства не используются в промышленном шпионаже, за исключением нескольких экспериментальных изделий.

Трубчатый щелевой приемник

Трубчатый щелевой приемник (иногда его называют приемником бегущей волны) – представляет собой трубку с отверстиями или сплошной осевой прорезью по всей длине. С некоторым приближением такую трубку можно рассматривать как множество трубок разной длины, поэтому трубчатый щелевой микрофон и относят к приемникам группового типа.

Если звук приходит по оси, то пути его распространения по трубке и через отверстия одинаковы и составляющие звукового давления от пришедших колебаний синфазны и, следовательно, сумма их, воздействующая на диафрагму микрофонного капсюля, максимальна. Если же звук приходит под углом θ к оси трубки, то разность пути звука по всей трубке и пути от входа в трубку до входа в отверстие, находящееся на расстоянии d, обусловит сдвиг фаз, определяемый как

$$\Delta\varphi = 2\pi d \cdot (1 - \cos\theta) / \lambda . \qquad (2.8)$$

В свою очередь, это создает сдвиг фаз различной величины между колебаниями, пришедшими через разные отверстия, что приводит, как и в предыдущем случае, к уменьшению результирующего давления на диафрагму.

Следует отметить, что чем более высокую направленность требуется получить, тем больше должна быть длина звукоприемного элемента (трубки), так как индекс направленности увеличивается с увеличением отношения длины трубки к длине волны принимаемого излучения. Для того чтобы не образовывалось стоячих волн, наружный конец звукоприемного элемента (трубки) закрывают поглощающей тканью.

Данный тип направленного микрофона получил наибольшее распространение. Причин этому можно назвать несколько:

- простота изготовления и, как следствие, низкая стоимость;
- наличие в стране нескольких производителей данной техники;
- простота в применении;
- возможность организации различных вариантов камуфляжа.

Рассмотрим в качестве примера несколько типов направленных микрофонов трубчатого щелевого типа.

Отечественный остронаправленный микрофон **МД-74** состоит из собственно микрофона динамического типа и примыкающей к нему трубки длиной 0,8 м. В стенках трубки (см. рис. 43, в котором обозначены: *1* - микрофон; *2* - усилитель; *3* - звуковые волны; *4*~ щели; *5* - ветрозащитный поролоновый чехол) проделан ряд отверстий через равные промежутки. Для компенсации падения чувствительности микрофона на высших частотах из-за большого поглощения их в трубке вокруг каждого из отверстий устанавливаются концен-

траторы – рупорки. Размеры их подобраны таким образом, чтобы обеспечить подъем частотной характеристики на высших частотах диапазона до 10...12 дБ.

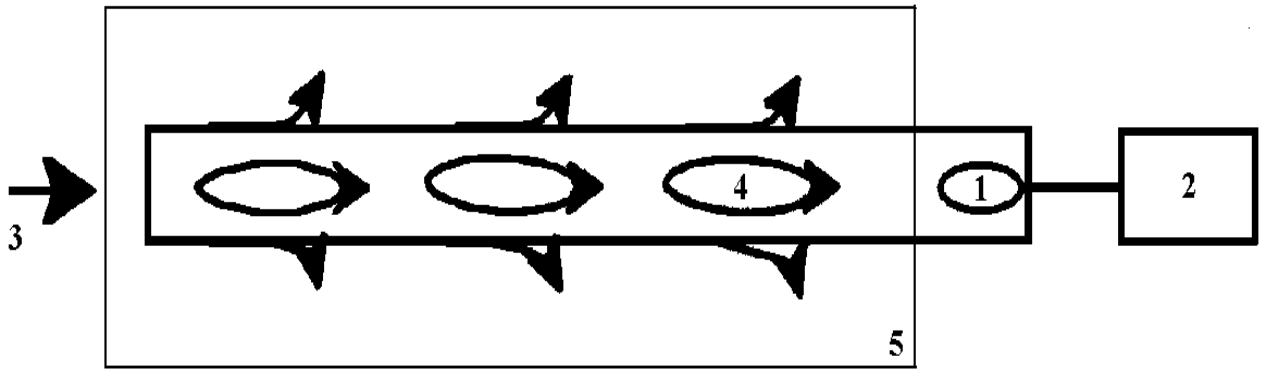

Рис. 43. Трубчатый щелевой направленный микрофон

В другом направленном микрофоне трубчатого типа **КМС-19-05** рупорки отсутствуют. Он предназначен для профессиональной записи звука при работе на относительно больших расстояниях от источника (до 100 м), в условиях повышенного окружающего шума. Основные его параметры также приведены в таблице. Блок усиления на ремнях размещается на боку оператора, что создает определенное удобство в работе. Однако опыт работы с такими микрофонами показывает, что декларируемые 100 м дальности возможно получить только в тихой загородной местности. В относительно тихом городском дворе – порядка 30 м, а на достаточно оживленной улице – 10-15 м. Можно предполагать, что подобные дальности присущи всем направленным микрофонам данного типа как отечественного, так и иностранного производства. Следует отметить, что многие направленные микрофоны трубчатого типа комплектуются ветрозащитным чехлом, обычно из поролона, благодаря чему снижается чувствительность к помехам от ветровых атмосферных воздействий.

Основные характеристики некоторых трубчатых щелевых направленных микрофонов приведены в табл. 4.

Таблица 4.

Тип микрофона	Номинальный диапазон частот, Гц	Неравномерность частотной характеристики, дБ	Направленные свойства	Внешние размеры, диаметр, мм	Масса, кг

МД-74	10- 10000	8	Остронаправленный (индекс направленности на частотах выше 125 Гц - не менее 6 дБ	71×810	0,5
КМС-19-05	20-20000	8	Остронаправленный	24×850	0,28
КМС-1909	20-20000	8	Односторонне направленный (угол раскрытия 115° при спаде на 6дБ)	24×203	0,19
МКЕ-802	50-15000	7	Суперкардиоида	22×292	0,185

Фазированные решетки

К *фазированным решеткам* по устоявшейся в настоящее время терминологии относят изделия, имеющие плоскость, на которой расположены открытые торцы звуководов; они обеспечивают синфазное сложение звуковых полей от источника в некотором акустическом сумматоре, на выходе которого расположен микрофон (см. рис. 44). На рисунке приняты обозначения: 1 - микрофон; 2 - усилитель; 3 - звуковая волна; 4 - торцы звуководы; 5 - звуководы; б - акустический микрофон. Если звук приходит с осевого направления, то все сигналы, распространяющиеся по звуководам, будут в фазе, и сложение в акустическом сумматоре даст максимальный результат. Если направление на источник звука не осевое, а под некоторым углом к оси, то сигналы от различных точек приемной плоскости будут разными по фазе и результат их сложения будет меньше. При этом число приемных точек может достигать нескольких десятков. Очевидно, что подобная решетка является менее громоздкой, чем микрофон органного типа, но она существенно проигрывает последнему в направленных свойствах.

Коэффициент направленного действия для данного типа направленного микрофона приблизительно определяют по формуле:

$$Q = 4\pi S/\lambda^2 = 4\pi N^2(0.5\lambda^2)/\lambda^2 = \pi N^2, \qquad (2.9)$$

где S – площадь входной аппертуры, м^2; λ – длина волны звука, м; N – число элементов решетки.

Данная формула применима при расположении элементов антенной решетки по фронту на расстоянии около 15 см. Примером направленного микрофона такого типа является изделие **«Шорох».**

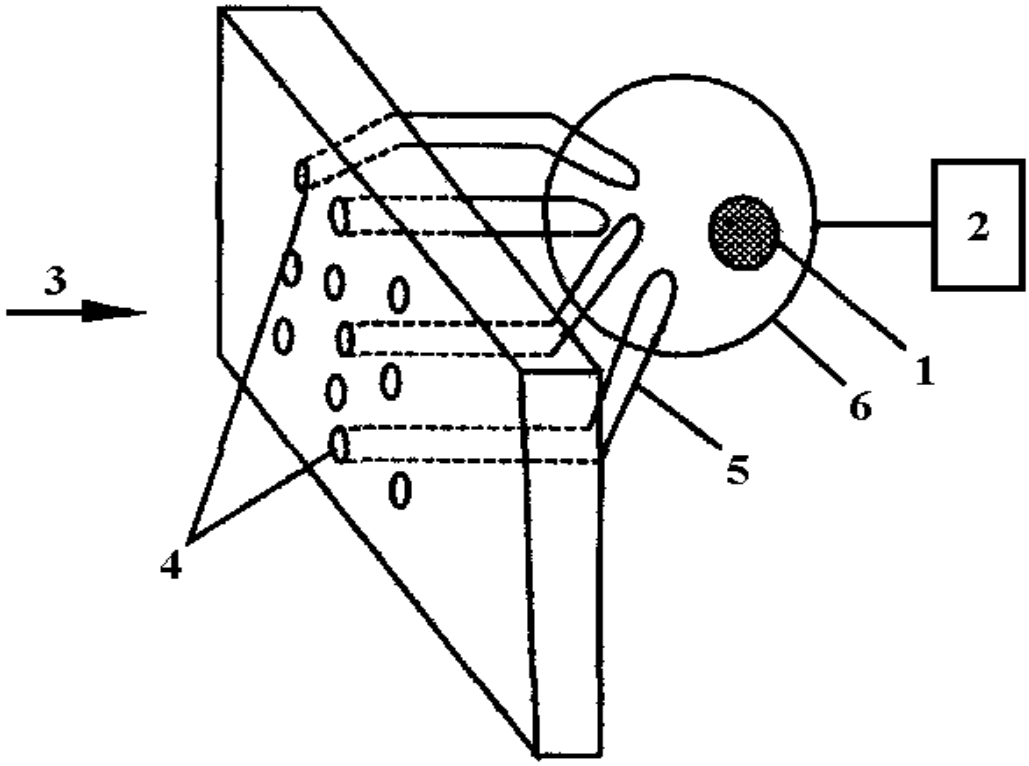

Рис. 44. Направленный микрофон типа «фазированная решетка»

Оно относится к устройствам, предназначенным для прослушивания и записи речевой информации в условиях открытого пространства, в диапазоне частот 100-10000 Гц. Предельная паспортная дальность съема информации – 30–40 м при уровнях шума 74-76 дБ и речи 70-74 дБ. Однако в зависимости от шумовой обстановки и уровня информации дальность съема будет изменяться. Микрофон выполнен в виде гибкой пластины размером 320×320 мм, имеющей на внешней поверхности (от оператора) большое число акустических входных отверстий. За счет звуководов и суммирующих устройств образуется фазированная решетка, позволяющая сформировать диаграмму с шириной основного лепестка около $30\text{-}40^0$ на частоте 1 кГц. Коэффициент направленного действия составляет около 12 дБ.

Микрофон, размещенный в специальном чехле, может устанавливаться на теле оператора, под одеждой в варианте «грудь–спина» (фронт–тыл). На поясе чехла размещен манипулятор, состоящий из усилителя низкой частоты с автоматической регулировкой усиления, источника питания и органов управления: «включено–выключено» с первоначальной установкой уровня полезного сигнала и два выхода на магнитофон и головные телефоны. Функциональные возможности изделия могут расширяться за счет дополнительной установки радиоканала и других сервисных устройств. Конструктивные особенности позволяют легко камуфлировать микрофон под папку, дипломат,

картину и т. д. Так как работа в помещении характеризуется наличием большого количества переотраженных сигналов от различных элементов строительных конструкций в виде стен, потолков, колонн, то максимальная эффективность работы такого направленного микрофона достигается в помещениях с объемом более 500 м^3.

Рекомендуется избегать использования двух слоев одежды поверх микрофона, один из которых утеплен или выполнен из кожи (кожзаменителя). Полезный сигнал можно записывать без предварительного контроля, но при этом следует помнить, что расстояние до источника звука не должно, более, чем 4–5 раз, превышать расстояние, при котором обеспечивается требуемое качество записи, выполненной ненаправленным микрофоном.

Известны и другие образцы антенных решеток, выполненные, например, в виде бруска, который может камуфлироваться под различные предметы. Оценочные расчеты показывают, что в зависимости от геометрических размеров бруска коэффициент направленного действия находится в пределах 2-5 дБ.

2.5. Направленные микрофоны с параболическим рефлектором

Принцип действия подобных устройств достаточно прост и понятен. Микрофон размещен в фокусе отражателя параболической формы (см. рис. 45). Звуковые волны 3 с осевого направления, отражаясь от параболического зеркала 2, суммируются в фазе в фокальной точке 1 (на микрофоне). Возникает усиление звукового поля. Чем больше диаметр зеркала отражателя, тем большее усиление может обеспечить устройство. Если направление прихода звука не осевое, то сложение отраженных от различных частей параболического зеркала звуковых волн, приходящих в фокус, даст меньший результат, поскольку не все слагаемые будут в фазе. Ослабление тем сильнее, чем больше угол прихода звука по отношению к оси. Создается, таким образом, угловая избирательность по приему.

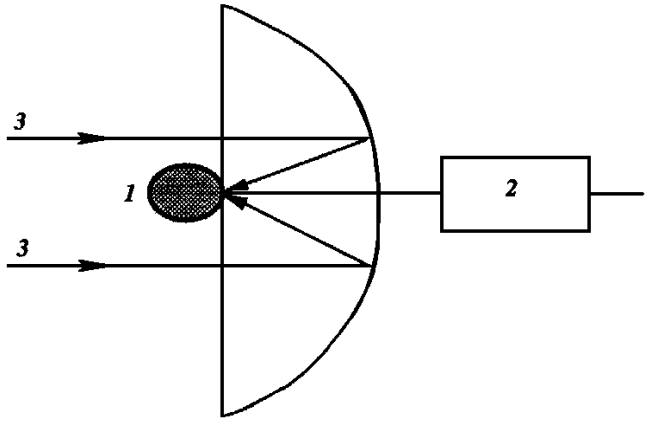

Рис. 45. Параболический направленный микрофон

Коэффициент направленного действия (КНД) для данного типа направленного микрофона можно приблизительно определить по формуле:

$$Q = 4\pi S_э / \lambda^2, \qquad (2.10)$$

где $S_э$ – эффективная поверхность антенны.

Понятие эффективной поверхности тесно связано с максимальной мощностью, которая может быть извлечена приемной антенной из падающей плоской акустической волны. При выполнении ряда условий, а именно $D > \lambda$, где D – диаметр рефлектора; совмещение максимума диаграммы направленности с направлением прихода волны и др. - можно приближенно считать, что $S_э \approx S$, где S – площадь входной аппертуры, м^2.

Как правило, фирмами-изготовителями поставляется в комплекте блок усиления с системой автоматической регулировки усиления и выходами на наушники и магнитофон, иногда акустические фильтры. При работе параболическую антенну с микрофоном можно держать в руках или закрепить на треноге.

В качестве примеров направленных микрофонов с параболическим отражателем рассмотрим несколько систем.

Портативный параболический приемник **PRO-200** предназначен для дистанционного приема звуковых волн. Обладает высокой чувствительностью и острой диаграммой направленности параболического зеркала. Оборудован дополнительным регулируемым фильтром, позволяющим осуществлять частотную селекцию сигнала по ширине и положению его спектра на оси частот. Паспортная дальность – 1 км. Очевидно эта величина приведена для наилучших условий приема: тихая открытая местность, ночь, человек говорит в полный голос. Имеется возможность подключения к магнитофону. Питание – от встроенного аккумулятора или внешнего зарядного устройства от сети 220 В. Диаметр зеркала – 60 и 75 см (качество приема улучшается с увеличением диаметра зеркала).

Значения коэффициента направленного действия (КНД) антенны в зависимости от диаметра зеркала и частоты принимаемого акустического сигнала приведены в табл. 5.

Таблица 5.

Частота, Гц	КНД при диаметре зеркала 0,6 м	КНД при диаметре зеркала 0,75 м
500	1	11
1000	15	17
5000	19	31
10000	35	37

Другой направленный микрофон (типа **А–2**) имеет параболический отражатель диаметром 43 см, снабжен усилителем и наушниками. Паспортная дальность действия на открытой местности также заявлена около 1км (!). Коэффициент усиления электронного блока – не менее 80 дБ. Имеется система автоматической регулировки усиления с динамическим диапазоном входных сигналов 40 дБ.

Параболические направленные микрофоны РК375 и РК390 (производство Германии) имеют следующие параметры.

РК375: габариты – Ø 600×300 мм, масса – 1,2 кг, коэффициент усиления – 90 дБ, питание – 5 В, автономность – 75 часов.

РК390, соответственно: Ø 130×100 мм, 1,1 кг, 70 дБ, 9 В, 50 часов. Паспортная дальность – до 50 м (пунктуальности немцев можно позавидовать).

Особенности оперативного применения направленных микрофонов таковы, что неподготовленный человек не сможет их скрытно использовать, так как необходимо не только правильно расположиться относительно объекта разведки и источников шумов, но при этом и самому не быть обнаруженным. Особенно в случае использования направленных микрофонов с параболическими отражателями из-за их существенных размеров. Зарубежные специалисты рекомендуют применять такие микрофоны только в условиях ограниченной видимости и при относительно низких уровнях окружающих шумов, например, ночью. При этом честно информируют, что акустический телескоп может не улавливать звуки на большом (заявленном) расстоянии, если он используется в местах с повышенным уровнем фонового шума. Внешний вид некоторых типов направленных микрофонов представлен на рис. 46-49.

Рис. 46. Параболический стационарный микрофон с наушниками

Рис. 47. Параболический переносной микрофон с наушниками

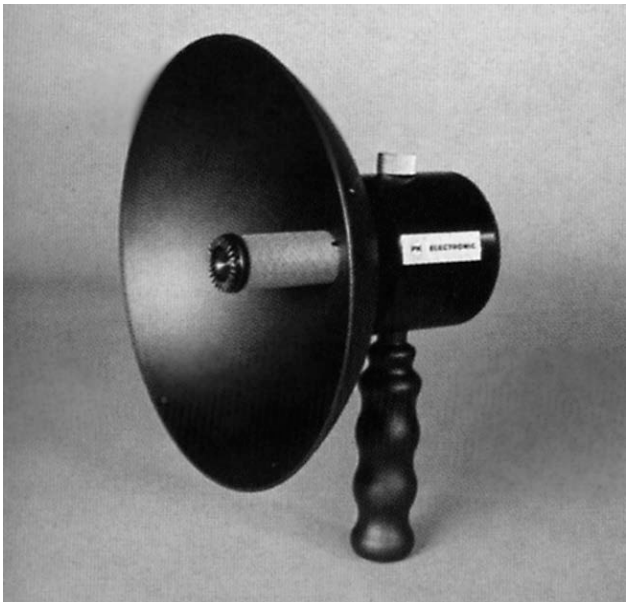

Рис. 48. Параболический ручной микрофон

Рис. 49. Трубчатый микрофон закамуфлированный под зонтик

2.6. Особенности применения направленных микрофонов

На дальность дистанционной записи влияют не только параметры микрофонов, но и условия, в которых применяются эти устройства, следует знать некоторые особенности использования направленных микрофонов.

На открытой местности

К открытой местности обычно относят участки, не имеющие ярко выраженных ограждающих конструкций, которые создают замкнутый объем. Как правило, это улицы, площади, стадионы, дворы, парки, залы летних кафе, пляжи и т. п. К работе на открытых площадках относят и прослушивание разговоров, ведущихся в помещениях, если перехват ведется через открытое окно, форточку или опущенное стекло автомобиля.

Основными ограничениями на ведение негласного съема информации в таких условиях является затухание, которое испытывает сигнал при его распространении, и высокий уровень фоновых шумов. Величина затухания обусловливается рядом факторов, которые зависят как от характеристик самого звука, так и от свойств среды распространения. Все их делят на две большие группы.

В первую группу входят факторы, связанные с законами распространения акустических волн. А именно:

- при распространении в неограниченной среде от источника конечных размеров интенсивность звука убывает обратно пропорционально квадрату пройденного расстояния;

- неоднородности среды (капли дождя, ветки деревьев и другие препятствия) вызывают рассеяние звуковых волн, приводящее к ослаблению сигнала в «основном» направлении;
- на распространение звука в атмосфере влияют турбулентности, распределения температуры и давления, сила и скорость ветра, которые вызывают искривление звуковых лучей, а иногда вообще нарушают передачу звука.

Действительно, звуковая волна, попадая на границу раздела двух слоев атмосферы с различными характеристиками, частично отражается, а частично проникает в другой слой. При этом преломление волны происходит в соответствии с законом физики, гласящим, что отношение угла падения φ_1 к углу преломления φ_2 определяется отношением скоростей распространения звуковых колебаний в этих средах (слоях):

$$\sin \varphi_1 / \sin \varphi_2 = C_1 / C_2, \qquad (2.10)$$

где C_1 и C_2 – скорости звука в обеих средах.

Если параметры обоих слоев близки друг к другу, то фактически вся энергия переходит из одной среды в другую и $\varphi_1 \approx \varphi_2$. Когда же параметры различны, имеет место искривление звуковых лучей. Именно по этой причине оператор часто вынужден размещать микрофон как можно выше над поверхностью земли, чтобы обеспечить максимальную дальность перехвата акустических сигналов.

Вторая группа связана с физическими процессами в веществе – необратимыми переходами звуковой энергии в другие формы (главным образом в тепло). Можно выделить следующие факторы, определяющие степень поглощения звуковых волн:

- поглощение звука возрастает пропорционально квадрату частоты (поэтому колебания с частотами выше 1000 Гц затухают особенно быстро);
- степень поглощения растет при уменьшении относительной влажности воздуха (так, например, при влажности 50 % акустические сигналы с частотой 10 кГц затухают только на 14 дБ на каждые 100 м, а при уменьшении влажности до 15 % затухание возрастает вдвое и достигает 28 дБ; ветер, дождь и снег могут добавить еще 8-10 дБ на каждые 100 м).

Строго говоря, открытых пространств, в которых звуковые волны распространялись бы беспрепятственно во всех направлениях, практически нет, так как, всегда имеют место отражения от земной поверхности, стен ближайших зданий, предметов и т. п. Однако эти переотражения можно учесть, а иногда и просто пренебречь ими, если они незначительны из-за высокого коэффициента поглощения (например, от снежного покрова).

Высокий уровень акустических шумов – другая специфика открытых пространств. Для осуществления оценки влияния их на качество фиксации акустической информации используют понятие *уровня громкости*, под которым понимают уровень равногромкого с мешающим сигналом чистого тона на частоте 1000 Гц, выраженный в децибелах. За единицу уровня принимают 1 (один) Фон, то есть

$$L_g[Фон] = L_{1000\,Гц}[дБ]. \qquad (2.11)$$

В табл. 6 приведены уровни громкости различных шумов в зависимости от дальности источника. Сравнивая приведенные значения с уровнем обычной речи, который составляет 65-75 дБ, делают вывод о степени влияния акустических помех на качество перехвата.

Таблица 6.

Источник шума и место его измерения	Уровень громкости, дБ
Громкий автомобильный гудок на расстоянии 8м	95-100
Электропоезд на эстакаде на расстоянии 6 м	90
Шум в поезде метро во время движения	85-90
Автобус (полный ход) на расстоянии 5 м	85-88
Трамвай на расстоянии 10-20м	80-85
Троллейбус на расстоянии 5 м	77
Грузовой автомобиль на расстоянии 5-20 м	60-75
Легковой автомобиль на расстоянии 5-20 м	50-65
Шумная улица без трамвайного движения	60-75
Обычный средний шум на улице	55-60
То же, в момент затишья днем	40
Тихая улица (без движения транспорта)	30-35
Тихий сад	20
Деревообрабатывающая фабрика	96-98
Зал при массовых сценах	75-95
Шумное собрание	65...70
Шепот на расстоянии 1 м	20
Разговор на расстоянии 1 м: громкий/обычный	65-70/55-60
Коридоры	35-40
Кафе	50-52

Из вышесказанного следует, что на дальность фиксации речевой информации на открытом участке местности влияют следующие факторы: направление и сила ветра, температура и влажность воздуха, характер рельефа, наличие строений, растительность, уровни фоновых шумов. Дальность ведения разведки увеличивается, если ветер дует со стороны источника звука, но-

чью и ранним утром, в пасмурную погоду, особенно после дождя, у водной поверхности, в горах, зимой (при отсутствии снегопада). Звук поглощается (становится слабее) в жаркую солнечную погоду, во время снегопада, дождя, в лесу, кустарнике и на местности с песчаным грунтом, при наличии искусственных и естественных препятствий.

Следует еще раз подчеркнуть, что приведенные цифры относятся к идеальной обстановке и открытому пространству, а в реальных городских условиях практически невозможно проводить съем информации с расстояний, превышающих 10-15 м на шумной улице, 15-25 м – в остальных случаях. В загородных условиях – это 30-100 м. В принципе, необходимо запомнить простое правило: если оператор слышит речь своим ухом, но не может разобрать лишь отдельные слова, то с помощью хорошего направленного микрофона возможно осуществить перехват и звукозапись разговора; в противном случае никакой направленный микрофон не поможет.

В помещениях

Отличительной особенностью применения направленных микрофонов в помещениях является более сложное звуковое поле полезного сигнала, которое представляет из себя суперпозицию составляющей «прямого» звука, созданной звуковыми волнами, не испытавшими ни одного отражения, и составляющих, созданных несколькими отраженными звуковыми волнами. Поле отраженных звуковых волн почти всегда близко к диффузному.

Акустические шумы в помещениях так же, как и на открытой местности, существенно ограничивают динамический диапазон принимаемой информации, снижают разборчивость речи. Эти шумы создаются как людьми, так и вибрациями, проникающими в помещение извне (с улицы или из соседних помещений). Уровни шумов, создаваемые людьми, зависят от их количества в помещении, громкости разговоров и т. д. Уровни шумов (вибраций), проникающих снаружи, определяются звукоизоляцией помещения и уровнями внешних шумов.

В табл. 7 приведены санитарные нормы допустимых уровней акустических шумов, характерных для различных типов помещений. Приведенные цифры позволяют составить представления об условиях перехвата речевой информации с помощью направленных микрофонов. Здесь уместно еще раз напомнить, что уровень обычной речи на расстоянии 1 м составляет 65-75 дБ.

Таблица 7.

Тип помещения	Норма, дБ
Для сна и отдыха	35

Для умственной работы без собственных источников шума (конструкторские бюро, комнаты программистов, лаборатории для теоретических работ и обработки экспериментальных данных)	45
Для конторского труда с источниками шума (принтеры), цеховой администрации, а также помещения, где источником шума являются люди (кассовые и справочные залы)	55
Производственные помещения, гаражи, механические мастерские	80

В общем случае лучшее качество перехвата информации в помещении обеспечивается при размещении направленного микрофона рабочей осью на источник сигнала (человека или группу людей), а тылом к источникам акустических помех. При этом оператор должен стремиться занять максимально тихое место (избегая углы, где особенно много переотраженных сигналов) в зоне действия прямого звука.

2.7. Перспективы развития направленных микрофонов

Конструкция направленных микрофонов непрерывно совершенствуется, так как проблема дистанционной записи речи становится все более актуальной в рамках развития систем негласного съема информации. Однако революционного переворота (в смысле увеличения радиуса перехвата до километров) в данной области техники не предвидится. В то же время можно выделить следующие направления улучшения характеристик направленных микрофонов:

1. Возможно появление приборов, способных к адаптивной пространственно-временной фильтрации акустических помех. Объективной основой таких приборов являются достижения в области цифровой многоканальной обработки данных (специализированный компьютер станет такой же привычной составной частью направленного микрофона, как наушники);

2. Прогресс в области высокочувствительных акустических сенсоров принципиально позволяет в ближайшем будущем создать микрофоны с пороговой чувствительностью –10-15 дБ, что позволит несколько повысить дальность перехвата акустической информации (при отсутствии акустических помех и шумов);

3. Ожидается появление принципиально новых устройств, использующих нелинейные и параметрические эффекты для реализации органолептических скрытых антенн большого размера, способных увеличить коэффициент направленного действия до 25 дБ и более.

3. ДИКТОФОНЫ

Осуществление негласной (скрытой) звукозаписи является одним из наиболее распространенных приемов промышленного шпионажа. Полученные записи используют для получения односторонних преимуществ в коммерческих сделках, оказания давления на партнеров, шантажа и т. д.

Для того чтобы уберечь себя от подобных последствий, необходимо знать основные особенности скрытой звукозаписи, факторы, влияющие на качество фиксации информации, характерные приемы. Эти знания помогут обратить внимание на особенности поведения людей, пытающихся вас записать, правильно выбрать место конфиденциальной встречи, исключить нахождение «случайно забытых» вещей в вашем рабочем кабинете или офисе.

3.1. Факторы, влияющие на качество звукозаписи

При рассмотрении вопросов применения направленных микрофонов в реальных условиях отмечалось, что работы на открытой местности и в замкнутом пространстве (помещении) различаются более сложными условиями для последнего случая. Рассмотрим его более подробно.

Звукозапись в помещении сопровождается большим количеством акустических помех, связанных, во-первых, с наличием многократно отраженных волн от внутренней обстановки помещения, а, во-вторых, с наличием шумов, создаваемых как людьми, так и шумами и вибрациями, проникающими в помещение извне (с улицы или из соседних помещений).

Акустическое поле в замкнутом объеме можно представить как сумму составляющих поля «прямого» звука, создаваемого звуковыми волнами, не испытавшими ни одного отражения, и составляющих поля, создаваемых отраженными звуковыми волнами. Поле отраженных звуковых волн почти всегда можно считать близким к диффузному, поэтому его часто называют диффузной составляющей.

Для оценки ее влияния на акустические свойства помещения, а следовательно и качество записи, вводят понятие *акустического отношения* для установившегося режима. Оно определяется как отношение суммарного уровня отраженных волн к уровню прямой волны.

В реальных условиях акустическое отношение для удаленных от источника звука точек помещения редко бывает меньше единицы, как правило, оно значительно больше, а иногда даже доходит до величины, равной 10-15. То есть уровень отраженных волн в помещении обычно выше уровня прямого звука. При акустическом отношении больше четырех отраженный звук создает недопустимые помехи для регистрации речевой информации.

Пороговое значение расстояния от источника звука, при котором акустическое отношение равно единице, называют *радиусом гулкости,* так как

при большем расстоянии диффузная составляющая становится больше составляющей прямого звука, и в записанном сигнале появляется характерная гулкость.

Однако акустическое отношение полностью не характеризует качество восприятия звука в помещении, так как не все отраженные сигналы вносят помехи, поэтому вводят еще одно понятие – *четкость звучания.* Под ним понимают отношение плотности энергии прямого звука ($E_{пр}$), суммируемой с плотностью отраженных звуковых волн, приходящих в данную точку помещения в течение времени t = 60 мс после прихода прямого звука $E_{t=60мс}$ (и потому воспринимаемых с ним слитно), к общей плотности энергии E_m:

$$S_t = (E_{пр}+E_{t=60\ мс})/E_m. \qquad (3.1)$$

То есть четкость звучания характеризует относительную величину всей полезной энергии $E_{пол}$. В этом её преимущество перед акустическим отношением. Чем больше четкость звучания, тем меньше влияние помех от запаздывающих лучей из-за явления реверберации. Однако на практике существуют большие трудности по измерению этой величины.

Акустические шумы в помещениях существенно ограничивают динамический диапазон регистрируемой информации, снижают разборчивость речи. Степень их влияния зависит от количества людей в помещении, громкости разговоров, а также уровня шумов, проникающих извне.

В условиях тишины слышны писк комара, жужжание мухи, тиканье часов и другие звуки, а в условиях шума и помех можно не услышать даже громкий разговор. Другими словами, в условиях шума и помех порог слышимости для приема слабого звука возрастает. Это повышение порога слышимости называют *акустической маскировкой*. Величина маскировки определяется величиной повышения порога слышимости для принимаемого звукового сигнала.

К сожалению, внешние шумы не исчерпывают список помех, возникающих при негласной записи акустической информации. Дело в том, что закамуфлированный в одежде магнитофон записывает все окружающие его шумы, и в первую очередь создаваемые самим оператором, так как он, как правило, ближе всего расположен к микрофону. Так, например, люди дышат, а это значит, что одежда на них постоянно находится в движении – ремень поскрипывает от поднимающейся и опускающейся диафрагмы, пиджак трется о сорочку и т. д. Люди этого не слышат, однако, микрофон, спрятанный в одежде, улавливает все, и записанный разговор будет сопровождать невероятный фоновый шум.

Множество различных звуков сопровождают нас, даже если человек неподвижно застывает в кресле. Работа желудка и та создает помеху качественной записи, если «сосет под ложечкой». Конечно, может быть интересным сидеть и изучать изменения внутренних ритмов организма в зависимости от развития ситуации. Но кто сумеет распознать все прочее? Самое большое неудобство для диктофонной записи – беседа на ходу. Здесь «фонит» все: рукава, трущиеся по мере размахивания руками, верхняя одежда, содержимое карманов (всякие ключики, мелочь, бумажки – все бряцает, шуршит и скрипит). Окружающие шумы также будут уловлены и записаны. И если в нормальной жизни мы их не слышим, используя природой данные фильтры, то при воспроизведении записи все будет воссоздано в самом неудобном виде.

Рассмотренные факторы являются принципиальными при проведении негласной звукозаписи, и они должны учитываться при выборе места для микрофона звукозаписывающего устройства.

3.2. Выбор типа микрофона и места его установки

Многие современные диктофоны позволяют выбирать между встроенным и выносным микрофонами в зависимости от условий ведения звукозаписи. Конечно, встроенный микрофон делает устройство более компактным и эргономичным. Однако его возможности по ведению скрытой фиксации аудиоинформации существенно ограничены, так как такие микрофоны обладают достаточно скромными характеристиками из-за предельно малых размеров, а их размещение полностью определяется размером и камуфляжем всего записывающего устройства.

Иначе обстоит дело с выносными акустическими приемниками. Они хорошо камуфлируются и поэтому могут быть установлены в зоне, обеспечивающей высокое качество записи. Выбору места возможного размещения и типа именно таких микрофонов следует уделить особое внимание.

При размещении выносных акустических приемников операторы, как правило, учитывают следующие ниже перечисленные три фактора.

Количество записываемых источников речевых сигналов

Для записи *одного собеседника* обычно применяют односторонне направленные микрофоны с расстояния 50–70 см. Реже используют и двусторонне направленные микрофоны (например, ленточные). Однако минимальная дальность до источника в этом случае возрастает до 80–100 см, так как на более близком расстоянии запись будет «бубнить».

Для фиксации *диалога* подходят как двусторонне, так и односторонне направленные микрофоны. В первом случае микрофон располагают между собеседниками, в последнем – его стараются установить так, чтобы оба объ-

екта оказались симметрично расположенными относительно рабочей оси акустического приемника.

Для фиксации разговора *нескольких собеседников* чаще применяют односторонне направленные микрофоны с большим перепадом чувствительности по линии «фронт–тыл». Их размещают таким образом, чтобы рабочая ось была направлена на собеседников, а тыл в сторону источников акустических помех.

Для записи *сцены «за круглым столом»* чаще используют односторонне направленные микрофоны. В идеальном случае их размещают в центре в вертикальном положении с направлением нулевой чувствительности вниз.

Пространственная ориентация микрофона

Вообще пространственная ориентация определяется зависимостью чувствительности микрофона от угла между его рабочей осью и направлением на источник звука. Для большинства типов акустических приемников увеличение этого угла сопровождается падением как общей чувствительности, так и, в особенности, чувствительности на высоких частотах. Лишь у некоторых типов микрофонов, например, двусторонне направленных (восьмеричных) и в меньшей степени односторонне направленных, чувствительность на высоких частотах изменяется при повороте рабочей оси от направления так же, как и чувствительность на низких частотах. Поэтому микрофоны направляются своей рабочей осью не на источник только в тех случаях, когда надо сделать запись этого звука менее громкой на фоне других или же придать звучанию большую мягкость и меньшую четкость.

Дальность до источника акустического сигнала

Величина расстояния до источника определяется, исходя из свойств помещения, в котором осуществляется аудиозапись, и свойств микрофона и источника.

Акустические процессы в каждой точке помещения довольно хорошо, как отмечалось выше, определяются величиной акустического отношения. Восприятие же источника в нем зависит от того, в каком соотношении находятся расстояние от источника до микрофона и радиус гулкости помещения.

Если расстояние от источника до микрофона меньше радиуса гулкости, то при воспроизведении кажущиеся размеры источника звука больше фактических, а размеры окружающего пространства меньше фактических. При этом создается общее впечатление близости и интимности звучания. При расстоянии микрофона от источника больше радиуса гулкости, наоборот, размеры источника кажутся меньше фактических, а окружающего пространства – больше. Общее впечатление от звучания – объемность, «воздушность», мощ-

ность. При расположении микрофона от источника звука на расстоянии, равном радиусу гулкости, качество звучания при воспроизведении является промежуточным по сравнению с описанным выше.

Организация сеанса деловой звукозаписи

В основном при проведении сеансов «деловой» звукозаписи с помощью диктофонов используются встроенные или выносные электретные микрофоны, входящие в комплект магнитофона. В штатный комплект профессионального магнитофона микрофоны, как правило, не входят, поэтому приходится подбирать их из числа имеющихся в продаже и подходящих для данной модели магнитофона.

При выборе микрофона для «деловой» звукозаписи следует в первую очередь обращать внимание на следующие параметры:

1. *Чувствительность* - отношение величины напряжения, развиваемого микрофоном на номинальном сопротивлении нагрузки, к величине звукового давления, воздействующего на диафрагму микрофона. Чувствительность профессиональных конденсаторных и электретных микрофонов может достигать 20 мВ/Па и выше, бытовых - до 3 мВ/Па, электродинамических микрофонов - до *2* мВ/Па.

2. *Номинальный частотный диапазон* - характеризует зависимость чувствительности микрофона от частоты акустических колебаний. Чем шире и равномернее частотный диапазон, тем выше качество микрофона. Для профессиональных микрофонов он может достигать 20 - 20000 Гц.

3. *Номинальное сопротивление нагрузки* - сопротивление, при котором обеспечиваются заданные параметры микрофона. Оно должно быть согласовано с входным сопротивлением магнитофона.

4. Диаграмма направленности - графическое изображение зависимости чувствительности микрофона от угла между направлением его максимальной чувствительности (рабочей осью) и направлением на источник звука. Наиболее часто встречаются круговая, косинусоидальная и кардиоидная диаграммы направленности.

Каждый сеанс деловой звукозаписи по своему уникален и, поэтому, требует продуманной организации и четкой реализации оператором всех заранее намеченных действий в ходе его проведения. Из многочисленных факторов, оказывающих влияние на выбор аппаратуры звукозаписи, оптимальные варианты ее размещения и тактику построения оператором предстоящей беседы особое внимание следует уделять предварительному выяснению следующих из них:

- где будет проводиться беседа;

- характер акустической обстановки в месте предполагаемого проведения сеанса звукозаписи (наличие в помещении звуковоспроизводящей аппаратуры, вентиляторов, кондиционеров, шумов с улицы, будет ли во время беседы приниматься пища, беседа будет проходить в тихом кабинете, шумном зале, в автомобиле, на шумной улице или в загородных условиях и т.д.);
- характерные особенности и привычки собеседника (наличие дефектов речи, привычки обниматься при встрече, похлопывать по карманам, говорить со своим окружением на другом языке и т, п.);
- имеющиеся в распоряжении средства деловой звукозаписи (малогабаритный микрокассетный магнитофон, портативный кассетный магнитофон, закамуфлированные средства звукозаписи и т.д.) и их максимальные ресурсы записи;
- возможные места размещения аппаратуры звукозаписи (наличие при операторе носимых предметов типа сумки, атташе-кейса, может ли он надеть на встречу верхнюю одежду свободного покроя, темную плотную сорочку и т.д.);
- ожидаемая продолжительность встречи, в какой период ее проведения предполагается обсудить наиболее значимые вопросы;
- возможность управления магнитофоном в процессе проведения мероприятия.

Если имеется предварительная возможность выбора места проведения сеанса деловой звукозаписи, то подготовка к нему начинается с подбора места, благоприятной для звукозаписи акустической обстановки. Дело в том, что в отличие от человеческого уха, которое, как правило, легко адаптируется к окружающей шумовой обстановке, микрофон любого магнитофона практически одинаково регистрирует все раздающиеся в данном помещении звуки, независимо от источника их происхождения. Следует отметить, что микрофоны аппаратуры магнитной звукозаписи в отличие от человеческого уха лучше воспринимают различные высокочастотные звуки (например, резкие женские голоса, щебет птиц и т.п.). При этом следует стремиться использовать выносной микрофон, т. к. им практически не воспринимаются помеховые шумы от движения лентопротяжного механизма магнитофона, также появляется возможность располагать сам микрофон наиболее близко к собеседнику и подальше от других источников помех в помещении. Наиболее удобными местами размещения выносного микрофона являются: на груди под узлом галстука, на краю плеча под пиджаком или курткой, на поясе около ремня и т.п.

Место расположения в помещении звукозаписывающего устройства или его выносного микрофона должно подбираться таким образом, чтобы оно было максимально удалено от источников акустических помех при возможно

минимальном расстоянии до источника интересующей вас информации и располагаться таким образом, чтобы максимум чувствительности микрофона, перпендикулярный плоскости, где находится его акустическое отверстие, был направлен в сторону вашего собеседника. Если позволяет ресурс магнитофона, с целью улучшения качества записи следует стремиться производить запись на более высокой скорости движения ленты магнитофона.

Таким образом, лучше всего проводить сеансы деловой звукозаписи в помещениях, расположенных на "своей" территории, устанавливая в них один или несколько выносных микрофонов, а магнитофон - в соседнем помещении (лучше стереофонический, профессионального типа, например, Uher 4400, Marantz PMD430 или минидисковые магнитофоны). Это позволит обеспечить возможность контроля качества записываемой информации со стороны помощника оператора, а в случае необходимости, и корректировки уровня записи, оптимального подключения микрофонов и своевременной замены кассет.

3.3. Средства обеспечения скрытности оперативной звукозаписи

Аппаратура звукозаписи

Все диктофоны можно разделить на две группы: диктофоны с широкой полосой записываемых частот (до 15Кгц, чаще всего стационарные) и с полосой до 4-6Кгц, чаще портативные.

Модели *первой группы* предназначены для профессиональной высококачественной записи и используются в случаях, когда важно хорошее качество записи.

Диктофоны *второй группы* представлены шире. Они способны записывать человеческий голос достаточно четко, отсекая при этом посторонние шумы за счет использования более узкой полосы частот. Однако при этом узнаваемость голоса, записанного на такой диктофон, естественно, хуже, чем у профессиональных моделей с широкой полосой частот.

Из второй группы можно выделить по меньшей мере еще четыре подгруппы по типу носителя информации.

- Первая подгруппа образована аппаратами, у которых для записи используются стандартные компакт-кассеты. Благодаря широкому распространению, которое получили подобные кассеты, записи, сделанные на них, можно слушать как на привычном всем аудиоплейере, так и на обыкновенной магнитоле.
- Фирмой Olympus был введен стандарт микрокассет. Диктофоны, использующие такие кассеты, как правило, меньше компакт-кассетных. Почти во всех микрокассетных устройствах существует возможность переключения скорости движения ленты на вдвое меньшую, что позволяет на обыкновенную 90-минутную кассету записать до 3 часов разговора (правда, с не-

большой потерей качества за счет сужения полосы записываемых частот). Записи, сделанные на микрокассетном диктофоне, придется слушать либо на нем самом, либо на микрокассетном же автоответчике.

- Принципиально другим видом устройств являются диктофоны с цифровой записью на микросхему памяти. Микросхемы бывают встроенные (как, например, у диктофонов Sony серии ICD) и сменные (как мини-карты в цифровом диктофоне Olympus). Максимальное время записи *в* таких устройствах уже сравнимо (а некоторых моделях и выше) с кассетными диктофонами, возможности сопряжения с компьютером их память можно освобождать, переписывая часть сообщений на жесткий диск. Благодаря тому, что сообщения в цифровом виде хранятся на чипе, доступ к ним происходит почти мгновенно, да и операции по редактированию существенно облегчаются. Но цена на такие диктофоны пока выше, чем у кассетных и качество записи несколько ниже.
- Необходимо упомянуть магнитофоны которые используют цифровую запись звука на оптический диск (minidisk) или специальную кассету (DAT). Такие магнитофоны отличаются высоким качеством записи сопоставимым со студийной записью на стационарных магнитофонах.

Как правило, звукозаписывающая аппаратура представляет собой функционально законченные устройства, т.е. на них можно выполнять полный цикл магнитной звукозаписи: запись акустической информации, воспроизведение и стирание фонограмм, ускоренную перемотку магнитной ленты и т.д.

Критерии выбора диктофона

Критерии, определяющие выбор той или другой модели диктофона:

1. Малые габариты и вес.
2. Бесшумность работы лентопротяжного механизма.
3. Широкий диапазон записываемых частот.
4. Большой динамический диапазон записываемого сигнала.
5. Возможность записи как от встроенного, так и от выносного микрофонов.
6. Дистанционное управление включением и выключением лентопротяжного механизма.
7. Отсутствие в процессе работы демаскирующих факторов, например, щелчка при возврате клавиш управления в исходное состояние по окончании пленки на кассете или подачи звукового сигнала за 1-2 мин. до окончания времени записи.
8. Возможность ступенчатого или плавного изменения чувствительности микрофона.
9. Наличие не менее двух скоростей движения ленты на микрокассете.

10. Возможность работы на кассетах с тонким звуконосителем.
11. Наличие механического или электронного счетчика движения ленты.
12. Наличие режима автореверса.
13. Наличие светодиодного (LED) или жидкокристаллического (LCD) индикатора записи.
14. Наличие гнезда внешнего питания магнитофона.
15. Возможность контроля записи или прослушивания записанной фонограммы через наушники.
16. Широкий температурный диапазон эксплуатации.

Помимо обязательных или желательных функций, которыми должны обладать микрокассетные магнитофоны для деловой звукозаписи, удобными, но необязательными могут быть и такие функции, как возможность включения магнитофона с помощью часового автопуска (таймера), возможность записи на фонограмму специальных акустических меток (Cue mark, Index), по которым затем легко можно найти нужный участок фонограмм.

Наиболее полно удовлетворяют этим требованиям диктофоны, выпускаемые японскими фирмами NATIONAL, SONY, OLYMPUS, AIWA.

При подборе магнитофона для осуществления деловых записей в тех случаях, когда в помещении, где происходит беседа устанавливается только микрофон, а сам магнитофон находится в другом помещении, следует обращать внимание на наличие у него следующих основных функций:
1. Возможность работы как от электросети, так и от автономных элементов питания.
2. Возможность контроля записи через так называемый "сквозной канал".
3. Возможность автоматической и ручной регулировки уровня записи.
4. Наличие стрелочного и т.п. индикатора уровня записи, а также счетчика движения ленты.
5. Широкий диапазон записываемых частот.
6. Большой динамический диапазон записываемого сигнала.
7. Наличие двух и более скоростей записи.
8. Возможность прослушивания записанной фонограммы через наушники.

Из числа имеющихся на рынке подобных магнитофонов предпочтение следует отдавать портативным профессиональным кассетным и ленточным магнитофонам фирм UHER, MARANTZ, SONY. При этом более качественная запись получается при использовании стереофонических магнитофонов, т.к. стереозапись позволяет значительно повысить разборчивость фонограмм при осуществлении деловой звукозаписи в гулких помещениях, к которым, как правило, относится большинство служебных кабинетов.

Типы портативных диктофонов

В зависимости от используемой модели диктофон может иметь встроенный или выносной микрофон.

Встроенный микрофон существенно уступает выносному микрофону по техническим характеристикам. Кроме того, он имеет меньшие возможности по скрытому применению. Поэтому на практике чаще используют выносные акустические приемники.

Выносной микрофон может быть закамуфлирован под любой элемент личных вещей. Часто он изготавливается в виде пуговицы и вставляется в петлицу на одежде. А так как пуговицы взаимозаменяемые, то достаточно просто провести общую маскировку из предлагаемого ассортимента. Например, стандартный вариант – белая пуговица на светлой рубашке.

Широко применяются и выносные микрофоны в виде колпачка от авторучки, заколки для галстука и других предметов (как правило, они не вызывают никаких подозрений).

Более простые устройства не имеют штатного камуфляжа, а благодаря своим небольшим размерам прячутся под одежду или в различных предметах (книге, папке, портфеле). В зависимости от типа используемого диктофона и расстояния от источника звука микрофоны могут оборудоваться дополнительным усилителем. Как правило, это делается в том случае, если микрофон устанавливается на значительном расстоянии от диктофона.

Необходимо упомянуть о миниатюрных диктофонах, которые используются для скрытной записи. Наиболее часто в интересах промышленного шпионажа применяются диктофоны типа NATIONAL-RNZ-36, OLYMPUS-L400, SONY-909M, SONY-950. Некоторые устройства не имеют внутреннего динамика, поэтому прослушивание записи в них приходится осуществлять через внешний акустический блок или наушники.

Микрокассета МС-90 позволяет обеспечивать до 6 часов непрерывной записи. Некоторые диктофоны снабжены беззвучным автостопом, большинство – системой VOX (автоматического включения записи при появлении источника акустического сигнала – акустомат), выносным микрофоном и системой дистанционного включения/выключения. Стоимость подобных изделий составляет от $200 до $500.

Иногда для несанкционированной записи используются и такие простые изделия, как OLIMPUS-S928 или SONY-359, цена которых составляет от $35 до $100. Правда, и качество записи у этих моделей похуже, к тому же изделия такого класса часто не имеют гнезда для подключения выносного микрофона.

В ряде случаев используют и магнитофоны, имеющие увеличенные по сравнению с описанными выше диктофонами габариты. Они, как правило,

соответствующим образом маскируются или используются для дистанционной записи, а фиксация информации в них осуществляется на стандартную кассету, как, например, в диктофонах РК660 и РК670. Некоторые устройства имеют автореверс и пониженную скорость протяжки, что позволяет обеспечивать длительное время записи, особенно на кассеты типа С-120 (естественно, за счет ухудшения качества записи). Основное достоинство в использовании стандартных кассет – это возможность прослушивания на обычной бытовой аппаратуре. Стандартным вариантом камуфляжа для РК660 и РК670 является книга со специальным вырезом для акустического сигнала.

Все основные типы портативных диктофонов, используемых в интересах промышленного шпионажа, отвечают, как правило, следующим требованиям к техническим характеристикам: диапазон частот – от 200-300 Гц до 3-5 кГц, коэффициент детонации (коэффициент колебания скорости ленты) – до 4 %, остаточный уровень шумов – 30 дБ, коэффициент гармоник – до 10 %, разборчивость слогов – 60-80 % при доверительной вероятности не хуже 0,9.

Внешний вид некоторых марок широко известных малогабаритных кассетных диктофонов приведен на рис. 50-52.

Однако закамуфлированное размещение выносного микрофона и самого диктофона не исчерпывает проблем скрытой звукозаписи, поэтому важно знать, с какими проблемами сталкиваются ваши конкуренты и как они их могут решить:

- Некоторые диктофоны имеют неприятные особенности управления – выключаться с характерным щелчком выстреливаемых кнопок или после окончания кассеты включать обратную перемотку, что также может вылиться в нежелательные последствия. Бывают экземпляры с программируемым управлением и таймером, автоматически включающиеся на воспроизведение в самый неподходящий момент (поэтому если во время разговора у вашего собеседника в кармане, что-то щелкнуло, то будьте готовы к тому, что вся предыдущая беседа уже на пленке).
- Другой важной проблемой является емкость записи. Поэтому человек, осуществляющий скрытую аудиозапись, вынужден постоянно следить за временем беседы для того, чтобы не выйти за кассетное время. Это иногда весьма неудобно. Для увеличения времени записи в некоторых диктофонах, как отмечалось выше, используется пониженная скорость лентопротяжного механизма (меньше 1,2 см/с), но качество записи при этом, как уже отмечалось, существенно ухудшается и иногда даже становится проблематично идентифицировать разговор.
- Низкое качество звукозаписи в силу различных ранее упомянутых причин (акустические помехи и т. п.).

Рис. 50. OLYMPUS-L250

Рис. 51. OLYMPUS-L400, 73×52×20

Рис. 52. OLYMPUS-S950, 120×58×24

Для того чтобы избежать неприятностей *с обнаружением факта негласной звукозаписи* из-за щелчков и переключений в диктофоне, в первую очередь идут по пути использования профессиональных средств, специально предназначенных для скрытой аудиозаписи. К ним относятся, например, диктофоны типа UHER CR-1600, UHER CR-1601, MARANTZ PMD-201, MARANTZ PMD-221. Их основные характеристики приведены в табл. 8. Главный недостаток – очень высокая цена, которая может достигать нескольких тысяч долларов.

Таблица 8.

Технические характеристики	UHER CR-1600	UHER CR-1601	MARANTZ PMD-201	MARANTZ PMD-221
Скорость движения ленты, см/с	4,7; 1,2	4,7; 2,4; 1,2	4,7; 2,4	4,7; 2,4
Диапазон раб. частот, Гц:				

- для скорости 4,7 см/с	300-16000	300-16000	40-14000	40-15000
- для скорости 2,4 см/с			40-8000	40-8500
- для скорости 1,2 см/с	600-3400	600-3400		
Отношение сигнал/шум	70	70	57	57
Длительность перемотки, с	90	90	1	
Количество головок, шт.	2	3	2	3
Режим работы	стерео	моно		
Габаритные размеры, мм			228×51×165	228×51×165
Масса, кг			1,3	1,3

Другой путь – использование магнитофонов с электронной записью звука. Например, диктофон Edic способен непрерывно вести фиксацию акустических сигналов в течении 1-2 суток, сохраняя последние 20–40 мин записи. Диктофон незаменим для звуковой регистрации неожиданных ситуаций, так как нет необходимости нажимать кнопку «Пуск» при внезапном интересе к какой–либо информации, она автоматически запишется и будет храниться до 40 мин пока не «затрется» новой записью. Единственное неудобство для оператора – надо не забыть нажать на «Стоп» после окончания интересующего разговора. Небольшие габаритные размеры (105×55×14 мм) позволяют легко камуфлировать диктофон. В нем нет движущихся частей, поэтому его применение сложно обнаружить. Комплектуется выносным микрофоном и зарядным устройством для встроенных аккумуляторов.

Более современными вариантами являются малогабаритные цифровые стереофонические диктофоны NT-1 и NT-2 фирмы SONY. Главное достоинство данных устройств – наличие специальных бесшумных кнопок и высокое качество записи. Дополнительные возможности создает встроенный календарь и часы, автоматически регистрирующие и сохраняющие время начала и конца записи.

Для увеличения времени непрерывной записи используют реверсивные системы. Однако и здесь не каждая модель может быть использована, так как при переключении записи на реверс некоторые диктофоны (а их, к сожалению, большинство) издают довольно громкий щелчок, о чем говорилось выше.

Иногда для экономии ресурсов используют функцию включения по голосу – акустомат. Но здесь, как и у закладного устройства, «съедается» начало первой фразы. Если порог срабатывания выставлен некорректно, то возможен пропуск целых предложений.

Для экономии рабочего тела (пленки) в ряде случаев используется система дистанционного включения. В простейшем случае она представляет со-

бой переключатель, соединенный проводом с соответствующим разъемом на диктофоне, а при отсутствии специального разъема используется доработанный вход по питанию. Система внешнего включения должна содержать переключатель с четкой фиксацией положения, чтобы в стрессовых ситуациях оператор был уверен, что его диктофон действительно работает. Иногда используют специальные системы включения, например, в виде зажима для авторучки. В случае, когда авторучка находится в зажиме, расположенном во внутреннем кармане, диктофон выключен, а когда она извлечена – производится запись.

Некоторого преимущества при использовании диктофонов позволяет достичь применение дистанционного включения по радиоканалу. Данная техника предназначена для применения устройств аудиозаписи в качестве закладки. Запуск диктофона производится специальной командой, передаваемой радиопередатчиком. Например, устройство дистанционного управления РК1670 имеет передатчик мощностью 1 Вт и дальность действия 500 м. Габариты приемника команд – 25×58×18 мм, вес – всего 55 г. Подключается приемник к соответствующему разъему магнитофона.

Существенно увеличить время непрерывной звукозаписи позволяет использование диктофонов с записью на жесткий проволочный носитель, изготовленный из специальных сплавов. Их память может простираться на сутки и более. Однако в будущем они, видимо, не найдут широкого применения для вышеуказанных целей. Это связано в первую очередь с такими недостатками, как трудность соединения проволоки при монтаже и обрывах, появление паразитной амплитудной модуляции сигнала из-за скручивания носителя, неудовлетворительная передача верхних частот, довольно высокая стоимость, сильный износ головок.

Перспективным по-прежнему остается применение цифровых диктофонов. Тем более, в последнее время появились диктофоны нового типа – с записью в память персональной ЭВМ.

Например, цифровая система регистрации переговоров «Аудиокод». Данная система предназначена для записи информации, ее сжатия (компрессии), хранения с автоматическим удалением устаревших материалов и прослушивания информации. Область фиксируемых звуковых частот канала «запись-воспроизведение» лежит в диапазоне 300-3000 Гц. Система защищена от несанкционированного доступа. Обеспечивается одновременная регистрация переговоров по 4 каналам с автоматической или ручной регулировкой уровня записи в каждом канале, реализована функция «эхо» (прослушивание записываемых каналов). Включение записи осуществляется по уровню входного сигнала или после нажатия клавиши. Кроме того, в диктофоне предусмотрен мгновенный доступ к любой записи базы данных, быст-

рый поиск по номеру канала и времени регистрации, прослушивание любой записи без прерывания процесса регистрации, воспроизведение с любого места, быстрый переход к любому участку фонограммы.

Для обеспечения цифровой записи в различных марках диктофонов используются различные форматы записи. К наиболее известным относятся следующие.

DAT (Digital Audio Tape) – формат цифровой магнитной записи звука на специальную DAT-кассету, время непрерывной работы которой достигает двух часов, а в режиме Long Play (LP) – четырех часов. Запись ведется вращающимися головками, как в видеомагнитофонах, а магнитная лента движется со скоростью всего 8,15 мм/с.

Исходный аналоговый сигнал преобразуется в цифровую форму и без сжатия записывается на ленту. Запись, сделанная на DAT-магнитофоне, отличается малым уровнем шумов, большим частотным и динамическим диапазоном, что обеспечивает высокое качество звука, зачастую превосходящее качество компакт-диска. Однако широкому распространению этих аппаратов помешала их высокая цена. Поэтому DAT-магнитофоны нашли применение только в профессиональной звукозаписи: на них, например, записывают мастер-ленты для изготовления компакт-дисков. Некоторые фирмы сейчас выпускают портативные DAT-магнитофоны, которые можно использовать в качестве диктофонов для получения высококачественной записи речи. Причем полоса записываемых частот настолько широка, что позволяет делать записи в режиме LP без заметного снижения качества звучания, а продолжительность записи при этом увеличивается вдвое. Кроме высокой стоимости самого аппарата и DAT-кассет, к недостаткам DAT-магнитофонов относится сравнительно быстрый износ механизма протяжки из-за высоких требований к нему по скорости перемотки и поиску интересующих фрагментов. Цена бытовых аппаратов – $700 и выше. Основные производители DAT-магнитофонов – Pioneer, Sony, Tascam.

DCC (Digital Compact Cassette) – цифровая компакт-кассета (изобретение фирмы Philips), выпущенная на рынок в 1992 году. Основным достоинством DCC-системы является полная совместимость с обычными компакт-кассетами. Цифровая звукозапись ведется с помощью стационарной многодорожечной головки при стандартной скорости протяжки ленты, при этом исходный звуковой сигнал подвергается многократному сжатию с помощью адаптивного алгоритма, учитывающего психологические особенности восприятия звука человеком. Стоимость первых образцов DCC-магнитофонов также оказалась высокой, а качество звука довольно низким, и это решило их судьбу – они не нашли широкого применения. Качество звучания впоследствии удалось существенно улучшить, однако доверие к новой системе было

подорвано. Сейчас фирма Philips производит DCC-магнитофоны, в том числе и портативные, которые можно приобрести в магазинах по цене от $700. Несомненный интерес представляет возможность воспроизводить на этих аппаратах записи, сделанные на компакт-кассетах обычным способом. Однако ограниченное распространение этого формата затрудняет его внедрение в практику.

MD (Mini Disc) – мини-диск – разработан фирмой Sony. Конструктивно он напоминает 3,5-дюймовую компьютерную дискету диаметром 64 мм. Материал, из которого изготовлен диск, меняет свои оптические свойства под воздействием магнитного поля. Запись на мини-диск осуществляется магнитной головкой, при этом поверхность диска в зоне действия магнитного поля разогревается лучом лазера. Считывание информации происходит также с помощью лазера, но меньшей мощности. Таким образом, информация сохраняется на диске даже в случае воздействия сильных магнитных полей и появляется возможность многократной (до 1 млн раз) перезаписи. На мини-диск можно записать стереозвук продолжительностью до 74 мин, а некоторые модели мини-дисковых аппаратов позволяют вести монофоническую запись в течение 148 мин.

Разработчиками формата применен адаптивный алгоритм сжатия и кодирования информации – ATRAC (подобный используемому в DCC-магнитофонах). Благодаря его постоянному совершенствованию качество звука приближается к уровню качества записи на компакт-диске. Минидисковая аппаратура успешно применяется в студиях звукозаписи, на радио, в любительской звукозаписи. Некоторые фирмы выпускают малогабаритные мини-дисковые плееры с возможностью записи. Их стоимость находится в пределах $350–$450. Производители – Sony, Pioneer, Kenwood, Denon, Aiwa.

CD-R, CD-RW– записываемый компакт-диск. Первый CD-рекодер был разработан фирмой Pioneer в 1996 году. В нем был применен записываемый компакт-диск с возможностью однократной записи (CD-R). Существует несколько технологий однократной записи цифровых данных на компакт-диск. Одна из них использует эффект химических превращений в органическом красителе под действием лазерного луча. По другой технологии луч сравнительно мощного лазера просто «прожигает» отверстия в тончайшем слое металла. Совсем недавно фирмой Philips и некоторыми другими были разработаны и выпущены в продажу CD-рекодеры с возможностью многократной перезаписи на компакт-диск (CD-RW). Продолжительность записи на эти диски обычно не превышает 74 мин. В продаже представлены CD-R и CD-RW рекодеры в стационарном исполнении, так как они в основном предназначены для копирования компакт–дисков, и записывающие CD-ROM для компьютеров. Поэтому этот формат представляет интерес в тех случаях, ко-

гда уже имеется соответствующее оборудование для воспроизведения компакт–дисков или CD-ROM.

NT (Non Tracking) – «бездорожечный» принцип записи на специальную микрокассету – разработан и реализован фирмой Sony в диктофонах NT-1 и NT-2. В них запись производится вращающимися со скоростью 3000 об./мин головками на ленту шириной 2,5 мм, которая движется со скоростью 6,35 мм/с. Это обеспечивает запись стереозвука в диапазоне 10-14 000 Гц при соотношении «сигнал/шум» 80 дБ. Цифровой звуковой сигнал записывается без сжатия. Продолжительность записи составляет 60, 90 и 120 минут в зависимости от типа микрокассеты. Диктофон весит 147 г, имеет габариты 113×23×55 мм. К недостаткам диктофонов следует отнести их высокую стоимость (порядка $2000)

Для улучшения разборчивости речи, полученной в результате скрытой звукозаписи, используют различные «очищающие» фильтры. Они особенно эффективны, если фиксация информации осуществлялась на фоне мощных, но сосредоточенных по спектру помех или специфически «окрашенных» шумов.

В простейшем случае можно использовать широко известные эквалайзеры. Однако часто этот прием не помогает, поэтому применяют специально разработанные устройства.

Более совершенными являются специальные программно-аппаратные комплексы очистки речи, например **«Золушка-97»**. Это двухканальное цифровое устройство шумоочистки речевых сигналов. Оно предназначено:

- для очистки «живого» звука и звукозаписей;
- для повышения разборчивости и качества речи в условиях низкого качества каналов связи;
- для выделения источника звука в условиях «шумного» производства.

При его применении обеспечивается обработка сигналов с изменяющимися во времени характеристиками шумов, одновременное устранение нескольких типов помех, использование свойств восприятия (психоакустики) при расшифровке текста и некоторые другие возможности.

3.4. Цифровые диктофоны

Большой интерес представляют цифровые диктофоны **EDIC-mini** с экстремальными характеристиками (самые маленькие в мире размеры, самое большое время записи, самое большое время непрерывной работы), с записью звука на энергонезависимый твердотелый носитель (FLASH-память). Диктофон имеет встроенный микрофон и возможность подключения наушников. Предусматривается передача накопленной информации в компьютер

по последовательному каналу. Этот диктофон представлен моделями A, B, B1, B2, B3, B4, C.

A – Пластмассовый корпус, размер 56×17×9 мм, время записи - до 2240 мин, время непрерывной работы -до 5 часов, часовая батарея Button Cell тип 357, FLASH-память до 2 Гбит.

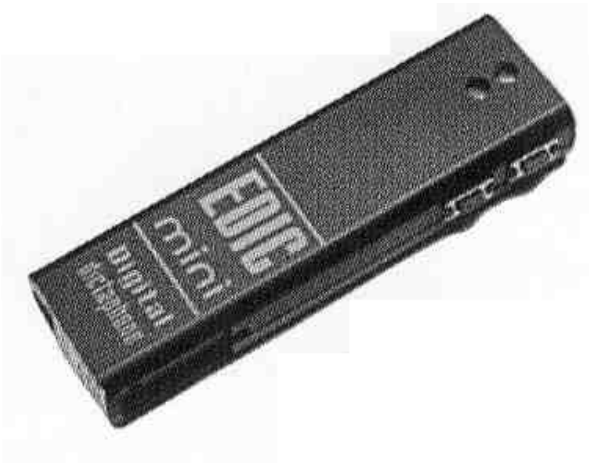

Рис. 53. Диктофон EDIC-mini, модель A

B – Металлический корпус (57×28×9 мм), время записи - до 2240 мин, время непрерывной работы - до 60 часов, литиевая батарея, FLASH-память до 2 Гбит.

Рис. 54. Диктофон EDIC-mini, модель B

B1 – Модификация модели B в оригинальном круглом металлическом корпусе (d29×h14 мм), время записи - до 2240 мин, время непрерывной работы - до 60 часов, литиевая батарея, FLASH-память до 2 Гбит.

Рис. 55. Диктофон EDIC-mini, модель B1

B2 – Самое большое время работы от батареек: 200 часов, цилиндрический корпус из металла (d18×h55 мм), время записи - до 2240 мин (38 часов), литиевая батарейка, FLASH-память до 2 Гбит.

Рис. 56. Диктофон EDIC-mini, модель B2

B3 – Пластмассовый корпус (35×31×12мм), время записи - до 2240 мин, время непрерывной работы от одной зарядки аккумулятора - до 15 часов, литий-ионный аккумулятор, FLASH-память до 2 Гбит.

B4 – Самый маленький размер этого диктофона: 40×25×8 мм, время записи - до 2240 мин (38 часов), время непрерывной работы от одной зарядки аккумулятора - 8 часов, литий-ионный аккумулятор, FLASH-память до 2 Гбит.

Рис. 57. Диктофон EDIC-mini, модель B4

C – Самое большое время записи - до 17920 мин (300 часов), прямоугольный металлический корпус (57×27×12мм), время непрерывной работы от одной батарейки - до 60 часов, литиевая батарея, FLASH-память до 16 Гбит.

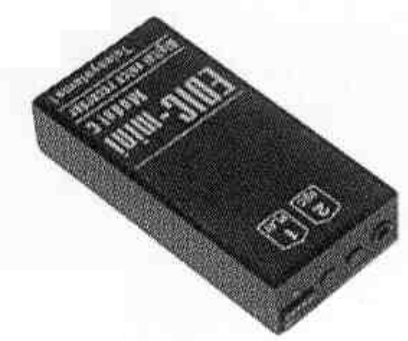

Рис. 58. Диктофон EDIC-mini, модель C

В комплект поставки цифрового диктофона EDIC-mini входят:

- **Адаптер записи телефонных переговоров.** Позволяет записывать телефонные переговоры по сигналу поднятия трубки телефона (рис. 59).

Рис. 59. Адаптер записи телефонных переговоров для диктофона EDIC-mini

- **Регистратор телефонных переговоров.** Позволяет регистрировать входящую и исходящую связь (определение номера звонящего абонента в российском и зарубежных стандартах, определение исходящего номера (в импульсе и DTMF), времени и даты разговора), производить запись телефонных переговоров (см. рис. 60).

Рис. 60. Регистратор телефонных переговоров для диктофона EDIC-mini

- **Выносной микрофон и усиливающий (+10dB) выносной микрофон.**
- **Пульт дистанционного управления.** Предназначен для дистанционного управления цифровыми диктофонами EDIC-mini. Можно использовать совместно с цифровыми диктофонами EDIC-mini (см. рис. 61).

Рис. 61. Пульт дистанционного управления для диктофона EDIC-mini

3.5. Обнаружители диктофонов

Выше отмечалось, что диктофон может быть использован как в качестве закладного подслушивающего устройства, так и для негласной записи доверительных бесед какой-либо из заинтересованных сторон. В одном случае его тайно устанавливают в контролируемом помещении и только периодически меняют кассеты, в другом – прячут в личных вещах или под одеждой. Данный прибор прост и надежен и в силу этого обстоятельства пользуется большой популярностью, но, к сожалению, не только у честных бизнесменов, которые без всяких черных намерений любят на досуге проанализировать ход переговоров. Поэтому задача защиты от несанкционированной аудиозаписи является достаточно актуальной.

Существуют два основных направления ее решения:

- это предотвращение проноса звукозаписывающих устройств в контролируемые помещения;
- фиксация факта применения диктофона и принятие адекватных мер.

Предотвращение проноса звукозаписывающих устройств

Этот способ может быть реализован только при наличии достаточно мощной службы безопасности и весьма солидных финансовых средств. Так, в соответствии с применяемыми в устройствах обнаружения физическими принципами можно выделить следующие виды аппаратуры, способные решать эти задачи: металлодетекторы; нелинейные радиолокаторы; устройства рентгеноскопии; специальные детекторы диктофонов.

Металлодетекторы могут применяться на входах в помещение или при наружном досмотре лиц и носимых ими предметов (кейсов, сумок и т. п.). Эти приборы бывают двух видов: стационарные и переносные. Переносные портативные приборы достаточно подробно будут описаны ниже в главе 9. Стационарные арочные металлообнаружители (см. рис. 62), как правило, имеют следующие основные характеристики:

- высота – 2000 мм;
- ширина – 800 мм;
- глубина – 500 мм;
- скорость прохода – до 1 м/с;
- питание от сети однофазного тока напряжением 220 В.

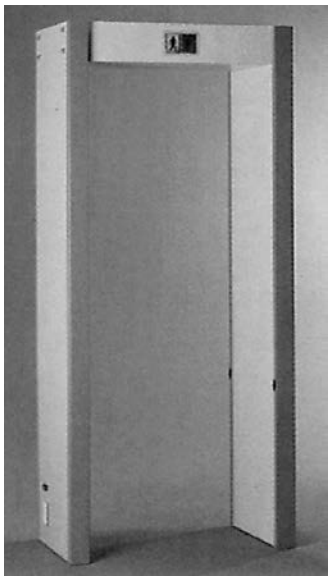

Рис. 62. Арочный металлодетектор

Вследствие ограниченной чувствительности металлодетекторов надежность обнаружения таких мелких объектов, как современные микрокассетные диктофоны, в большинстве случаев оказывается недостаточной, особенно когда нежелательно или просто невозможно проведение открытого досмотра. Таким образом, металлодетекторы можно рассматривать только как вспомогательное средство в комплексе с другими более эффективными мероприятиями по обнаружению и подавлению средств звукозаписи. На рис. 63 приведена примерная схема организации поста контроля для ведения проверки в негласном режиме.

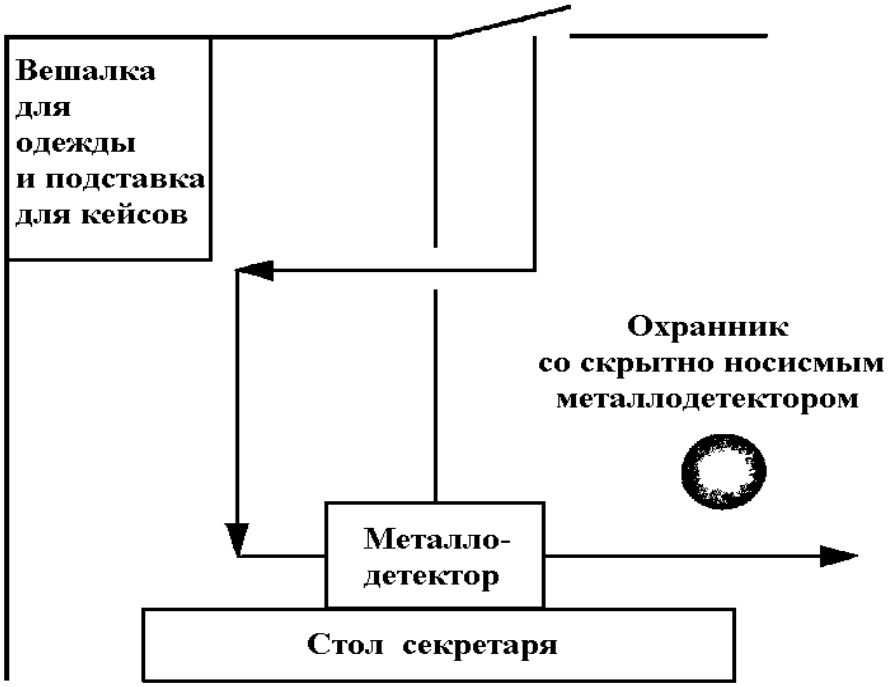

Рис. 63. Схема поста контроля

На постах такого типа аппаратура контроля камуфлируется под предметы интерьера. Главной трудностью является обеспечение строго заданного маршрута движения посетителей. Тип ручной клади при контролируемом человеке тоже должен быть ограничен визиткой, дамской сумочкой, папкой для бумаг и т. д. В качестве дополнения к стационарному металлодетектору часто используются портативные металлоискатели, скрытно размещенные под одеждой персонала поста контроля.

Нелинейные радиолокаторы способны обнаруживать диктофоны на значительно больших расстояниях, чем металлодетекторы, и в принципе могут использоваться для контроля за проносом устройств звукозаписи на входах в помещения. Однако при этом возникают такие проблемы, как уровень безопасного излучения, идентификация отклика, наличие «мертвых» зон, совместимость с окружающими системами и электронной техникой.

В настоящее время наиболее полное практическое решение проблем обнаружения скрытно проносимых диктофонов методом нелинейной локации обеспечивает система **G-1400**. Имеется также модификация данной системы (**G-1500**), которая размещается в боковых панелях стандартного арочного металлодетектора.

Системы **G-1400** и **G-1500** легко обнаруживают даже одиночный точечный диод в створе между передающей и приемной антеннами шириной 130 см. При этом энергетическая СВЧ-нагрузка в 2000 раз меньше предельной безопасной нормы, допускаемой согласно ГОСТ 12.1.006–84, то есть совершенно безвредна как для обследуемых лиц, так и для персонала службы безопасности. Конфигурация и состав системы обеспечивают сплошную ВЧ-завесу по всей площади поперечного сечения прохода. Требуемая эффективность и надежность работы достигаются за счет совместного использования с металлодетектором, а также в результате обучающего тестирования оператора и настройкой с полным учетом местных условий.

Устройства рентгеноскопии позволяют надежно выявить наличие диктофонов, но только в проносимых предметах. Очевидно, что область применения этих средств контроля крайне ограничена, так как они практически не могут использоваться для целей личного досмотра и скрытого контроля (см. рис. 64, 65).

Рис. 64. Рентгеновская установка MINISCAN

Рис. 65. Рентгеновская установка LINESCAN-112

Стационарный рентгеноскоп имеет следующие характеристики:

- максимальные габаритные размеры просматриваемой ручной клади – 500×400×350 мм;
- питание от сети однофазного тока напряжением 220 В;

- потребляемая мощность 1500 Вт.

Необходимость и возможность их использования следует рассматривать в контексте конкретных задач и существующих местных условий. Вместе с тем, стоит отметить, что, вопреки расхожему негативному мнению, современные образцы рентгеновской техники создают минимальные дозовые нагрузки на обследуемый объект, не влияющие даже на кинофотоматериалы. Для лучших образцов этой техники доза – менее 100 микрорентген за одно обследование.

Фиксация факта применения диктофона

Для определения наличия работающих диктофонов используют специальные устройства. Различают два принципа работы таких устройств, основанных на эффекте обнаружения акустических сигналов и выявлении побочных электромагнитных излучений (ПЭМИ).

Характерный шум лентопротяжного механизма и щелчки при нажатии на кнопки – обычные явления для кассетных магнитофонов 70–80-х годов. Поэтому для маскировки их работы применяли специальные приемы, от помещения приборов рядом с источниками звука (типа часов) до перебора во время беседы четок, чтобы замаскировать стуком костяшек щелчки диктофона. Сейчас у подавляющего количества современных приборов выявить акустический сигнал от лентопротяжного механизма при обычном фоне в помещении и других помех практически невозможно. А цифровые диктофоны – вообще абсолютно бесшумны. Таким образом, регистрация побочных электромагнитных излучений сейчас является единственно возможным способом выявления работающих диктофонов.

Как правило, работа многих обнаружителей диктофонов (особенно портативных) основана на принципе выявления излучений от *генератора стирания – подмагничивания* (ГСП). Однако при работе таких обнаружителей возникают следующие проблемы:

- Используемый частотный диапазон характеризуется большим количеством источников мощных магнитных полей (телевизоры, контактная сеть городского транспорта, лампы дневного света, электродвигатели бытовых приборов и т. д.), которые буквально «глушат» излучения диктофонов гораздо эффективнее, чем во времена оные глушили «забугорные» радиостанции;
- Многие из современных диктофонов иностранного производства вообще не имеют ГСП. Стирание обеспечивается постоянным магнитом, а подмагничивание – так называемой «постоянной составляющей».

Следовательно, для обнаружения самых современных средств звукозаписи данные устройства практически непригодны.

Теоретически возможно осуществить обнаружение побочных излучений, возникающих в результате самовозбуждения электронного устройства из-за паразитных связей в генераторных и усилительных каскадах, например, микрофонного усилителя. Однако измерения показывают, что дальность возможной регистрации ПЭМИ такого рода (в диапазоне 20 кГц-50 Мгц) не превышает нескольких сантиметров для бытовых средств звукозаписи, а от специальных устройств с металлическим корпусом вообще не регистрируются даже высокочувствительными лабораторными приборами.

Существуют устройства, которые реагируют на переменное магнитное поле, возникающее при работе электродвигателей. В лаборатории они работают очень четко, но на практике главной трудностью их реализации является наличие большого числа источников низкочастотных магнитных полей, разнообразие спектральных портретов излучений диктофонов разных типов, низкие уровни сигналов. Правда, металлические корпуса диктофонов уже не являются препятствием для обнаружения полей данного типа.

В результате анализа этой можно сделать вывод об объективной сложности создания по-настоящему надежной аппаратуры выявления работающей звукозаписывающей техники. И, тем не менее, попытки создать подобные устройства не прекращаются, а ряд моделей даже имеется в продаже. В общем виде данная аппаратура включает в себя следующие блоки:

- Низкочастотную магнитную антенну, выполненную конструктивно как отдельный элемент и выносимую как можно ближе к предполагаемому месторасположению диктофона;
- Детекторный блок, выполняющий операцию обнаружения ПЭМИ, с регулируемым порогом срабатывания;
- Фильтры, ограничивающие полосу частот, в которых осуществляется контроль; иногда добавляют и режекторные (то есть «закрывающие» определенные диапазоны) фильтры, настроенные на частоты наиболее мощных источников местных помех (как правило, они конструктивно выполнены в детекторном блоке);
- Устройства световой (шкала светодиодов, стрелочный индикатор, контрольная лампочка) и звуковой (вибрационной) индикации наличия ПЭМИ (конструктивно выполняются или в детекторном блоке, или выносятся на специальный пульт);
- Блок питания.

Рассмотрим некоторые примеры практической реализации данных средств.

На первый взгляд, наилучший вариант представляет собой изделие **РК 645-SS**, реализующее первое направление борьбы с диктофонами. Плоские магнитные антенны размещаются по периметру двери. Дальность обнаруже-

ния стандартного звукозаписывающего прибора – до 1 м. Однако, существенный недостаток – полная невозможность обнаружения выключенных диктофонов, то есть если человек входит в кабинет (здание) с неработающим диктофоном, а только затем его включает, то система его не зафиксирует. Следовательно, такое устройство необходимо дополнять другими: арочным металлоискателем и нелинейным локатором, а это уже очень и очень дорогое удовольствие.

Интересной отечественной разработкой является обнаружитель диктофонов **PTRD-018** (Portable tape recorder detector). Он предназначен для скрытного обнаружения работающих магнитных звукозаписывающих устройств. Прибор состоит из блока регистрации и 4 (8 или 16) датчиков, которые устанавливаются стационарно (например, в стол, за которым ведутся наиболее важные переговоры, или в подлокотники кресла клиента). Внешний вид комплекса приведен на рис. 66.

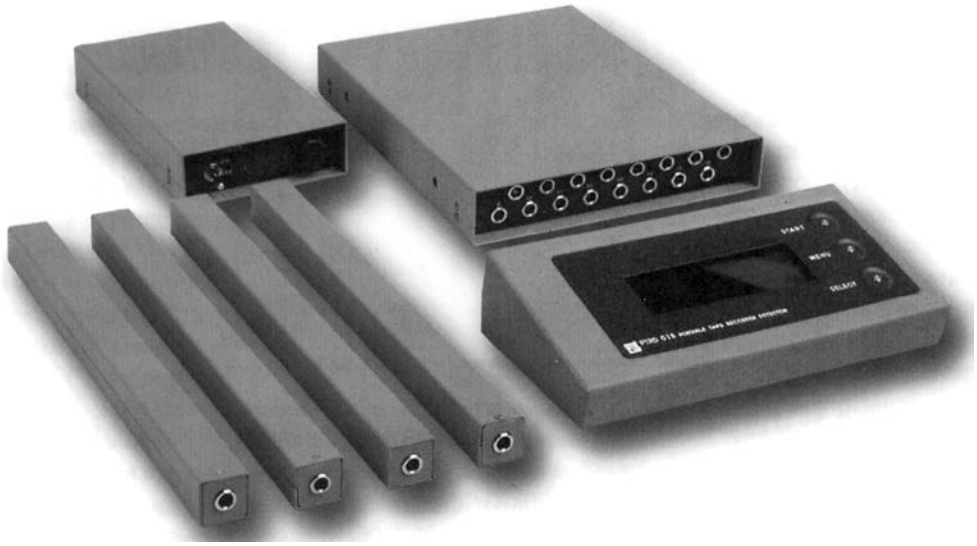

Рис. 66. Устройство обнаружения диктофонов PTRD-018

Используемым признаком, по которому обнаруживается диктофон, служит электромагнитное поле, создаваемое работающим электродвигателем лентопротяжного механизма. Отметим, что спектр этого электромагнитного поля лежит в диапазоне очень низких частот, и вследствие этого даже металлические корпуса «фирменных» приборов для скрытой звукозаписи не защищают их от обнаружения данным устройством.

Основным препятствием к обнаружению сигнала устройствами подобного типа является электромагнитное поле промышленных помех, как на основных частотах, так и на их гармониках (вплоть до 9-й), что существенно ограничивает применение таких приборов. Кроме того, выявление факта

применения цифровых диктофонов оказывается принципиально невозможным.

Существуют и портативные варианты обнаружителей работающих диктофонов, которыми можно пользоваться и за пределами офиса. В качестве примера может служить изделие **TRD 009V** фирмы CCS. Размеры устройства позволяют легко разместить его в кармане. Сигнал тревоги – легкая вибрация корпуса. При этом, чем вы ближе к диктофону, тем сильнее вибрация.

Однако следует учесть тот факт, что на практике подобные портативные системы малоэффективны, поскольку их применение требует максимального приближения датчика к предполагаемому месту нахождения диктофона. Приходится буквально обнимать собеседника, что не только неудобно, но и просто нетактично. Характеристики некоторых обнаружителей работающих диктофонов приведены в табл. 9.

Таблица 9.

Характеристика	PTRD-016	PTRD-018	TRD-800	RM200	РК 645-S
Страна-изготовитель	Россия	Россия	США	Россия	Германия
Макс. дальность обнаружения от датчика, м	до 0,7	до 1,5	до 0,5 при наличии ГСП	до 0,5	до 1
Количество датчиков	4	4/8/16	1	до 6	1
Питание, В	220	220	-	-	9
Потребляемая мощность, Вт	0,6	0,8	-	-	-
Габариты, мм Основного блока Датчика	 160×110×20 170×20×20	 160×80×40 170×20×20	22×57×89	 170×170×30 230×35×25	25×70×25

В табл. 9 указано максимальное расстояние, на котором датчик может среагировать на ПЭМИ диктофона. К сожалению, на практике, когда применяют специальные приборы для скрытой записи, это расстояние несколько меньше.

3.6. Устройства подавления записи работающих диктофонов

Из материалов предыдущего подраздела видно, что обнаружение диктофона – очень сложная техническая задача. Вместе с тем, работающий на

запись диктофон можно подавить, то есть создать условия, при которых запись невозможна. Существуют следующие виды воздействия на диктофоны:

- на сам носитель информации, то есть на магнитную ленту;
- на микрофоны в акустическом диапазоне;
- на электронные цепи звукозаписывающего устройства.

Воздействие на носитель информации

Этот способ нашел применение в устройствах типа размагничивающей арки, которая устанавливается в тамбуре входной двери и создает мощное переменное магнитное поле (обычно с частотой сети или ей кратной). В результате, находящиеся в тамбуре предметы (в том числе и кассеты с записанной информацией) размагничиваются.

Эти устройства характеризуются высоким энергопотреблением и опасны для здоровья, особенно тех лиц, которые пользуются различного рода внедренными в организм электронными стимуляторами. Поэтому организация, применяющая такие системы, обязана информировать посетителей о наличие опасности, что является демаскирующим фактором и приводит к тому, что, по настоянию клиента, разговор может состояться за стенами данного учреждения.

Системы противодействия, использующие принцип воздействия непосредственно на сам микрофон, можно разделить на две группы:

- воздействие на микрофон в ультразвуковом диапазоне с целью перегрузки микрофонного усилителя;
- использование генератора активных акустических помех в речевом диапазоне.

Системы ультразвукового подавления излучают мощные неслышимые человеческим ухом ультразвуковые колебания (обычно частота излучения – около 20 кГц), воздействующие непосредственно и на микрофоны диктофонов, и акустические закладки, что является их несомненным достоинством. Данное ультразвуковое воздействие приводит к перегрузке усилителя низкой частоты, стоящего сразу после акустического приемника. Перегрузка усилителя приводит к значительным искажениям записываемых (передаваемых) сигналов, часто до степени, не поддающейся дешифровке.

Например, комплекс **«Завеса»** при использовании двух ультразвуковых излучателей способен обеспечить подавление диктофонов и акустических закладок в помещении объемом 27 $м^3$. Однако системы ультразвукового подавления имеют важный недостаток: эффективность их резко снижается, если микрофон диктофона или «закладки» прикрыть фильтром из специального материала или в усилителе с низкой частотой установить фильтр низких частот с граничной частотой 3,4-4 кГц.

Воздействие на микрофоны в акустическом диапазоне

Вторая группа средств подавления, использующая генераторы активных акустических помех в речевом диапазоне, применяется в ограниченных случаях. Действительно, трудно представить себе доверительный разговор между партнерами под аккомпанемент генератора шума мощностью в 75-90 дБ.

Воздействие на электронные цепи звукозаписывающего устройства

Наибольшее распространение на практике получили *у*стройства, где способом подавления является *воздействие на электронные цепи диктофона*.

Для этих целей используются системы электромагнитного подавления типа **«Рубеж»** (см. рис. 67), **«РаМЗес», «Шумотрон», «Буран», «УПД».** Принцип действия таких устройств основан на генерации в дециметровом диапазоне волн электромагнитных колебаний, несущая которых модулирована шумоподобным или хаотическим импульсным сигналом.

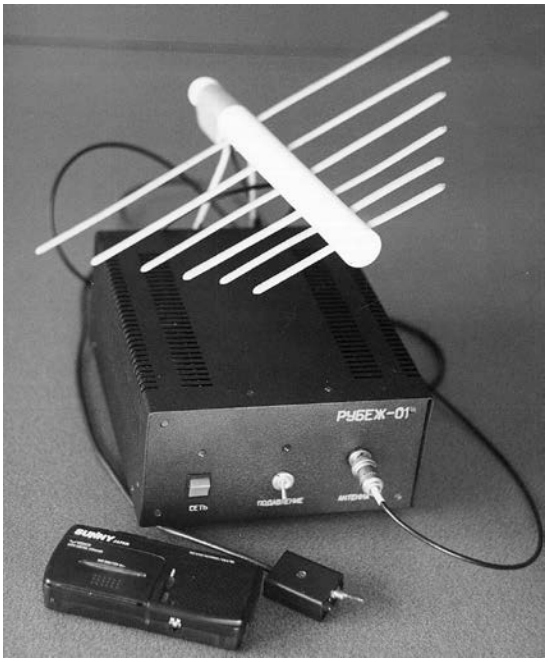

Рис. 67. Внешний вид устройства «Рубеж-01»

Излучаемые направленными антеннами помехи, воздействуя на элементы электронной схемы диктофона, вызывают в них шумоподобные наводки. Вследствие этого одновременно с речью осуществляется запись и шума, что приводит к значительному искажению записываемой информации или вообще к полному ее подавлению.

Зона подавления зависит от мощности излучения, а также от типа используемых антенн. Обычно это сектор с углом от 30˚ до 80˚ и радиусом до 1,5 м (для диктофонов в экранированном корпусе). Для диктофонов в пластмассовом корпусе дальность подавления может вырости до 6 и даже больше. Если диктофон оборудован выносным микрофоном, то дальность подавления становится еще больше за счет того, что соединительный кабель выполняет роль антенны, принимающей излучение от аппаратуры подавления.

Еще один момент, на который следует обратить внимание. Если записывающее устройство, находится у его владельца на теле (в костюме и т. д.), то не исключен факт, что речь самого хозяина диктофона не обязательно, но может и записаться, а вот с записью речи собеседника наверняка будут большие проблемы. Это произойдет из-за того, что звуковое давление, воздействующее на микрофон записывающего устройства, создаваемое голосом хозяина диктофона и его собеседника несоизмеримы по уровню. Владельцу подавителя важно как раз то, чтобы не записали именно его речь. Это и происходит благодаря применению системы подавления.

Некоторые типы диктофонов в режиме записи (UHER, DICTAPHONE, некоторые модели SONY, PANASONIC и т. д.) при попадании в зону подавления начинают сами «шуметь» в акустическом диапазоне, выдавая тем самым намерения своего хозяина. Так что если у вашего собеседника в кармане вдруг что-то зашумело при включении подавителя диктофонов, значит он хотел вас записать, и принятые меры предосторожности не напрасны.

Интересно отметить, что данная аппаратура будет одинаково успешно «давить» запись как кинематических, так и цифровых диктофонов.

Технические характеристики одного из таких приборов – изделия «**РаМЗес-Дубль**»: дальность подавления диктофонов – 1,5-6 м; время непрерывной работы – 20 ч; питание – сеть 220 В; габариты блок подавления - 245×180×70 мм, антенна - 340×220×30 мм; масса – 3 кг.

Обычно подобные приборы используются в офисе, но возможно их применение и в автомобилях с питанием от бортовой сети, иногда применяется камуфляж в виде «кейса».

Другим примером может служить подавитель диктофонов «Шумотрон-2», работающий в импульсном режиме на частоте 915 МГц. Длительность излучаемого импульса в приборе – не более 300 мкс, а импульсная мощность – не менее 150 Вт, таким образом, при средней мощности излучения 20 Вт обеспечивается дальность подавления диктофонов в экранированном корпусе (типа Olimpus-400) до 1,5 м в секторе около 30˚. Дальность подавления диктофонов в неэкранированном корпусе составляет несколько метров.

4. МЕТОДЫ И УСТРОЙСТВА ВЫСОКОЧАСТОТНОГО НАВЯЗЫВАНИЯ И СРЕДСТВА ЗАЩИТЫ

Под высокочастотным навязыванием (ВЧ-навязыванием) понимают способ несанкционированного получения речевой информации, основанный на зондировании мощным ВЧ-сигналом заданной области пространства. Он заключается в модуляции электромагнитного зондирующего сигнала речевым в результате их одновременного воздействия на элементы обстановки или специально внедренные устройства.

4.1. Общая характеристика высокочастотного навязывания

Качество перехвата аудиоинформации с помощью ВЧ-навязывания зависит от ряда факторов:

- характеристик и пространственного положения источника акустического сигнала;
- наличия в контролируемом помещении нелинейного элемента (устройства), параметры которого (геометрические размеры, положение в пространстве, индуктивность, емкость, сопротивление и т. д.) изменяются по закону акустического сигнала;
- характеристик внешнего источника, облучающего данный элемент (устройство);
- типа приемника отраженного сигнала.

Высокочастотное зондирование

Принцип организации съема информации, основанный на ВЧ-зондировании, показан на рис. 53. Однако в некоторых случаях применяются и более сложные схемы.

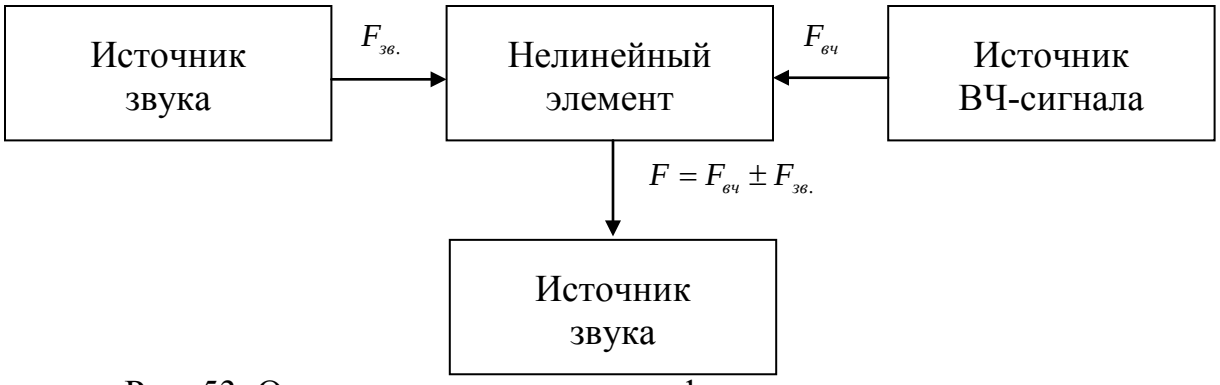

Рис. 53. Организация перехвата информации с использованием ВЧ-навязывания

Основные достоинства данного способа заключаются в активации модуляторов ВЧ-сигнала (нелинейных элементов) только на момент съема информации, а также в возможности (в ряде случаев) вести акустический кон-

троль помещений без непосредственного проникновения для установки закладных устройств.

Основной недостаток метода – как правило, малая дальность действия и высокие уровни облучающих сигналов, наносящие вред здоровью людей. Данные обстоятельства существенно снижают ценность ВЧ-зондирования. Однако определенные методы, о которых будет рассказано в дальнейшем, получили достаточно широкое распространение.

Классификация методов высокочастотного навязывания

Общее представление о многообразии методов такого перехвата дает следующая классификация.

1. По диапазону частот:	радио; оптические.
2. По среде распространения:	по токопроводящей среде; через диэлектрик (воздух).
3. По использованию специально внедренных на объект устройств:	с внедрением; дистанционные.
4. По оперативности получения результатов:	в реальном масштабе времени; с временной задержкой.

Ниже рассмотрим некоторые из принципов ВЧ-навязывания, описанных в доступной литературе.

4.2. Устройства для перехвата речевой информации в проводных каналах

В настоящее время ВЧ-навязывание нашло широкое применение в телефонных линиях для акустического контроля помещений через микрофон телефонной трубки, лежащей на аппарате.

Принцип реализации метода заключается в том, что в телефонную линию относительно общего корпуса (в качестве которого, например, используют контур заземления или трубы парового отопления) на один из проводов подают ВЧ-колебания от специального генератора-передатчика (ПРД). Через элементы схемы телефонного аппарата (ТА), даже если трубка не «снята», они поступают на микрофон и модулируются речью ничего не подозревающих собеседников (см. рис. 54).

Прием информации производится также относительно общего корпуса, но уже через второй провод линии. Амплитудный детектор приемника (ПРМ) позволяет выделить низкочастотную огибающую для дальнейшего усиления и записи. Очевидно, что качество перехватываемой информации тем выше, чем ближе осуществлено подключение к (оконечному устройству) телефонному аппарату. Это обстоятельство вносит определенные неудобства в ис-

пользование данного метода. Фильтр нижних частот (ФНЧ) в линии необходим для одностороннего распространения высокочастотных зондирующих колебаний.

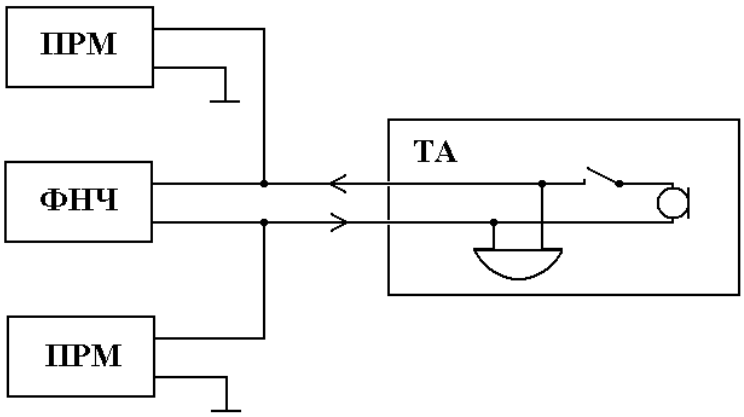

Рис. 54. Принцип реализации ВЧ-навязывания на телефонный аппарат

Принципиально ВЧ-сигнал в данном случае используется для преодоления разомкнутых контактов микрофонной цепи аппарата при положенной телефонной трубке. Дело в том, что для зондирующего сигнала механически разомкнутый контакт является своего рода воздушным конденсатором, сопротивление которого будет тем меньше, чем выше частота сигнала от генератора.

При воздействии ВЧ-излучения на телефонный аппарат нелинейные процессы происходят в целом ряде элементов его электрической схемы. Однако наиболее сильно они проявляются именно в микрофоне, сопротивление которого изменяется по закону случайно воздействующего акустического сигнала, что и приводит к амплитудной модуляции несущей. Для гарантированного возникновения указанного эффекта уровень зондирующего сигнала в микрофонной цепи должен быть не меньше 150 мВ, а выходное сопротивление генератора должно быть выше, чем у микрофона, в 5–10 раз. Частота зондирующего сигнала должна лежать в диапазоне 30 кГц.-20 МГц. Чаще ее выбирают примерно равной 1 МГц, так как при этом обеспечиваются наилучшие условия распространения.

Дальность действия подобных устройств в реальных условиях не превышает нескольких десятков метров. Схема устройства, реализующего описанный выше метод приведена на рис. 55.

В перспективе в области использования проводных каналов, вероятно, будут осваиваться способы зондирования не только телефонных аппаратов, но и других устройств, в том числе по цепям питания, заземления и т. д.

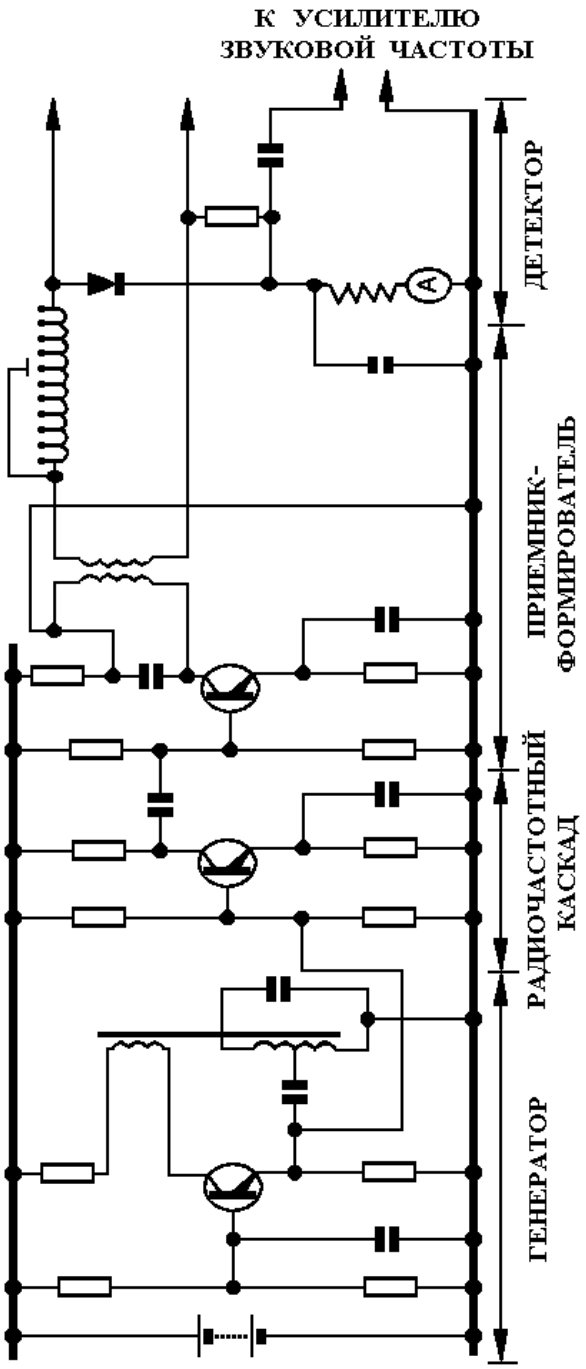

Рис. 55. Схема устройства перехвата информации через телефонный аппарат

4.3. Перехват речевой информации с использованием радиоканала

О работе устройств, использующих принцип ВЧ-навязывания через электромагнитное поле уже упоминалось при описании пассивных и полуактивных радиозакладок. Рассмотрим их более подробно.

Следует отметить, что использованию систем с ВЧ-навязыванием в радиодиапазоне «повезло» – они стали причиной громкого международного скандала. Благодаря этому обстоятельству появилась редкая для технических средств разведки возможность не только обнародовать их технические характеристики и принципы работы, но и изложить историю разработки и применения.

Так, постоянный представитель США при ООН Генри Кэбот Лодж на одном из заседаний Совета Безопасности продемонстрировал в разобранном виде подслушивающее устройство, выполненное в виде гипсового орла – герба Соединенных Штатов Америки. Этот герб был подарен американскому дипломату – послу Соединенных Штатов Америки в Москве Авереллу Гарриману в 1945 году и провисел на стене кабинета в общей сложности при четырех послах. Только в начале 50-х годов специалисты по обнаружению скрытых электронных средств нашли вмонтированное в герб подслушивающее устройство. Инициатор создания программы ЦРУ по разработке миниатюрных средств оперативной техники Питер Карлоу вспоминает, что «мы нашли его, но долго не знали принцип действия. В гербе находилось пассивное устройство, похожее на головастика с маленьким хвостом».

Таким образом, долгое время советское руководство имело возможность получать актуальную, очень важную оперативную информацию, что давало нам определенные преимущества в прогнозировании и осуществлении мировой политики в сложный период «холодной войны».

Имеются данные о том, что, даже зная, что в кабинете посла находится подслушивающее устройство, специалисты обнаружили его только тогда, когда вынесли из кабинета практически всю мебель. В наших разведывательных кругах ходили тогда слухи, что первые подозрение появились у американцев после одной из речей Н. С. Хрущева, когда в результате анализа сведений, высказанных им, специалисты пришли к выводу, что источник утечки информации находится в посольстве США в Москве.

Опубликование информации о необычном закладном устройстве явилось сенсационным еще и потому, что США было заявлено об отсутствии у них аналогичной спецтехники. Она явилась для них полной неожиданностью. Также сообщалось, что Соединенные Штаты приступили к разработке подобных систем съема информации. И действительно через много лет американцы

создали у себя аналогичный вид техники съема информации, который и внедрили в советское посольство за рубежом.

Автором и ведущим руководителем проекта первого пассивного закладного устройства был выдающийся изобретатель Лев Сергеевич Термен. Большой Энциклопедический Словарь уделил ему несколько строк. Родился в 1896 году. Советский физик. Музыкант. В 1920 году изобрел электромузыкальный инструмент «Терменвокс». В 1931–1938 годах – директор акционерного общества по производству электромузыкальных инструментов в США. С 1966 года – научный сотрудник кафедры МГУ. Известно, что Л. С. Термен лично демонстрировал В. И. Ленину свой инструмент, основанный на изменении тона звука генератора при поднесении рук к двум антеннам. В начале 30-х годов Термен после поездки остался в Америке, где основал акционерное общество. Помимо изготовления музыкальных инструментов он участвовал в оборудовании границы между США и Мексикой системой охранной сигнализации для регистрации незаконного пересечения границы нелегалами-мексиканцами. Принцип действия сигнализации такой же, как и аппарата «Терменвокс», емкостной, то есть основывался на регистрации изменений электрической емкости провода, натянутого вдоль границы, при приближении к нему человека.

Когда Термен перед войной приехал туристом в СССР, он, по приказу Берии, был арестован и отправлен в организацию, подобную той, которая была описана А. И. Солженицыным в романе «В круге первом» под названием «шарашка». В эти годы (в середине 40-х) Л. С. Термен и создал свой шедевр, пассивный радиомикрофон.

На рис. 56 обозначены основные элементы пассивного радиомикрофона: 1 - верхняя пластмассовая крышка; 2 - ферритовое кольцо; 3 - изолятор; 4- антенна (четвертьволновой вибратор); 5 - согласующий конденсатор; 6 - корпус; 7 - жидкость; 8 - медный цилиндр (индуктивность); 9 - металлическая диафрагма.

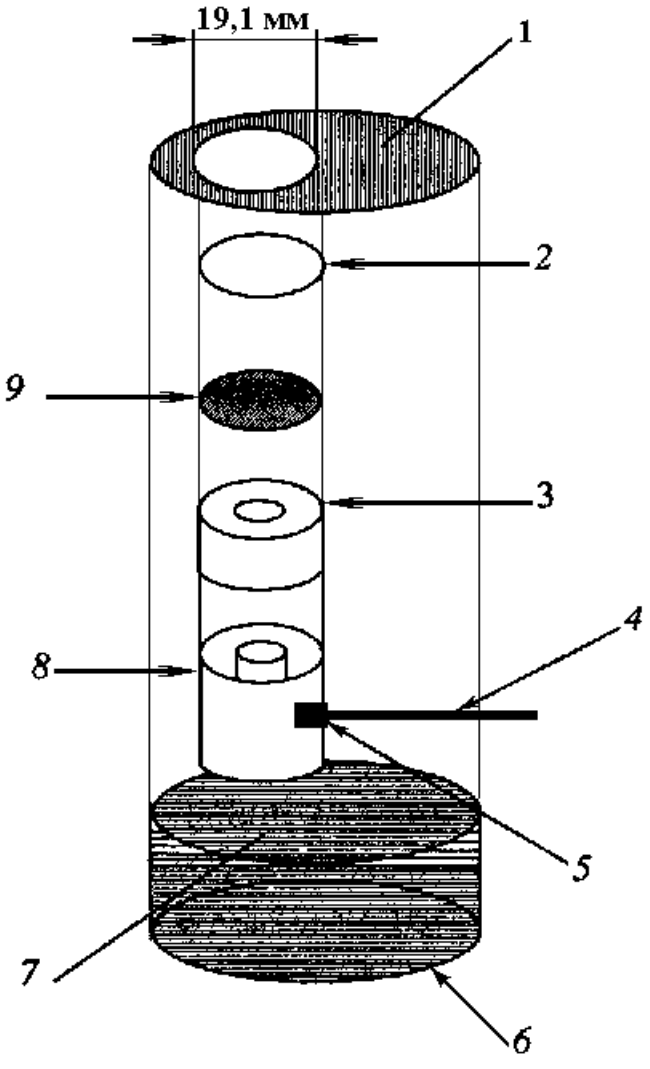

Рис. 56. Пассивный радиомикрофон

Основой устройства является цилиндрический объемный резонатор, на дне которого налит небольшой слой масла. Верхняя часть закрыта крышкой из пластмассы, являющейся радиопрозрачной для радиоволн, но препятствующей проникновению акустических колебаний. В крышке имеется отверстие, через него внутренний объем резонатора сообщается с воздухом помещения, в котором ведутся переговоры. В указанное отверстие вставлена металлическая втулка, снабженная четвертьволновым вибратором, настроенным на частоту 330 МГц. Размеры резонатора и уровень жидкости подобраны таким образом, чтобы вся система резонировала на внешнее излучение с частотой 330 МГц. При этом собственный четвертьволновый вибратор внутри резонатора создает внешнее поле переизлучения. При ведении разговоров вблизи резонатора на поверхности масла появляются микроколебания, вызывающие изменение добротности и резонансной частоты резонатора. Этих изменений достаточно, чтобы влиять на характеристики переизлученного поля, создаваемого внутренним вибратором. Сигнал становится модулированным по амплитуде и фазе акустическими колебаниями. Работать такой радиомикрофон может только тогда, когда он облучается мощным источником на частоте резонатора, то есть 330 МГц.

Главным достоинством такого радиомикрофона является невозможность его обнаружения известными средствами поиска радиозакладок при отсутствии внешнего облучения.

Наряду с пассивными закладками, аналогичными выше описанной, для съема информации используются и полуактивные закладки, называемые аудио-транспондерами; (ответчиками; Audiotransponder). К таким закладкам относятся, например, SIM-ATP-16, SIM-ATP-40 (Hildenbrand-Elektronik), PK500 (PK-Elektronik) и некоторые другие.

Транспондеры начинают работать только при облучении их мощным узкополосным высокочастотным зондирующим (опорным) сигналом. Приемники транспондеров выделяют зондирующий сигнал и подают его на модулятор, где, как правило, осуществляется узкополосная частотная модуляция сигнала. В качестве модулирующего используется сигнал, поступающий или непосредственно с микрофона, или с микрофонного усилителя. Промодулированный ВЧ-сигнал переизлучается, при этом его частота смещается относительно несущей частоты зондирующего сигнала. Время работы транспондеров составляет несколько месяцев, так как потребляемый ток незначителен.

Современные закладные устройства, реализующие вышеописанные принципы, имеют различные габариты и форму. Самые маленькие из них напоминают пластмассовую рыболовную блесну. Отличительные особенности и технические характеристики некоторых типов аудиотранспондеров были описаны ранее в табл. 2. Об их достаточно широком использовании говорит

тот факт, что в 60-е годы американцы жаловались на постоянное облучение ВЧ-сигналами их представительства в СССР с целью активизации встроенных резонаторов.

Кстати, использование подобных систем – достаточно вредное для здоровья дело как для тех, кого подслушивают, так и для тех, кто подслушивает. Специалисты ЦРУ вынуждены были одевать специальные фартуки, предохраняющие важнейшие органы от влияния вредного излучения, когда сами облучали советские учреждения.

Применение полуактивных систем в рамках промышленного шпионажа явление на Западе довольно редкое. На российском рынке подобные системы также пока не представлены и, видимо, не будут представлены еще несколько лет. Однако при дальнейшем совершенствовании противодействия техническим средствам разведки жизнь заставит заинтересованные организации настоятельно потребовать от производителей спецтехники выпуска полуактивных систем.

Кроме использования специальных средств, устанавливаемых на объекте, теоретически возможно зондирование отдельных радиотехнических устройств (телевизоров, приемников и т. д.), узлов бытовой техники, строительных конструкций. Однако на практике это крайне сложная задача, так как требуется перебрать множество вариантов по направлению излучения, частоте зондирующего сигнала, уровня, вида модуляции и т. п.

Перспективой развития подобных средств в радиодиапазоне является модернизация резонаторов с целью повышения индекса модуляции отраженного излучения и рациональный выбор частоты. Приоритетным направлением развития является и освоение более высокочастотных диапазонов (вплоть до миллиметровых волн). Можно предположить, что подобные резонаторы будут выполняться в виде отдельных узлов различного оборудования (кондиционеров, радиоприемников и т. д.) или элементов строительных конструкций. Об этом можно судить по широко известной истории строительства нового здания американского посольства в Москве. Обнаружив в 1982 году подслушивающие устройства, американцы прекратили строительство. Советская сторона в лице председателя КГБ В. Бакатина передала схемы размещения аппаратуры. Многие изделия удивили специалистов, при этом вершиной всего сочли саму конструкцию здания – «восьмиэтажного микрофона». Было объявлено, что направленное на него излучение соответствующей частоты модулируется некими специальными конструктивными элементами, которые способны улавливать звуковые колебания, возникающие при разговоре. Подозревали, что источник и приемник излучения находятся в стоящей через дорогу церкви Девяти мучеников Кизических. В разговорах американских экспертов она часто фигурировала как «храм Богородицы на телеметрии».

4.4. Оптико-акустическая аппаратура перехвата речевой информации

Наиболее перспективным направлением в области ВЧ-навязывания является использование лазерных микрофонов, первые образцы которых были приняты на вооружение американскими спецслужбами еще в 60-е годы.

Принцип работы этих устройств, получивших название лазерные системы акустической разведки (ЛСАР), заключается в следующем. Генерируемое лазерным передатчиком излучение (ВЧ-сигнал) распространяется через атмосферу, отражается от поверхности оконного стекла, модулируется при этом по закону акустического сигнала, также воздействующего на стекло, повторно преодолевает атмосферу и принимается фотоприемником (ПРМ), восстанавливающим разведываемый сигнал (рис. 57).

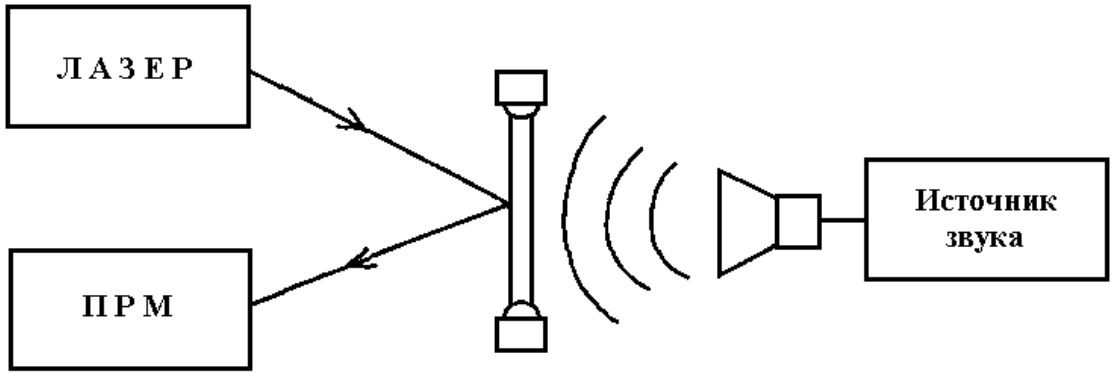

Рис. 57. Принцип работы лазерного микрофона

Сама модуляция зондирующего сигнала на нелинейном элементе, в качестве которого выступает оконное стекло, достаточно сложный физический процесс, который упрощенно может быть представлен в следующем виде:

1. Звуковая волна, генерируемая источником акустического сигнала, падая на границу раздела воздух–стекло, вызывает отклонения поверхности стекла от исходного положения. Отклонения приводят к дифракции света, отражающегося от этой границы.

Действительно, это заметно, например, при падении плоской монохроматической звуковой волны на плоскую границу раздела. Отклонения границы от стационарного состояния представляют собой бегущую вдоль стекла «поверхностную» волну с амплитудой, пропорциональной амплитуде смещений среды в поле звуковой волны, а длина $\lambda_{\text{П}}$ этой «поверхностной» волны равна

$$\lambda_n = \lambda_a / \sin\theta_3, \qquad (4.1)$$

где $\theta_З$ – угол падения, а λ_a – длина падающей акустической волны.

2. Отраженный от возмущенной поверхности свет содержит сдвинутые по частоте дифракционные компоненты. Если поперечный размер падающего пучка лазерного излучения значительно превышают длину «поверхностной» волны, то отраженный свет представляет собой совокупность дифрагирующих пучков, распространяющихся по дискретным направлениям, определяемым из равенства

$$\lambda_a = k_c(\sin\theta_o - \sin\theta_m) = \pi, \qquad (4.2)$$

где $\theta_О$ – угол падения исходного светового пучка, $k_С = 2\pi/\lambda_С$ – волновое число, $\lambda_С$ – длина световой волны.

В результате в отраженных пучках присутствуют три вида модуляции оптического излучения.

Во-первых, частотная модуляция, вызванная эффектом Доплера, вследствие колебательных движений оконного стекла под воздействием акустических сигналов.

При этом девиация частоты относительно центрального значения монохроматического излучения лазера подсветки имеет величину

$$\Delta\varpi = 2\pi / \lambda_a V_n, \qquad (4.3)$$

где $V_n = C_З \sin\theta_З$ – скорость распространения «поверхностной» волны, $С_З$ – скорость звука в среде.

Во-вторых, фазовая модуляция, вызванная наличием в отраженном сигнале как зеркально-отраженного, так и дифракционных компонентов.

Результат суперпозиции последних приводит к тому, что если поперечные размеры падающего оптического пучка малы по сравнению с длиной «поверхностной» волны, то в отраженном сигнале будет доминировать дифракционный пучок нулевого порядка. В этом случае и окажется, что фаза световой волны будет промодулирована во времени с частотой звукового сигнала.

В-третьих, амплитудная модуляция, вызванная колебаниями подсвечивающего пучка относительно направления зеркального (максимального) отражения.

Эти колебания вызваны также пространственным перемещением оконного стекла под воздействием акустического сигнала.

На практике наиболее часто используют системы, работающие на восприятии именно этого вида модуляции.

Для того чтобы работать с лазерными системами акустической разведки, требуется большой опыт. В частности, необходимо правильно выбрать точку съема, грамотно расположить аппаратуру на местности, провести тщательную юстировку. Для обработки перехваченных сообщений необходимо в большинстве случаев использование профессиональной аппаратуры обработки речевых сигналов на базе компьютера. Однако пока подобная техника не для любителей. В нашу страну несколько раз ввозились лазерные системы, но большинство из них так и не были проданы из-за высокой стоимости (от 10 до 130 тысяч $) и неподготовленности потенциальных пользователей, которые, кроме крика ворон, ничего не могли услышать.

Однако из печати известно, что лазерные микрофоны широко использовались против сотрудников советского (российского) посольства и консульств в США, подслушивались разговоры даже в семьях их сотрудников по месту жительства. Поэтому можно полагать, что так как опытные специалисты в состоянии скрытно применять подобные устройства, то весьма вероятно привлечение лазерных систем для решения задач конкурентной борьбы уже в ближайшем будущем.

На сегодняшний день создано целое семейство лазерных средств акустической разведки. Достижения в развитии лазерной техники позволили значительно улучшить технические характеристики и надежность работы данных систем разведки. Достаточно сказать, что появилась возможность дистанционной регистрации колебаний стекла с амплитудой вплоть до 10^{-14} – 10^{-16} м, имеются сообщения о потенциальной возможности работы по объектам на расстояниях до 10 км, а наработка на отказ серийного гелий-неонового лазера составляет не менее 10 000 часов.

Примером современных ЛСАР могут служить устройства HPO150 фирмы «Хьюлет Паккард» и SIPE LASER 3-DA SUPER.

HPO150 – лазерная система, обеспечивающая эффективное обнаружение, подслушивание и регистрацию разговоров, ведущихся в помещениях. Дальность его действия – 1000 м. Устройство использует излучение гелий-неонового или полупроводникового лазера с длиной волны 0,63 мкм (что, кстати, является большим недостатком, так как пятно видно глазом, более современные системы работают в ближнем ИК-диапазоне). Прослушивание и перехват разговоров ведутся, благодаря приему переотраженного сигнала от обычного оконного стекла, представляющего собой своеобразную мембрану, колеблющуюся со звуковой частотой и создающую фонограмму происходящего разговора. Приемник и передатчик выполнены раздельно. Кассетное устройство магнитной записи и специальный блок компенсации помех, а также треноги поставляются в комплекте устройства. Вся аппаратура размещена в небольшом чемодане. Электропитание – от батареи.

SIPE LASER 3-DA SUPER – данная модель состоит из источника излучения (гелий –неонового лазера), приемника этого излучения с блоком фильтрации шумов, двух пар головных телефонов, аккумулятора питания и штатива. Наводка лазерного излучения на оконное стекло нужного помещения осуществляется с помощью телескопического визира. Используется оптическая насадка, позволяющая изменять угол расходимости выходящего пучка, и система автоматического регулирования, задающая высокую стабильность параметров. Система обеспечивает съем речевой информации с хорошим качеством с оконных рам с двойными стеклами на расстоянии до 250 м. На рис. 58 показан внешний вид переносной ЛСАР PK ELECTRONIC.

Рис. 58. Лазерная система акустической разведки

На качество работы лазерных микрофонов существенно влияет большое количество различных факторов: погодные условия, уровни фоновых шумов, толщина и марка стекла, жесткость крепления стекла в раме, способ крепления рамы к стене, длина волны передатчика, точность юстировки аппаратуры, обработки сигнала, длина волны, уровень речи в помещении и т. д. В связи с этим сложно говорить о дальности перехвата информации вообще, можно рассчитать дальность съема информации из данного помещения данной аппаратурой в данных условиях. Кстати, немецкие специалисты даже в рекламных проспектах отмечают, что дальность действия лазерной аппаратуры от единиц до сотен метров.

Дальнейшее развитие лазерных систем, вероятнее всего, пойдет по пути уменьшения массогабаритных характеристик устройств за счет использования современных полупроводниковых лазеров, оптических устройств и средств первичной обработки сигналов с использованием ЭВМ.

В целом, о возможности применения вышеизложенных методов в интересах промышленного шпионажа можно сделать следующие выводы:

- Аппаратура, использующая принцип ВЧ-навязывания, – реальное средство несанкционированного получения речевой информации.
- Эффективность применения ЛСАР зависит от следующих факторов: уровня речи; расстояния от пункта контроля до объекта; технических характеристик аппаратуры и средств вторичной обработки перехваченных сигналов; погодных условий; степени подготовки лиц, использующих технические средства разведки.
- Применение подобной техники возможно только при тщательной предварительной подготовке.
- Использование аппаратуры ВЧ-навязывания в проводных каналах имеет хорошую перспективу из-за сравнительной простоты и дешевизны, известных методов.
- Использование лазерных систем в техническом плане не имеет серьезных проблем, и в обозримом будущем они станут обычным средством несанкционированного получения речевой информации не только спецслужб.

4.5. Защита информации от высокочастотного навязывания

В предыдущих параграфах были выделены основные принципы и устройства для применения методов ВЧ-навязывания на различных защищаемых объектах. В этом параграфе рассмотрим методы защиты в соответствии с вышеизложенным материалом по каждому из возможных каналов воздействия.

Защита в проводных каналах

Защита информации от ВЧ-навязывания в проводных каналах осуществляется с помощью как организационных, так и технических мероприятий.

К *организационным мероприятиям* относятся:

- использование телефонных аппаратов, выполненных в защищенном виде;
- осуществление физического контроля телефонных линий на предмет наличия подключений (на расстояниях до 100 м от аппарата, что соответствует предельной дальности действия систем перехвата информации такого типа);
- отключение ТА от сети на время проведения переговоров.

Однако организовать постоянный контроль телефонных линий в реальных городских условиях достаточно проблематично. Это можно сделать только при размещении организации в обособленном здании либо при наличии собственной АТС. Отключение аппаратов от линии на время проведения переговоров также нельзя отнести к надежным мероприятиям: опыт показывает, что об этом часто забывают. Поэтому надежной защиты не может быть без применения технических средств.

Технические мероприятия проводятся по следующим направлениям:

- инструментальный контроль излучений на предмет выявления зондирующих ВЧ-сигналов в линиях связи;
- установка пассивных схем защиты.

Рассмотрим перечисленные технические способы более подробно. Проведение контроля телефонных линий на предмет выявления зондирующих сигналов технически легко осуществимое мероприятие. Для этого необходимо иметь приемник со следующими характеристиками:

- частотный диапазон 9 кГц -30 МГц;
- чувствительность порядка нескольких единиц микровольт;
- наличие АМ и ЧМ-детекторов.

Кроме того, требуется обеспечить прием сигналов, распространяющихся по проводным линиям. Для этого можно использовать обычные электрические и магнитные антенны, например, электрические НЕ 010, НЕ 013/015, HFH 2Z1 и магнитные HFH 2-Z3, HFH 2-Z2. Могут использоваться упоминавшиеся ранее комбинированные антенны, предназначенные для измерения как магнитной, так и электрической составляющей поля, например FMA-11. Однако располагать антенны следует в непосредственной близости от проводов телефонной сети. Очень эффективны для этих целей специальные антенны типа токосъемных клещей.

В табл. 9 приведены технические характеристики приемных устройств для обнаружения ВЧ-излучений в проводных каналах связи.

Таблица 9.

Модель	Диапазон, МГц	Вид модуляции	Чувствительность, мкВ (с/ш = 12 дБ)	Шаг настройки, кГц	Габариты, мм Вес, кг
IC-R72	0,03-30	AM, FM, SSB, CW	0,5-1	0,01; 0,1; 1; 5; 9; 10; 1000	241×94×229 5,5
IC-R71A/E	0,1-30	AM, FM, WFM, SSB, FSK, CW	0,3-3	0,01; 1; 1000	286×110×276 7,5
HF-150	0.03-30	AM, FM, SSB	0.2-2	1	185×80×175 1,3
AR3030	0,03-30	AM, FM, WFM, USB LSB, CW	0,3-3	0,005; 0,01; 1; 1000	250×88×240 2,2
FRG-100	0.005-30	AM, FM, SSB, CW	0,25-10	0,001; 0,1; 1	238×93×243 3
TS-140	ОД5-30	AM, FM, SSB, CW	0.25-10	—	270×96×270 6,1
FRG-100	0,005-30	AM, FM, SSB, CW	0.25-10	0,001; 0,1; 1	238×93×243 3
STV-301	0,01-30	AM, FM, WFM	2	—	360×320×130 7
FSM11	0,01-30	AM, FM, WFM	0,1	0,2; 1,7; 9	450×145×545 26

Недостатком рассматриваемого метода защиты является возможность выключения аппаратуры перехвата информации во время проверки, следовательно, эпизодический контроль оказывается не вполне надежным.

Гарантированным способом противодействия является шунтирование линии или микрофона телефонной трубки конденсатором емкостью 0,01 мкФ. Он имеет предельно низкую цену, а обеспечивает достаточно надежную защиту. Зондирующий сигнал по законам физики «идет по пути наименьшего сопротивления», а конденсатор для высокой частоты имеет относительно низкое по сравнению с микрофоном сопротивление.

В связи с этим обстоятельством интересен тот факт, что как у нас, так и за границей существуют предприниматели, которые продают «защищенные» от ВЧ-навязывания телефонные аппараты по цене до нескольких сотен дол-

ларов. Экономическая нецелесообразность приобретения подобных аппаратов очевидна.

Защита информации в радиодиапазоне

Основная сложность применения пассивных и полуактивных радиозакладных устройств, описанных выше, – это необходимость проникновения на объект с целью их установки, что требует проведения специальных операций. В качестве примера в том же подразделе был приведен исторический случай проведения мероприятия по внедрению «орла» в американское посольство. Вернемся к нему еще раз, чтобы четко сформулировать требования по обеспечению защиты.

Так, перед непосредственными исполнителями была поставлена задача получения достоверной информации из американского посольства в Москве. Агентурное проникновение было весьма затруднено, подходов к американским дипломатам практически не имелось. Поэтому рассматривались различные варианты мероприятий, которые смогли бы обеспечить конспиративность постановки спецтехники для съема информации. Обычные классические методы внедрения технических средств для организации контроля разговоров были неприемлемы, так как не было соответствующей агентуры для внесения в помещения каких-либо предметов – камуфляжей, в которых располагалась бы техника для съема информации. К тому же было известно, что американская служба безопасности постоянно осуществляет в своем посольстве в Москве контроль эфира в диапазоне радиоволн, на которых имеется возможность работать передатчиками для съема информационных сигналов.

В связи с этим начались исследования по созданию различных вариантов новой спецаппаратуры съема информации с использованием нетрадиционных принципов создания технических устройств. В результате остановились на методе облучения высокой частоты нелинейного пассивного эндовибратора (микрофона).

Помимо разработки принципиально нового вида спецтехники было уделено серьезное внимание созданию камуфляжа для обеспечения максимума безопасности. Было решено смонтировать спецтехнику внутри овального предмета из алебастра и гипса с рельефной символикой в виде американского национального герба. А сама пористость поверхности герба была достаточна для прохождения звуковой энергии человеческого голоса к микрофону. Контрольный пункт для приема информативных сигналов от «герба» располагался в помещениях гостиницы «Националь» (речь идет о старом здании Посольства США в Москве, располагавшемся на Манежной площади).

Следующим этапом в проведении мероприятий по получению информации из кабинета американского посла стала разработка убедительной ле-

генды для внесения «герба» в здание посольства. В день национального праздника Америки в посольство пришла пионерская делегация и в торжественной обстановке вручила американскому послу «герб». Посол поблагодарил за приятный подарок и повесил «герб» у себя в кабинете на стене над своим письменным столом.

Следовательно, в случае более четких действий службы безопасности появление подобного подарка в кабинете, где обсуждаются конфиденциальные вопросы, было бы невозможно. Сотрудники спецслужб понадеялись на проверку «орла» (по существующему порядку все вносимые предметы, особенно в такую ответственную зону, как кабинет посла, подвергались тщательной проверке, в том числе рентгеновскому просвечиванию), которая ничего не дала. Действительно, выявить подобные устройства крайне сложно и самый *действенный* метод защиты – никаких подарков не принимать.

Второй недостаток данной системы, который возможно использовать для организации защиты, это очень большие уровни мощности передатчика. Современные приборы легко обнаруживают такое излучение. Трудность заключается только в том, что необходимо зарегистрировать излучение непосредственно в момент перехвата информации.

Кабинет американского посла многократно проверялся на наличие радиозакладок с отрицательным результатом. Однако американская спецслужба решилась серьезно заняться поиском техники съема информации, которая, как они предполагали, установлена в здании посольства в Москве. Поэтому из США прибыли специалисты с соответствующей аппаратурой. События происходили следующим образом: была проведена рутинная проверка, после чего специалисты удалились. Шторы на окнах оставались открытыми и наблюдатели зафиксировали, что посол приступил к диктовке писем секретарю. Сотрудники с аппаратурой в это время находились под подоконником с радиоприемным устройством и скрытно разворачивали антенны. Вот тут и было обнаружено направленное излучение высокой частоты. После этого определили и место. Вначале со стены был снят «герб», а саму кирпичную стену почти всю разобрали. Образовалось большое отверстие с выходом на улицу. «Герб» несколько дней лежал в кабинете, и только затем они решили посмотреть, нет ли чего-нибудь у него внутри. «Герб» разломали и нашли резонатор.

Следовательно, *для обнаружения факта облучения необходимо проводить либо постоянный радиоконтроль, либо провоцировать противостоящую сторону на применение средства разведки в известные сроки*. Обнаружение зондирующего ВЧ-сигнала – довольно простое дело даже для неспециалиста. Для этих целей необходим панорамный радиоприемник или анализатор спектра. Выбранный прибор переводится в режим максимального обзора при минимальной чувствительности, и осуществляется изучение радио-

электронной обстановки в районе расположения объекта (идентифицируются все мощные излучения). Антенны поворачиваются в сторону возможного расположения передатчиков. После этого достаточно фиксировать появление зондирующих сигналов. Главная сложность – периодические ложные срабатывания: радиотелефоны в прилегающих помещениях, радиомаяки различного назначения, мощные радиостанции армии и спецслужб, которые работают не постоянно.

Еще один способ защиты – экранирование помещения. Способ действенный, проблема состоит только в том, что он очень дорогой и резко снижающий эргономические характеристики помещения. Особую сложность вызывает защита окон и дверей. Другое направление – размещение помещений, выделенных для проведения конфиденциальных мероприятий, в заглубленных железобетонных подвалах.

Защита информации в оптическом диапазоне

Для защиты от лазерных микрофонов возможно использование организационных и технических мероприятий. Последние, в свою очередь, реализуются путем различных видов воздействия на канал перехвата информации активными и пассивными средствами в оптическом и акустическом диапазонах.

К *организационным методам* можно отнести:

- использование погодных и климатических условий (дождь, снег, сильный ветер и т. д.);
- ведение переговоров в местах с высоким уровнем фоновых шумов (как внешних, так и внутренних);
- размещение на местности таким образом, чтобы на пути распространения лазерного луча были естественные и искусственные препятствия (кустарник, строения и т. д.);
- использование недоступных для лазерного подслушивания помещений (окна выходят во двор; подвальные, полуподвальные помещения);
- увеличение расстояния до границы контролируемой территории;
- расположение рабочих мест, исключающих прохождение акустических сигналов к окнам;
- использование аппаратуры предупреждения о применении лазерных систем;
- ведение переговоров не повышая голоса, не срываясь на крик (разница в уровне речи между нормальным и громким голосом может достигать 15 дБ);
- увеличение расстояния от говорящего до окна.

К применению организационных мероприятий необходимо подходить разумно. Например, глупо было бы ждать резкого ухудшения погоды, чтобы провести конфиденциальную беседу.

Более надежными являются *технические методы* защиты информации. Так, радикальным средством защиты в оптическом диапазоне является прерывание сигнала с использованием ставней, экранов и т. д. Однако это приводит к отсутствию в помещении дневного света. Представляется возможным ослабить зондирующий лазерный сигнал и путем его рассеивания, поглощения или отражения. Технической реализацией данных способов является использование различных пленок, наносимых на поверхность стекла. Таковы в общих чертах возможности противодействия пассивным методам в оптическом диапазоне. При активном противодействии задача сводится к электромагнитному воздействию на приемные (а, возможно, и передающие) тракты аппаратуры разведки с целью выведения их из строя либо временного ухудшения работоспособности.

Целью противодействия в акустическом диапазоне является уменьшение отношения сигнал/шум в точке ведения съема (на поверхности стекла), при которых восстановление речевой информации невозможно (от –10 до –14 дБ).

Решение данной задачи возможно двумя способами:

- увеличением уровня маскирующего шума, то есть применением активных средств акустической маскировки;
- снижением уровня сигнала, то есть усилением звукоизоляции окна.

В настоящее время существует большое количество типов систем активного зашумления в акустическом диапазоне. Они используются для подавления дистанционных и забрасываемых средств перехвата речевой информации. В существующих системах формируется маскирующий сигнал типа «белый» шум или типа «разговор трех и более лиц», спектр которого представляет собой усредненный спектр голоса человека. У подобных систем имеется целый ряд недостатков.

Во-первых, значительно повышается уровень фоновых акустических шумов в защищенном помещении, что приводит к быстрой утомляемости находящихся в нем людей.

Во-вторых, при разговоре в зашумленном помещении человек инстинктивно начинает говорить громче, тем самым повышается величина отношения сигнал/помеха на входе приемника, акустической разведки. Таким образом, с учетом того, что активная акустическая маскировка ухудшает эргономические показатели, основным путем защиты речевой информации является обеспечение необходимых акустических характеристик ограждающих конструкций выделенных помещений.

Звукоизолирующая способность ограждающих конструкций определяется отношением величины интенсивности J_1, прошедшего через ограждение звука, к интенсивности падающего J_2, и характеризуется коэффициентом $t = J_1 / J_2$.

В расчетах и измерениях наиболее часто используют величину, называемую звукоизоляцией R или потерями на прохождение звука через препятствие (ограждение) и определяемую соотношением

$$R = -10 \times \lg(t) \qquad (4.4)$$

Значение звукоизоляции R для различных типов ограждающих конструкций и ряда акустических частот приведены в табл. 10. Необходимо отметить, что существенное влияние на звукоизоляцию оконных конструкций оказывает наличие в них щелей и отверстий.

Таблица 10.

Тип конструкции	Акустическая частота, Гц			
	500	1000	2000	4000
Кладка в 1/2 кирпича	42	48	54	60
Кладка в 2 кирпича, оштукатуренная	59	65	70	70
Плита железобетонная, 50 см	35	45	51	58
Щитовая дверь	24	24	24	23
Двери тяжелые двойные с облицовкой тамбура	65	70	70	71
Одинарное остекление, 3 мм	22	28	31	32
Двойное остекление, 4 мм, между стеклами — 200 мм	39	47	54	56
Тройное комбинированное остекление	71	66	73	77

Наиболее совершенными в настоящее время являются конструкции окон с повышенным звукопоглощением на основе стеклопакетов с герметизацией воздушного промежутка и с заполнением промежутка между стеклами различными газовыми смесями. Стеклопакеты устанавливаются в оконных блоках, выполненных из различных материалов, обладающих низкой звукопроводностью. Стекла выбираются разной толщины и устанавливаются с небольшими наклонами относительно друг друга. Все это позволяет при значительном ослаблении сигнала избежать резонансных явлений в воздушных промежутках. В результате интенсивность речевого сигнала на внешнем стекле оказывается значительно ниже интенсивности фоновых акустических

шумов и съем информации традиционными для акустики методами оказывается невозможным.

Наиболее радикальной мерой защиты является прерывание распространения звука. Это достижимо только в случае применения вакуумной звукоизоляции. В основе способа лежит физическое явление, состоящее в том, что звук не может распространяться в пустоте. Таким образом, теоретически при вакууме между точкой ведения разведки и источником речи получаем идеальную звукоизоляцию. Однако на практике обеспечить полное прерывание невозможно, так как требуется обеспечить герметизацию не только межстекольного пространства, но и пространства между переплетом и рамой, а кроме того, предотвратить структурное распространение звука через материал рам.

Окна обычной конструкции имеют низкий уровень звукоизоляции (см. табл. 10). Кроме того, на звукоизоляцию влияют: герметичность швов между стеклом и переплетом, переплетом и оконной рамой, оконной рамой и стеной; длина, высота и размер поперечного сечения переплета и стекла; поглощение звука в звукопоглощающих элементах между стеклами и рамой; особенности конструкции и способы ее изготовления и т. д.

Широкое распространение получили и так называемые акустические экраны, которые используются при невозможности применения стационарных методов звукоизоляции. Обычно применяются передвижные, складные и легко монтируемые акустические экраны.

С целью решения задач по защите помещений акустические экраны могут быть использованы для дополнительной защиты окон, имеющих низкую звукоизолирующую способность.

В целом можно утверждать, что применение даже простейших приемов позволит избежать перехвата информации либо существенно ухудшит качество записанного разговора.

Таким образом, организация защиты информации от перехвата лазерными микрофонами возможна различными способами и средствами. Необходимо проведение оптимизации существующих мер защиты при их комплексном использовании, так как наличие большого количества противоречивых требований и ограничений (в основном эргономических и стоимостных) требует проведения многоспектральной оценки эффективности системы защиты объекта от лазерных систем перехвата речи.

Защита информации от ВЧ-навязывания вирусов

Дистанционное внедрение компьютерных вирусов с помощью ВЧ-навязывания в настоящее время не является актуальной угрозой, но в недалеком будущем сможет наносить существенный урон государственным и ком-

мерческим структурам. В связи с этим рассмотрим возможные способы защиты информации, циркулирующей в ЭВМ, реализация которых возможна с помощью организационных, программных и технических мер.

К *организационным мерам* можно отнести следующие:

- Увеличение радиуса контролируемой территории вокруг объекта электронно-вычислительной техники (это ведет к необходимости существенно увеличивать мощность передатчика ВЧ-навязывания);
- Обучение персонала по обнаружению признаков воздействия ВЧ-сигналов (помехи на экране монитора, сбои в работе отдельных устройств и т. д.);
- Осуществление контроля доступа к линиям связи, терминалам, сетям электропитания и другим элементам сети и вспомогательного оборудования;
- Расположение электронно-вычислительной техники в заглубленных помещениях, бетонных зданиях и использование естественных экранов на пути возможного распространения ВЧ-сигналов.

Программные меры подразумевают использование систем антивирусной защиты и будут рассмотрены ниже.

К дополнительным *техническим мероприятиям* следует отнести:

- Создание и использование системы предупреждения о применении «вирусного орудия» путем проведения постоянного радиоконтроля на предмет выявления мощных электромагнитных сигналов вблизи ЭВМ;
- Экранирование персонального компьютера, соединительных кабелей, другого оборудования или в целом зданий и сооружений;
- Установка фильтров в цепях электроснабжения, управления и связи;
- Широкое внедрение оптоволоконных соединений.

5. ОПТИЧЕСКИЕ СРЕДСТВА ДОБЫВАНИЯ ИНФОРМАЦИИ

Зрение человека играет исключительно важную роль в познании окружающего мира, так как примерно 90% получаемой информации приходится именно на зрение и только 10% – на другие органы чувств. Интерес к секретам конкурентов, с долей иронии, также может рассматриваться как тяга к познанию. Отсюда и стремление определенной категории людей к «прослушиванию» конкурентов и получению некоторой зрительно осязаемой информации, например, о содержании интересующих документов и фотографий, о внешнем виде собеседников или передаваемых предметов во время конфиденциальной встречи.

Однако мудрая природа, дав людям такой важный для восприятия окружающего мира прибор, существенно ограничила его возможности. Так, основными характеристиками человеческого глаза являются следующие:

- *Мгновенное угловое поле зрения*: в горизонтальной плоскости составляет 65-95°; в вертикальной плоскости – 60-72°.
- Расстояние наилучшего зрения – 250 мм.
- Время удержания взглядом изображения – 0,06 с.
- Область спектральной чувствительности лежит в диапазоне от 0,37 до 0,72 мкм (см. рис. 59).

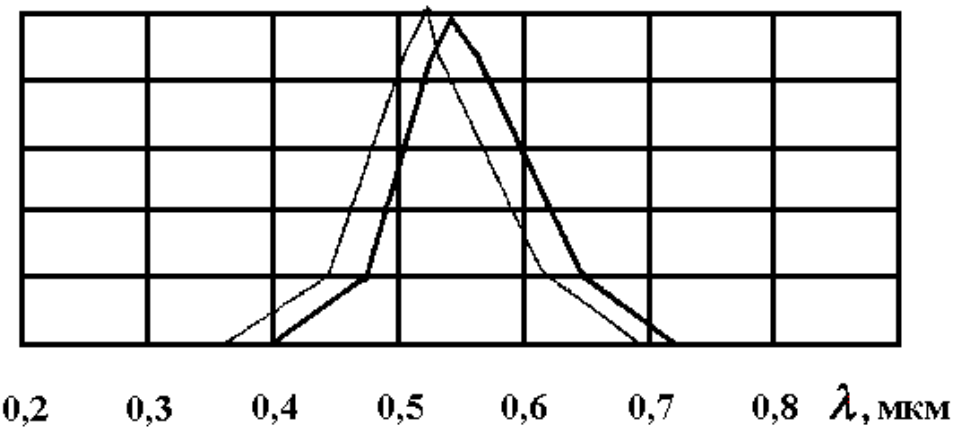

Рис. 59. Характеристика спектральной Чувствительности человеческого глаза: —— для дневного света; ▬▬ для слабой освещенности

В соответствии с приведенной характеристикой максимальная восприимчивость для дневных условий соответствует темно-зеленому излучению с длиной волны $\lambda = 0{,}54$ мкм (поэтому на зеленом цвете глаз «отдыхает»), а в сумеречное время – излучению с длиной волны $\lambda = 0{,}507$ мкм – голубой цвет. Отсюда и известное выражение, что ночью все кошки серые.

5.1. Оптико-механические приборы

Естественно и вечное стремление людей расширить границы своего зрения. Люди старались улучшить все характеристики зрения и создали огромное количество оптических приборов: для увеличения дальности наблюдения – зрительные трубы, бинокли и телескопы, для расширения области спектральной чувствительности – так называемые приборы ночного видения, для расширения поля зрения – системы телевизионного наблюдения, а для фиксации изображения – фотоаппараты кино- и видеокамеры.

Наиболее древними из перечисленных являются так называемые оптико-механические приборы, позволяющие зрительно приблизить удаленные предметы. Несмотря на свой «преклонный возраст» они до сих пор очень популярны и практически незаменимы для наблюдения за конкурентами с больших расстояний или из укрытий.

Принцип действия таких приборов основан на том свойстве, что один и тот же предмет виден под большим углом $(\psi_2 > \psi_1)$ при меньшей дальности $R_2 < R_1$ (см. рис. 60).

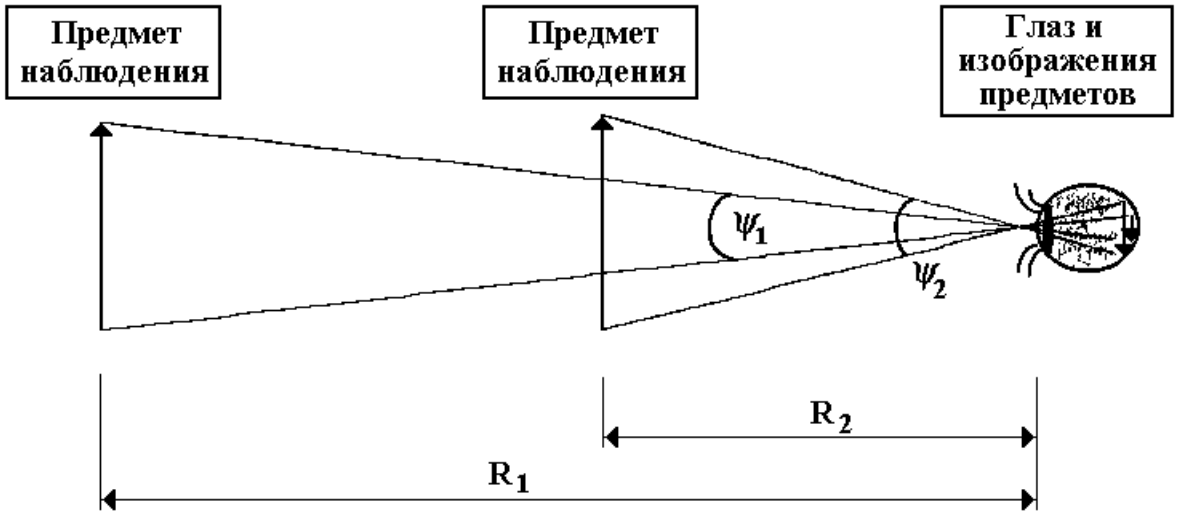

Рис. 60. Схема формирования изображения на сетчатке глаза

Так, если невооруженным глазом предмет виден под углом ψ_1, а оптическая система создает изображение, видимое под углом ψ_2, то видимое увеличение, или кратность увеличения определяется выражением

$$\Gamma = \frac{tg\,\psi_2}{tg\,\psi_1} \approx \frac{\psi_2}{\psi_1}. \qquad (5.1)$$

В простейшем случае такая телескопическая система представляет собой двухкомпонентную афокальную систему, изображенную на рис. 61. Чем

больше ее длина, тем меньше угол ψ_1 ($\psi_1^{11} < \psi_1^1$ при $R^{11} > R^1$), а, следовательно, больше видимое увеличение Г. Так как величина угла ψ_2 согласована с размерами и воспринимающей способностью глаза и для нормальных условий составляет значение ψ_2 = 60°, то видимое увеличение оптико-механического прибора может быть оценено по диаметру входного отверстия объектива D, выраженного в миллиметрах

$$\Gamma\ [\text{крат}] \approx 0{,}43\ D\ [\text{мм}]. \qquad (5.2)$$

Более точное значение величины Г лежит в пределах от 0,2 до 0,75 D. Однако надо иметь в виду, что чем больше кратность увеличения, тем меньше мгновенное угловое поле зрения θ, которое связано с величиной угла ψ_1 соотношением $\theta = 2\ \psi_1$.

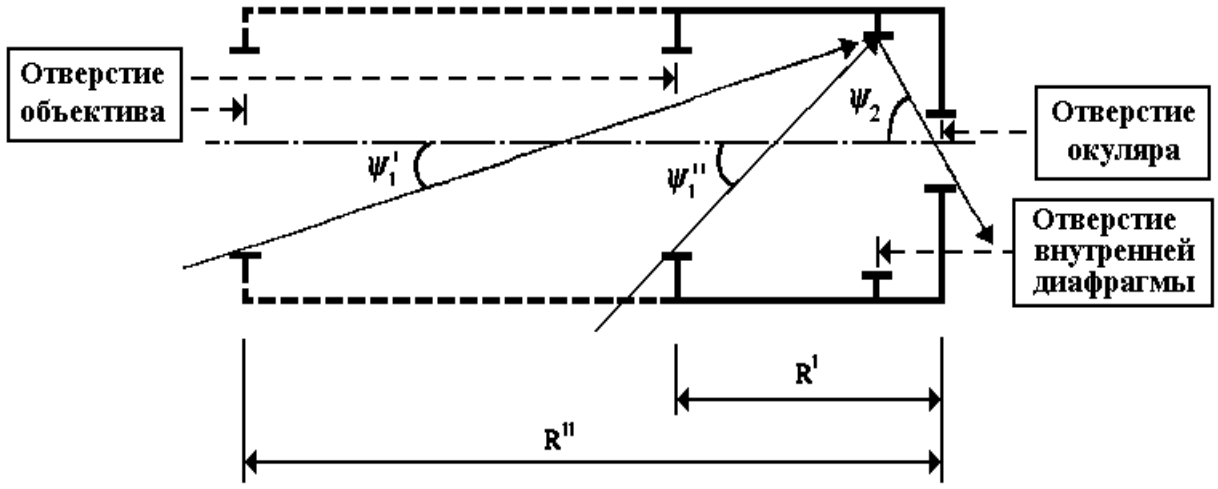

Рис. 60. Двухкомпонентная телескопическая афокальная система

В отверстия объектива и окуляра могут быть вставлены различные линзы (выпуклые, вогнутые, выпукло-вогнутые и др.), но для целей получения конфиденциальной информации лучше всего подходят двояковыпуклые линзы. Такая оптическая система известна под названием *системы Кеплера,* или астрономической трубы.

Достоинством системы Кеплера является то, что в плоскости изображения может быть установлена сетка (шкала). Она позволяет решать измерительные задачи по определению дальности до объекта наблюдения, в то время как другие оптические системы не могут быть использованы для этих целей.

Для того чтобы измерить расстояние R до объекта наблюдения необходимо знать ориентировочный линейный размер объекта L, выраженный в метрах, и его угловой размер Y. Последний определяется по шкале оптиче-

ской системы в условных единицах, называемых тысячные. Величина Y измеряется, исходя из цены деления шкалы (расстояния между двумя соседними делениями). Эта цена составляет 5 тысячных, такому же значению соответствует собственный размер малого штриха деления. Расстояние между двумя большими делениями и размер штриха большого деления – 10 тысячных.

Значение расстояния R [м] рассчитывается по формуле

$$R[м] \approx L[м] \times \frac{1000}{Y[тыс]}. \qquad (5.3)$$

Так, например, на рис. 61 представлен случай, когда в поле зрения оптической системы находятся одновременно человек и автомобиль.

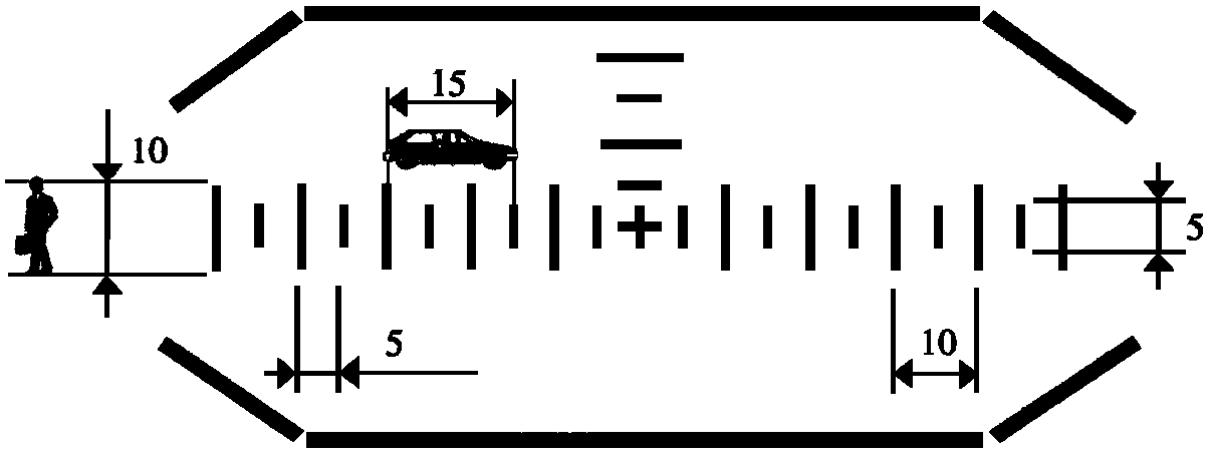

Рис. 61. Определение расстояния до объекта по шкале установленной в оптической системе Кеплера

Известно, что средний рост мужчины составляет 1м 75 см (L=1,75 м), А его угловой размер для случая, изображенного на рисунке, Y=10 тысячных, таким образом, расстояние от наблюдателя до человека составляет величину

$$R \approx L[м] \times \frac{1000}{Y[тыс]} = 1{,}7 \times \frac{1000}{10} = 170м. \qquad (5.4)$$

Длина другого объекта – автомобиля около 4,5 м (L= 4,5м), его угловой размер – Y=15 тысячных, следовательно дальность до автомобиля в рассматриваемом примере имеет значение

$$R \approx L[м] \times \frac{1000}{Y[тыс]} = 4{,}5 \times \frac{1000}{15} = 300м. \qquad (5.5)$$

Однако необходимо знать, что существует метод оценки дальности до объекта и с помощью подручных средств, например обычной линейки (см. рис. 62).

Он основан на том, что угловой размер 1 мм на удалении 50 см от глаз составляет около 2 тысячных. Таким образом, если определить величину «видимого размера» объекта на удалении 0,5 м от глаз, то примерное расстояние будет иметь значение

$$R \approx L[м] \times \frac{500}{d[мм]}, \tag{5.6}$$

где d [мм] – видимый размер объекта на удалении 0,5 м.

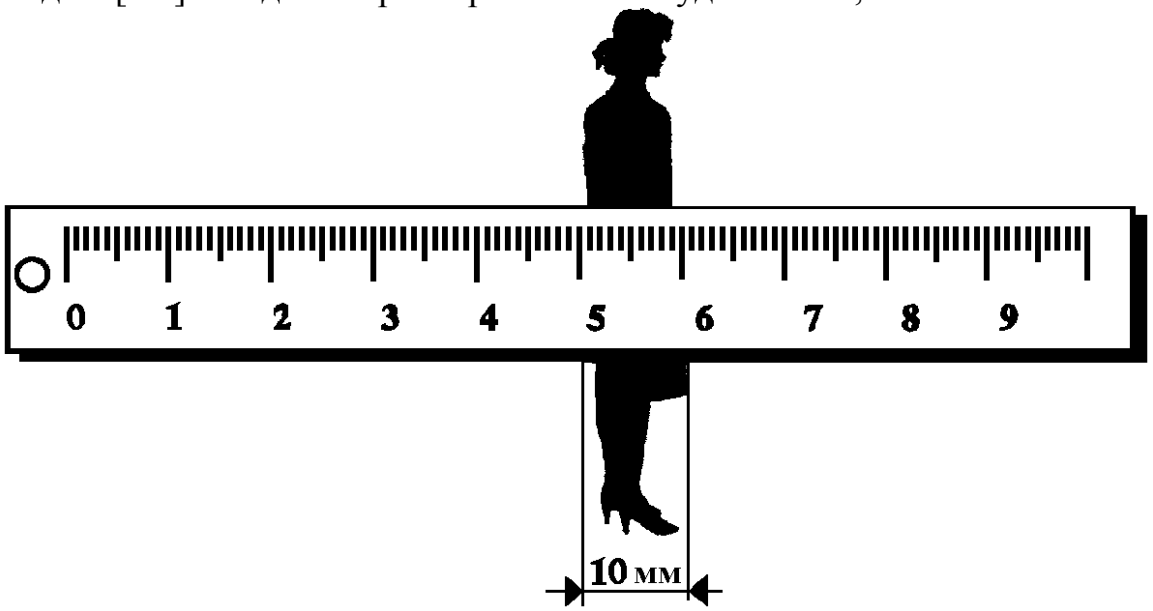

Рис. 62. Определение расстояния до объекта с использованием обычной линейки

Для случая, изображенного на рис. 62, линейный «видимый размер» фигуры имеет значение $d \approx 10$ мм, а реальный размер – L ≈ 0,5 м. Следовательно, дальность до объекта

$$R \approx L[м] \times \frac{500}{d[мм]} = 0{,}5 \times \frac{500}{10} = 25м. \tag{5.7}$$

Вместо линейки может быть использован любой другой небольшой предмет геометрические размеры которого известны: спичечная коробка, карандаш, пластиковая карта, бумажная купюра и т. п.

Основной недостаток оптической системы Кеплера – переворачивание изображения, из-за чего наблюдатель видит все «вверх ногами». Для устранения недостатка в систему вводят компоненты, обеспечивающие восстановление нормального положения изображения. В качестве таких элементов используют дополнительные линзы (см. рис. 63), например, в подзорных трубах или телескопах.

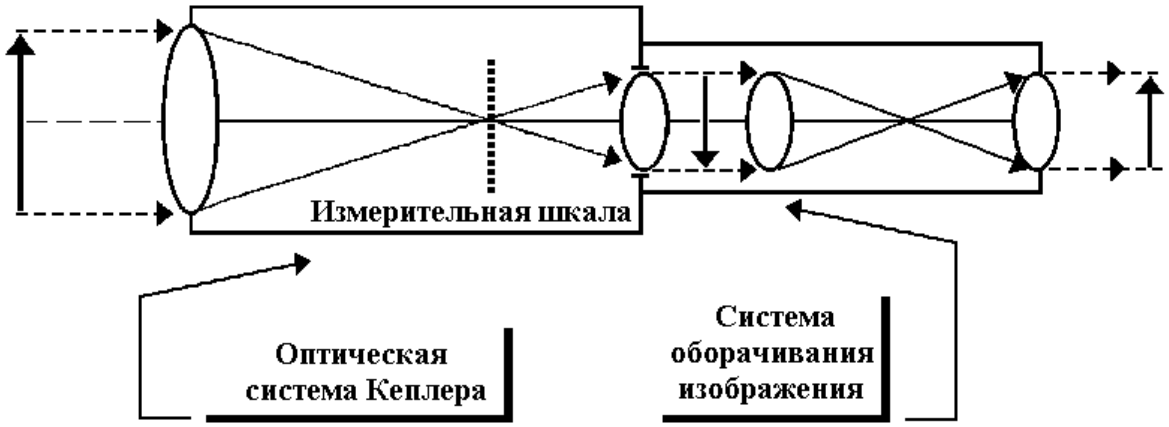

Рис. 63. Восстановление нормального изображения в телескопе

Иногда изображение восстанавливают с помощью призм (см. рис. 64), например, в биноклях или артиллерийских панорамах.

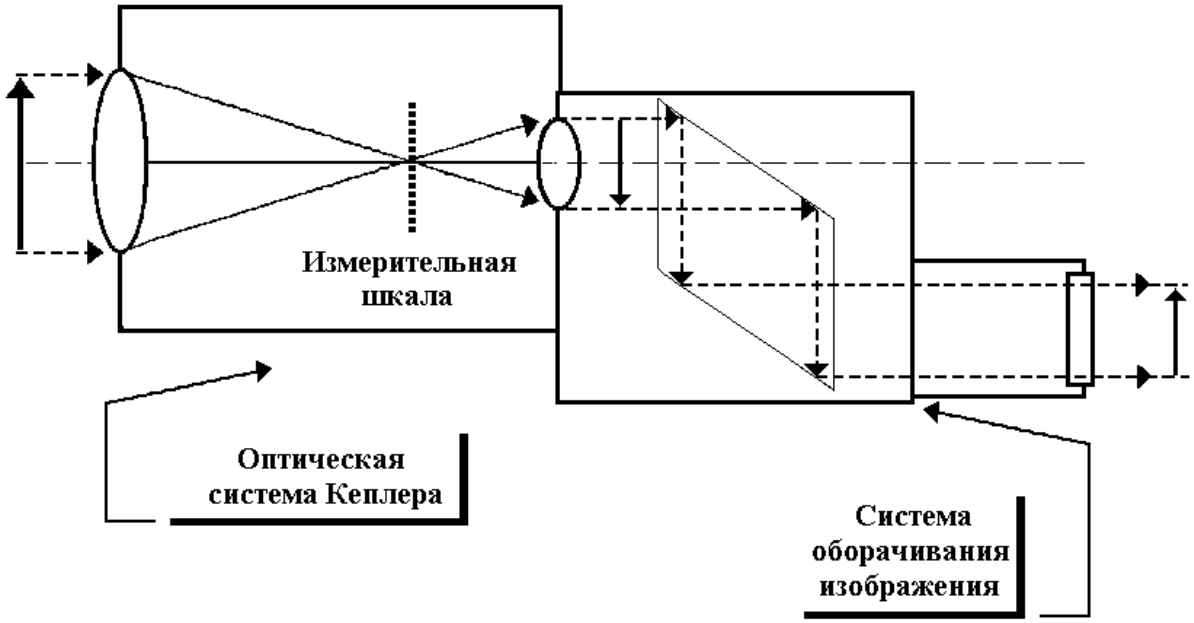

Рис. 64. Восстановление нормального изображения в бинокле

Для ведения скрытного наблюдения необходимо тщательно выбирать позицию с учетом местных условий и окружающего ландшафта. Хорошо для этих целей подходит густая листва деревьев, различные строения, места складирования крупногабаритных предметов. Однако в ряде случаев оказывается затруднительно выбрать удобное место, и наблюдение приходится вести из-за угла, через препятствие и т. п. В этом случае хорошую услугу могут оказать упомянутые выше артиллерийские панорамы или другие оптические системы перископического типа, имеющие достаточно малые геометрические размеры

входного объектива и изменяющие направление распространения оптических лучей.

Ведя скрытое наблюдение за объектом с помощью оптико-механического прибора, необходимо помнить о таком коварном демаскирующем факторе, как солнечные блики на стекле вашей оптической системы, которые могут быть видны на расстоянии, достигающем нескольких километров. Чтобы не быть обнаруженным, необходимо выбирать позицию для наблюдения таким образом, чтобы прямые солнечные лучи не попадали на оптические стекла. Также надо знать, что существуют профессиональные оптические приборы, например военного назначения, с так называемой просветленной оптикой. Их отличительной особенностью является то, что на поверхность стекла входного объектива нанесена специальная пленка, толщина которой подобрана таким образом, чтобы лучи света, отраженные пленкой и стеклом, взаимно компенсировались, исключая появление бликов. Приборы с просветленной оптикой имеют характерный темный цвет входных линз объектива.

Хорошей защитой от бликов может служить и бленда – специальный козырек в виде раструба, надеваемого на объектив оптического прибора. Она, во–первых, предотвращает попадание прямых солнечных лучей на вход объектива, а, во-вторых, существенно ослабляет переотражение лучей за счет специальной формы внутренней поверхности (см. рис. 65).

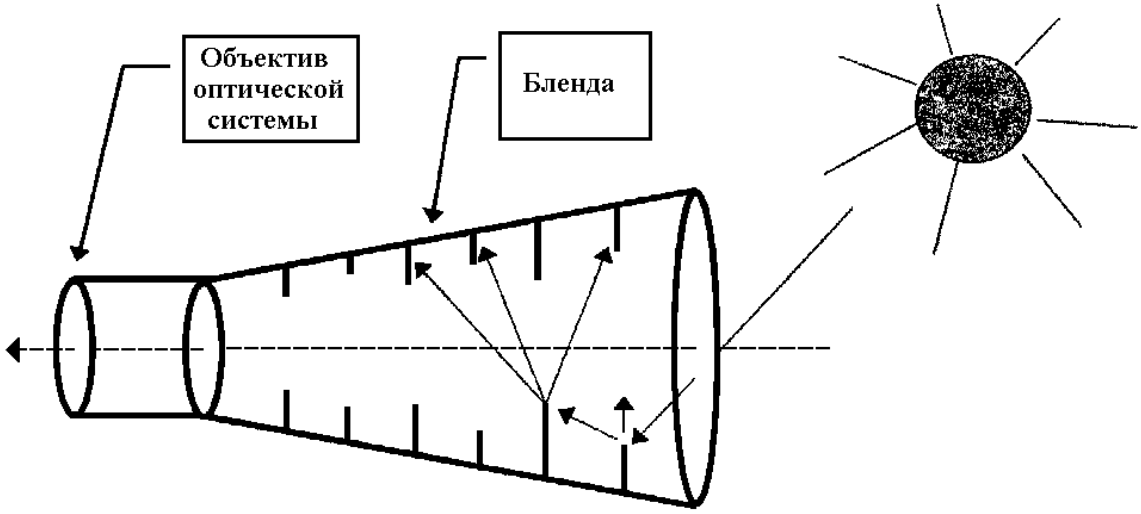

Рис. 65. Устройство защиты оптической системы от солнечных бликов

Примеры современных оптико-механических приборов приведены на рис. 66-68.

Рис. 66. Полевой бинокль с 20-кратным увеличением

Рис. 67. Бинокль фирмы Pentax с 10- кратным увеличением

Рис. 68. Монокуляр фирмы Pentax с 8-кратным увеличением

5.2. Приборы ночного видения

Рассмотренные выше оптико-механические приборы позволяют вести наблюдение при освещенности, близкой к нормальной (в светлое время суток), и при удовлетворительных погодных условиях (ясно или слабая дымка).

Естественно, что в жизни возникают ситуации, когда условия наблюдения затруднены – это вечернее или ночное время суток, чердаки, подвалы и т. п. В этих условиях неоценимую услугу могут оказать так называемые приборы ночного видения и тепловизоры, работающие в ближнем инфракрасном (ИК) диапазоне длин волн ($\lambda = 0{,}8–1{,}0$ мкм).

Основное отличие между первыми и вторыми заключается в том, что тепловизоры реагируют на температурный контраст и поэтому принципиально не работают без охлаждения оптического приемника. Именно это обстоятельство говорит за то, что применение тепловизоров в интересах промышленного шпионажа маловероятно потому, что при таком целевом назначении они дают преимущества незначительные, а по массогабаритным характеристикам существенно уступают приборам ночного видения. Так, например, пе-

реносной тепловизор **Д-4** имеет габариты 195×212×260 мм и массу 3,4 кг, аналогичные характеристики и у прибора **ТМ-100**. Это, примерно, в 4–10 раз больше, чем у приборов ночного видения, а «легкий и компактный» тепловизионный датчик **V3900** (GEC-Masrconi Ltd – Великобритания), вообще имеет массу около 32 кг.

Главными достоинствами приборов ночного видения являются:

- возможность наблюдения объекта в полной темноте или в условиях слабой освещенности;
- меньшее по сравнению с видимой областью спектра затухание электромагнитных волн ИК-диапазона в осадках.

К недостаткам приборов следует отнести:

- значительно худшую разрешающую способность, связанную с большой длиной волны (человека, например, можно опознать только по силуэту, так как черты лица не распознаются);
- нечувствительность человеческого глаза к ИК-излучению.

Для того чтобы объединить достоинства оптико-механических приборов и ИК-приборов и устранить (уменьшить) недостатки последних приборы ночного видения строятся по схеме, изображенной на рис. 69.

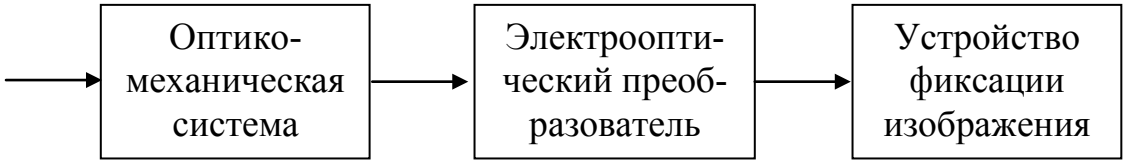

Рис. 69. Структурная схема прибора ночного видения

Здесь оптико-механическая система аналогична рассмотренным выше оптико-механическим приборам, и именно она определяет такие характеристики прибора, как мгновенный угол поля зрения и кратность увеличения.

Электрооптический преобразователь преобразует ИК-излучение в видимое, выводя его на небольшой встроенный экран. Эта часть устройства принципиально не работает без источника электрического питания, что можно отнести к еще одному из недостатков приборов ночного видения. В качестве устройства фиксации изображения обычно выступает человеческий глаз или фотоаппарат.

Приборы ночного видения могут работать как в *пассивном*, так и в *активном* режиме. Пассивный режим применяется при наличии собственного излучения объекта наблюдения и в условиях слабого рассеянного излучения случайных искусственных или естественных источников, уровень которого превышает 10^{-5} лк. Активный режим используется в условиях полного отсутствия освещения. Он сопровождается применением источника подсветки

объекта наблюдения. Таким источником может быть лазер, например полупроводниковый или на стекле с неодимом, или специальный ИК-прожектор. Прожекторы с мощностью излучения до 100–120 Вт функционируют, как правило, от автономных источников с напряжением питания 12 В. Диапазон расстояний, подсвечиваемых такими прожекторами, варьируется в диапазоне 10–110 м, в зависимости от мощности источника и ширины луча, вид последнего формируется специальными насадками.

Внешний вид приборов ночного видения и источников подсветки

Внешний вид приборов ночного видения и источников подсветки приведены на рис. 70–76.

Рис. 70.
Монокуляр RETRON RN-M02

Рис. 71.
Бинокуляр RETRON RN-B03

Рис. 72. Активный ночной наблюдательный прибор с импульсной лазерной подсветкой

Рис. 73. Очки ночного видения OR11

Рис. 74. Лазерный источник излучения фирмы Dedal

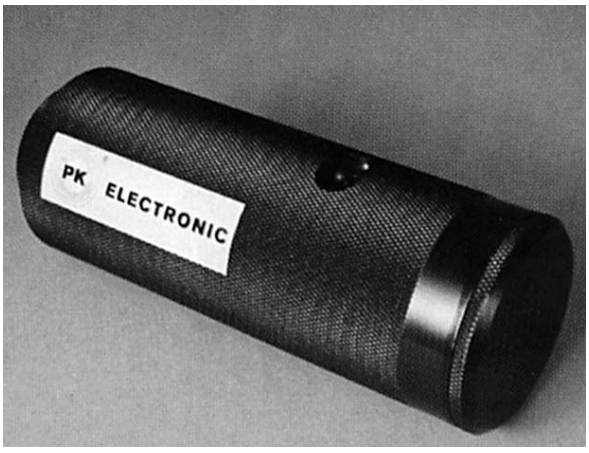

Рис. 75. Инфракрасный лазерный осветительный прибор РК-765

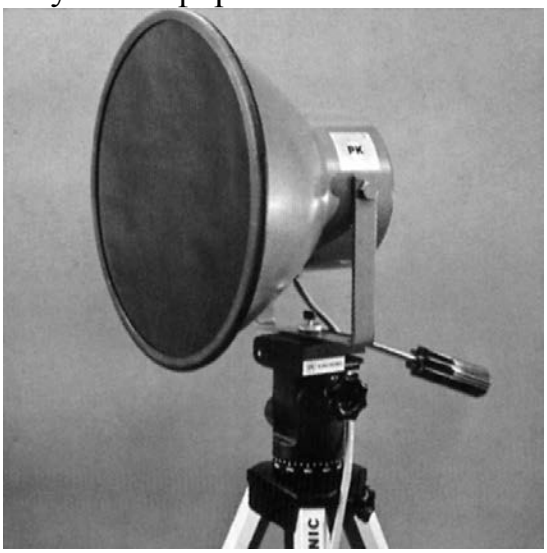

Рис. 76. ИК-прожектор РК-325

Технические характеристики приборов ночного видения

Приведём технические характеристики ряда приборов ночного видения:

РК300 – прибор ночного видения, предназначенный для получения фотоснимков на стандартную пленку 35 мм. Применяется с объективами, имеющими фокусное расстояние 75 мм (светосила – F 1,4), фокусное расстояние – 135 мм (светосила – F 1,8) или 180 мм (светосила – F 2,8), угол зрения – 13,7°. Габариты: диаметр – 75 мм, длина – 350 мм; вес – 1,9 кг. Для фиксации изображения может комплексироваться с фотоаппаратом или видеокамерой.

РК1260-S – прибор ночного видения, предназначенный для получения фотоснимков объектов, находящихся на расстоянии до 10 км. Использует обычную фотопленку 35 мм.

РК1245 – прибор для наблюдения удаленных объектов в условиях слабой освещенности (до 10^{-5} лк), фокусное расстояние объектива – 25 мм, светосила – F 1,4, угол зрения – 40°. Напряжение питания – 6,75 В, время непрерывной работы – 20 часов. Вес – 980 г. Выполнен в виде бинокля; **РК1245-S** – в виде шлем-маски.

РК305 – прибор ночного видения активного типа, предназначенный для наблюдения объектов в условиях полного отсутствия освещенности. Имеет объектив с фокусным расстоянием 135 мм и светосилой объектива F 2,8. ИК-прожектор имеет мощность 35 Вт и обеспечивает дальность наблюдения до 350 м. Собственный источник питания с напряжением 8 В обеспечивает время непрерывной работы 1,5 часа. Габариты прибора – 250×280×80 мм, вес – 1,3 кг.

Dedal-220 – монокулярный прибор ночного видения с угловым полем зрения прибора 28° в вертикальной и горизонтальной области. Диаметр объектива – 37 мм, светосила – F 1,0, кратность увеличения – 1,3. Усиление яркости изображения, создаваемое прибором, достигает 30 000. Габаритные размеры – 122×58×58, вес – 8 кг. Время непрерывной работы – 40 часов.

Dedal-040 – прибор ночного видения, выпускаемый как в монокулярном, так и бинокулярном исполнении. Угловое поле зрения прибора в зависимости от конструктивного исполнения лежит в диапазоне 14°-17°. Диаметр объектива – 85–100 мм, светосила – F 1,5-F 2,0, кратность увеличения – 1,9-3,2. Усиление яркости изображения, создаваемое прибором, достигает 50 000. Габаритные размеры монокуляра – 210×76×93, бинокуляра – 325×76×103 мм, вес, соответственно, 1,12 и 1,52 кг. Время непрерывной работы – 50 часов.

Spylux – прибор ночного видения индивидуального применения. Заключен в прочный и компактный корпус, дает высококонтрастное изображение с хорошим разрешением при низких уровнях освещенности. Прибор име-

ет окуляр с регулированием фокусировки, кнопку включения–выключения и держатель объектива типа **C** с адаптером, дающим возможность менять объектив в соответствии с условиями наблюдения. Стандартно прибор поставляется с объективом диаметром 75 мм и светосилой F 1,4. Масса прибора – 0,5 кг, напряжение питания – 2,0-5,0 В, потребляемый ток – 16 мА.

EEV Nite-Watch Plus – самый компактный и легкий из приборов ночного видения фирмы EEV (Великобритания). Его масса (с объективом и батареей) составляет 330 г, габаритные размеры – диаметр 46×120 мм. Его легко спрятать в кармане. Прибор может комплексироваться через адаптеры с различными кино-, фото- и видеокамерами. Усиление яркости в приборе составляет не менее 20 000. Продолжительность непрерывной работы от одной батареи – 3 часа. Источник питания – литиевый элемент типа DL1/3N с напряжением 2,5-3,5 В. Потребляемый ток – 18 мА.

EEV Black Watch – прибор, специально разработанный для таких применений, как скрытое фотографирование и видеонаблюдение. Усиление яркости изображения, создаваемое прибором, достигает 2 000 000, что позволяет получать высококачественные фотографии в самых неблагоприятных условиях.

Источники ИК-подсветки

PK765 – ИК-лазер с длиной волны 0,85 мкм и мощностью излучения в импульсе 180 мВт. Имеет форму цилиндра диаметром 65 мм и длиной 200 мм, напряжение питания – 12 В.

IL-7/LR – лазерный ИК-прибор подсветки, предназначенный для использования с приборами ночного видения при очень низких уровнях освещенности. Расходимость пучка регулируется от интенсивного карандашного пучка для точечной подсветки до пучка с расходимостью 40°. Масса прибора – 130 г с батареей электропитания, габариты – 63×50×20 мм. Длина волны излучения – 0,83 мкм, минимальная выходная мощность – 15 мВт. Электропитание – батарея литиевых элементов типа AA с напряжением 3,5 В. Продолжительность непрерывной работы – 5-20 часов.

PK1420-S – ИК-прожектор, предназначенный для подсветки фотографируемого объекта ИК-лучами. Дальность подсветки – 10-100 м. Диаметр прибора – 130 мм, длина – 240 мм, вес – 720 г.

PK325 – ИК-прожектор, работающий в диапазоне длин волн 0,82-0,98 мкм. Мощность – 110 Вт, дальность подсветки достигает 500 м. Напряжение питания – 220/110/12 В. Габариты: диаметр – 260 мм, длина – 200 мм. Вес – 2 кг.

Minilight 500 – миниатюрный ИК-излучатель на основе галогенной дихроичной лампы. В зависимости от модификации мощность лампы может

быть 20 или 50 Вт. Напряжение питания – 12 В. ИК-фильтр, предназначенный для задержки видимого света, пропускает излучение с длиной волны 0,84 мкм. Размеры источника излучения – 65×65×115 мм, масса – 350 г.

AVS IR-1/48V – светодиодный ИК-излучатель с длиной волны излучения 0,88 мкм. Минимальная дальность подсветки – 70 м, расходимость пучка – 30°, потребляемая мощность – 48 Вт. Питание осуществляется от источника постоянного напряжения 10-14 В. Габаритные размеры – 160×160×100 мм.

При ведении наблюдения с использованием приборов ночного видения необходимо учитывать следующие факторы:

- оптимальная дальность ведения наблюдения составляет несколько десятков метров;
- в поле зрения прибора не должно быть ярких источников света, так как их излучение может «ослепить» прибор или даже вывести из строя;
- работать в активном режиме следует только в том случае, если точно известно, что объект наблюдения не использует приборы ночного видения, иначе вы будете им обнаружены.

5.3. Средства для проведения скрытой фотосъемки

Важным элементом промышленного шпионажа является получение документов, подтверждающих тот или иной вид деятельности конкурентов. При этом фотоматериалы могут быть незаменимы при решении задач документального подтверждения конфиденциальных встреч, факта посещения объектом наблюдения определенных мест, а также при анализе особенностей малознакомой, труднодоступной местности или при решении задач копирования текстовых документов, рисунков, схем, чертежей в условиях дефицита времени.

В зависимости от решаемых задач различают два вида фотосъемки: съемку объекта наблюдения и съемку документов.

Съемка объекта

Съемка объекта может осуществляться как с больших, так и с малых расстояний. С *больших* расстояний фотографирование осуществляется из специальных укрытий, расположенных на крышах домов, чердаках, в автомобилях, в помещениях с окнами, выходящими на участок местности, представляющей определенный интерес. Высококачественные снимки при этом могут быть получены, если правильно решены следующие задачи:

- выбор времени экспозиции и степени открытия диафрагмы;
- подбор объектива;
- определение точки производства фотосъемки.

Выбор времени экспозиции и степени открытия диафрагмы решаются достаточно просто при наличии фотоэкспонометра, определяющего величину светового потока, отраженного объектом и местными предметами. Прибор выдает несколько пар цифр, оптимальных для той *чувствительности пленки,* которая установлена в фотоаппарате. Для примера рассмотрим шесть комбинаций, представленных в табл. 9.

Таблица 9.

Время экспозиции, с	1/15	1/30	1/60	1/125	1/250	1/500
Диафрагменное число, k	16	11	8	5,6	4	2,8

Любая комбинация из приведенных в табл. 9 пар цифр (от 1/15 – 16 до 1/500 – 2,8) обеспечит один и тот же уровень светового потока, воздействующего на фотопленку. Однако конкретная пара должна выбираться, исходя из условий и задач съемки.

Так, при съемке движущихся объектов время экспозиции должно выбираться как можно меньше (например, 1/250 или 1/500 с) для того, чтобы уменьшить «смаз» изображения, вызванный перемещением объекта в момент съемки. При этом, как видно из приведенной ниже таблицы, степень открытия диафрагмы будет максимальна (диафрагменное число 4 или 2,8, соответственно). В свою очередь, это приведет к уменьшению глубины резкости изображения. Например, при съемке объективом Гелиос-44М (табл. 10) с расстояния R = 10 м и k = 2,8 обеспечивается приемлемая резкость изображений только в интервале дальностей от 8 м до 15 м. Все предметы и объекты, находящиеся за пределами этого интервала будут выглядеть расплывчатыми (нечеткими). Глубина резкости изображения будет тем выше, чем больше значение диафрагменного числа k.

Таблица 10.

Тип объектива	Диаметр апертуры, мм	Светосила	Фокусное расстояние (f), мм	Угол поля зрения, град
Гелиос-44М	29	F2	58	31
Уран-9	100	F2,5	250	54
Уран-12	200	F2,5	500	38
Уран-24	167	F3	500	46
Таир-16	111	F4,5	500	13
Таир-30	67	F4,5	300	22
Телемар-2	120	F6,3	750	30
Телемар-17	64	F6,3	400	30

Важное значение для получения высококачественных снимков имеет правильный выбор объектива. Так, если необходимо получить детальный снимок объекта, находящегося на значительном расстоянии, то следует применять специальные длиннофокусные объективы, например, «Уран», «Таир» или «Телемар».

Они позволяют обеспечить хорошую опознаваемость изображенного объекта при съемке с расстояния, достигающего величины, примерно равной половине фокусного расстояния оптической системы объектива, выраженного в метрах (R = 0,5×f [м]). Так как объективы с фокусным расстоянием f =400 мм и более оказываются достаточно громоздкими, то их часто строят по специальным многолинзовым схемам, позволяющим существенно уменьшить продольные габариты, примерно до значения $l = 0{,}2 \times \mathrm{f}$.

Однако рассмотренные выше объективы имеют малый угол поля зрения, а в ряде случаев возникает необходимость получения общего панорамного изображения какой-либо территории. Для этих целей следует применять специальные широкоугольные или сверхширокоугольные объективы с угловыми полями от 90° до 180°. Примеры таких объективов приведены в табл. 11.

Таблица 11.

Тип объектива	Диаметр апертуры, мм	Светосила	Фокусное расстояние (f), мм	Угол поля зрения, град
Русар-29	8,8	F9	70	120
Родина-26	6,7	F8,2	55	133
Орион-20	-	F4,5	-	130

Выбор типа фотоаппарата для осуществления вышеописанных видов съемки принципиального значения не имеет, лишь бы он позволял менять при необходимости объективы. Тем не менее предпочтительней использовать аппараты с так называемыми зеркальными объективами, у которых визирование (наведение) осуществляется непосредственно через оптическую систему объектива. Здесь незаменимым может оказаться фотоаппарат марки «Зенит» практически любой модификации, имеющий хорошие показатели по параметру «качество–цена» (см. пример на рис. 77).

Определение точки съемки производится на основе комплексного анализа решаемой задачи, местных условий, возможностей аппаратуры и наличия естественных укрытий.

Рис. 77. Фотоаппарат для съёмки с больших расстояний
«Фотоснайпер» ФС-122

Тем не менее, два следующих правила надо помнить всегда:

- При проведении фотосъемки из помещения (или автомобиля) с закрытыми окнами стекла последних должны быть тщательно вымыты.
- Опасным демаскирующим признаком скрытой фотосъемки может быть появление солнечных бликов на стеклах объектива. Способы устранения бликов аналогичны тем, которые применяются при работе с оптико-механическими приборами.

Съемка объекта наблюдения может производиться и с *малых* расстояний, не превышающих нескольких метров. Естественно, что громоздким аппаратом как «Зенит» в таких условиях можно снимать только под видом туриста, фоторепортера и т. п. Однако это не всегда безопасно и может насторожить объект наблюдения, тем более он может запомнить «фотографа».

В этом случае целесообразно маскировать аппарат под одеждой, в сумке, папке или в другом малогабаритном предмете, который можно, не вызывая подозрений, держать в руках (см. рис. 78 – 80).

Естественно, что и фотоаппарат должен отвечать решаемым задачам, поэтому он должен быть наделен следующими функциями:

- иметь достаточно малые габариты и вес;
- иметь автоматическую перемотку кадров после каждого снимка;
- иметь автоматическую установку экспозиции;

- иметь автоматическую наводку на резкость.

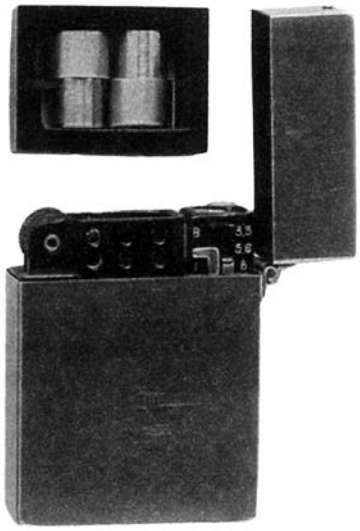

Рис. 78. Фотоаппарат в зажигалке

Рис. 79. Фотоаппарат в ручных часах

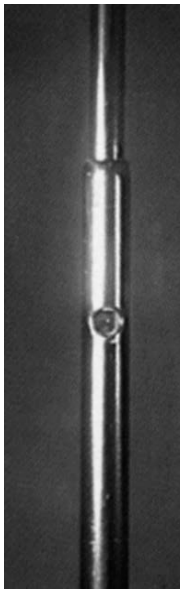

Рис. 80. Фотоаппарат в автомобильной антенне

На удивление полно этим требованиям отвечают широко распространенные в продаже аппараты, получившие в просторечии название «мыльница» за внешнее сходство с вышеназванным предметом (рис. 81). Их массогабаритные характеристики позволяют легко маскировать аппарат.

Рис. 81. Фотоаппарат «мыльница» AF-10 MINI фирмы Olympus

Эти аппараты идеально подходят для скрытой съёмки с малых расстояний. Благодаря встроенному электродвижку они обеспечивают производство повторных снимков с интервалом 2–3 с путем простого нажатия на кнопку пуска, а автоматическое наведение позволяет получать качественные снимки в интервале дальностей от 1,2 до 3,7 м. Тип фотоаппарата не имеет особого значения (Canon, Conica, Premier, Olympus), единственное условие – наличие функции отключения встроенной в аппарат фотовспышки.

Съемку можно производить как через специально проделанные в предметах камуфляжа отверстия (в сумке, папке), так и непосредственно через ткань легкой одежды (хлопок, шелк, ситец). Демаскирующими призна-

ками описанной съемки являются достаточно громкий щелчок фотоспуска и характерный звук работы мотора при перемотке пленки.

Съемка документов

Человеческая память обладает совершенно уникальным свойством со временем забывать то, что в нее попадает. Эта защитная функция организма спасает наш мозг от переполнения ненужными знаниями, освобождая место для новой полезной информации. К сожалению, участи забывания не избегают и полезные сведения, именно это и побудило в свое время людей изобрести письменность.

Записями в том или ином виде пользуются все, в том числе и ваши конкуренты, а получение этих записей или иных документов на бумажном носителе может иметь для вас стратегическое значение. Лучше всего, конечно, скрытно сделать копии этих документов, воспользовавшись, например сканером, факсом или ксероксом. Однако, вероятнее всего, этих удобных и полезных вещей в нужный момент под рукой у вас не окажется, и вы будете ограничены во времени. На выручку в такой ситуации может прийти старый хорошо зарекомендовавший себя способ – *репродукционная фотосъемка документов.*

Для ее производства пригоден практически любой фотоаппарат, позволяющий установить специальный репродукционный объектив, предназначенный для копирования документов (см. рис. 82-84).

Особенностью этих объективов является конструкция, позволяющая снимать документы с предельно малого расстояния (≥1 см), в то время как обычные короткофокусные объективы ограничивают минимальную дальность величиной 0,5–0,6 м, а при такой дистанции изображение получается мелким и труднораспознаваемым.

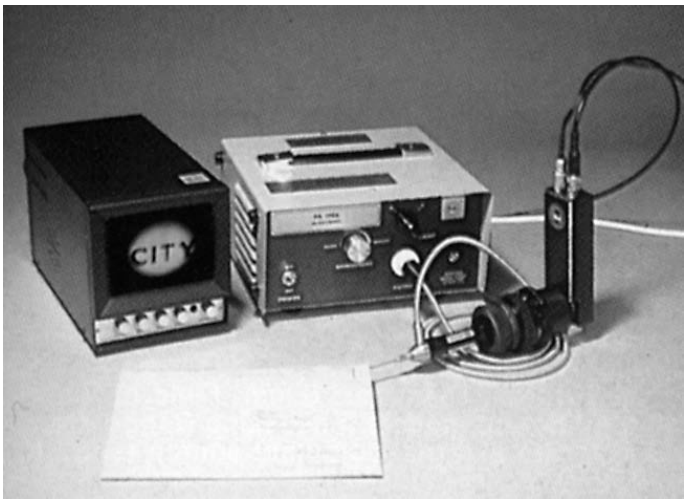

Рис. 84. Устройство для чтения, фотографирования или снятия на видеокамеру текстов (писем), запечатанных в конверты, РК1700.

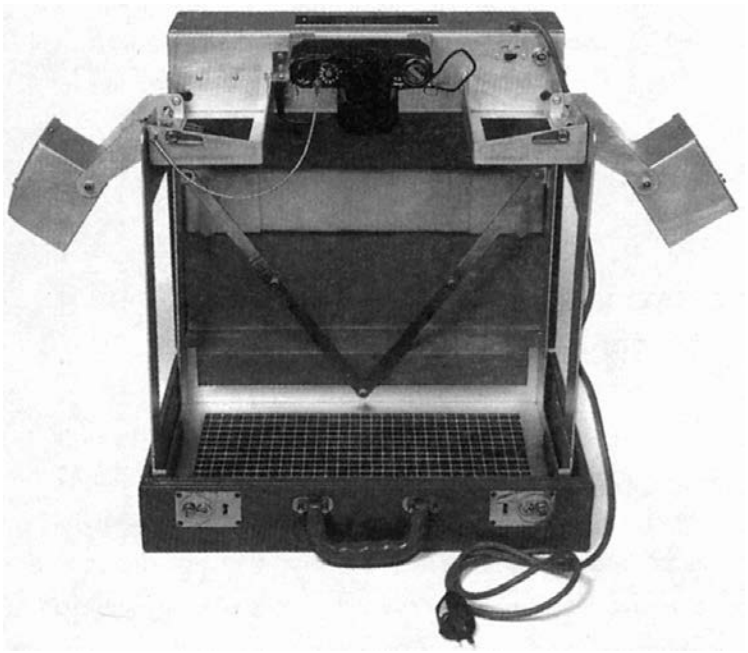

Рис. 85. Установка для репродукционной фотосъемки в атташе-кейсе с аппаратом фирмы Pentax

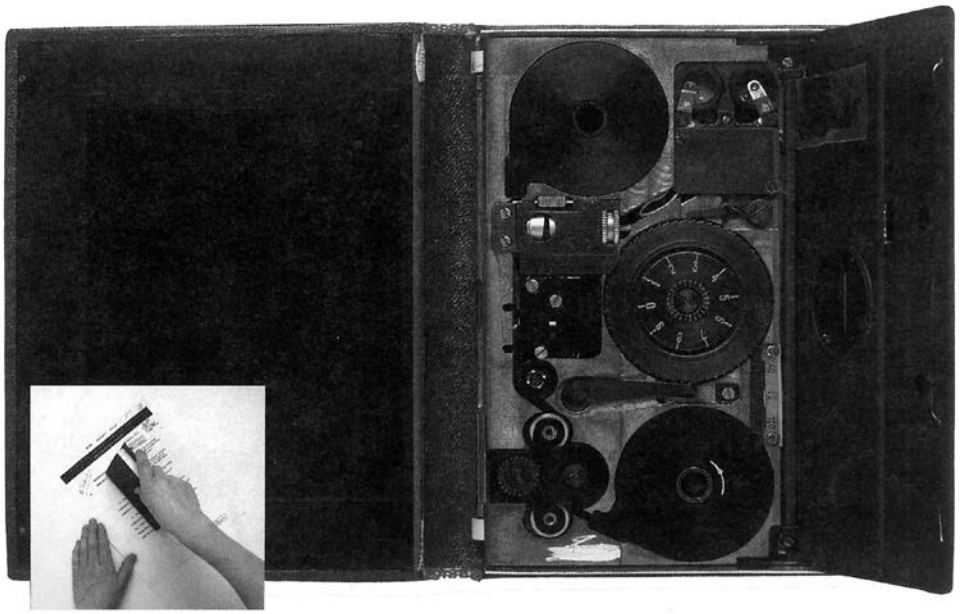

Рис. 86. Репродукционная фотокамера в записной книжке, работающая по принципу проката (сканирования) текста - специальные колесики на ребре переплета приводили в действие механизм камеры и включали встроенный источник света

Некоторые типы репродукционных объективов отечественного производства представлены в табл. 12.

Таблица 12.

Тип объектива	Диаметр апертуры, мм	Светосила	Фокусное расстояние, мм	Угол поля зрения, град
Гелиос-91	9	F4.5	40	19
Эра-5	7	F3.5-	25	26
Эра-7	38	F2,8	105	11
Эра-12	31	F4.0	125	16
Эра- 13	33	F4,5	150	17
Эра-14	48	F2,8	135	12
Эра- 15	28	F4,5	125	21
Маяк-1	36	F2,8	100	21

Следует отметить, что для указанных целей хорошо подходит уже упомянутый фотоаппарат «Зенит», так как он имеет зеркальную систему визирования (что важно для получения хорошей резкости изображения) и позволяет копировать документы не только с использованием репродукционных объективов, но и с помощью обычных короткофокусных, например, «Гелиос-44М» (см. табл. 10). Однако в этом случае необходимы специальные дополнительные кольца, устанавливаемые между фотоаппаратом и объективом.

К сожалению, выбор объектива не исчерпывает особенностей репродукционной съемки. Важное значение играет и подбор чувствительности фотопленки. С одной стороны, она должна быть достаточной для получения снимка в условиях естественной освещенности, а с другой – предельно малой. Так как, чем ниже чувствительность, тем меньше размер «зерна» фоточувствительного слоя и, следовательно, выше разрешение пленки (меньше размер фиксируемых деталей). Лучше всего для этих целей подходит фотопленка с чувствительностью по ГОСТу от 8 до 22 единиц.

Особо следует остановиться на новом типе аппаратов, обладающими удивительно широкими возможностями. Это цифровые аппараты – digital cameras (рис. 87, 88), фиксирующие изображение не на фотопленку, а в память, в виде, удобном для хранения, просмотра и обработки на персональном компьютере (форматы BMP, JPEG, TIFF).

Объем внутренней памяти аппарата может достигать 4 MB. Этого вполне достаточно для производства примерно 190 снимков с нормальным уровнем разрешения. Перенос необходимых кадров на персональный компьютер осуществляется по специальному кабелю.

Скрытая съемка объекта наблюдения цифровым аппаратом в режиме автоматической установки параметров может осуществляться на дистанции от 0,6 м до ∞, а оптимальная дальность лежит в пределах от 0,6 до 3,0 м.

Рис. 87. Цифровая камера RC 600 фирмы YASHICA

Рис. 88. Цифровая камера Dimage V фирмы Minolta

Частота производства снимков 0,5 – 5 с, и при этом полностью отсутствует демаскирующий фактор, связанный с работой мотора при перемотке пленки в камере.

Уникальность цифрового аппарата заключается и в том, что он пригоден для получения репродукционных снимков (пересъемки документов), так как позволяет в режиме ручных регулировок снимать на расстоянии 0,01 – 0,6 м. Специальные мини-дисплеи, установленные на некоторых типах камер (например, Philips ESP-2), дают возможность контролировать качество получаемых изображений и оперативно менять параметры съемки. Более подробно технические характеристики ряда аппаратов, предназначенных для негласной фотосъемки, приведены ниже.

PK420 – специальная фотокамера, вмонтированная в электронные часы с жидкокристаллическим дисплеем (ЖКД), секундомером и будильником. Диаметр часов – 34 мм, толщина – 10 мм, вес – 70 г. Фотопленка представлена в виде кассеты из 7 кадров. В каждом кадре пленка имеет свою чувствительность в диапазоне от 15 DIN (ASA 25) до 22 DIN (ASA 125) для обеспечения съемки в различных условиях освещенности. Фиксиро-

ванное фокусное расстояние обеспечивает диапазон дальностей производства фотосъемки от 1 м до бесконечности. Негатив диаметром 5,5 мм позволяет получать фотоснимки хорошего качества размером 9×9 см.

РК415 – мини-фотокамера для репродукционной съемки и съемки на расстоянии на дальностях от 1м до бесконечности. Фиксированное фокусное расстояние объектива – 15 мм, светосила – F 5,6. Автоматическая регулировка времени экспозиции от 1/500 с до 8 с позволяет осуществлять фотосъемку в широком диапазоне уровня освещенности на пленку с чувствительностью от 15 DIN (ASA 25) до 27 DIN (ASA 400). Емкость кассеты – 12, 24 или 36 кадров. Размеры аппарата – 30×18×80 мм, вес – 50 г.

РК1570-SS – мини-фотокамера, закамуфлированная под зажигалку. Имеет объектив с фокусным расстоянием 12,5 мм и светосилой F 2,5. Позволяет использовать кассеты с 12, 24 и 36 кадрами, размер получаемого негатива – 8×11 мм. Фиксированное время экспозиции – 1/125 с. Размеры камеры – 26×16×110 мм, вес – 70.

РК335-SS – представляет из себя бинокль 9×30 мм с углом зрения 7°10ŕ, совмещенный с фотоаппаратом, объектив которого имеет фокусное расстояние 300 мм и светосилу – F 5,6. Идеально подходит для наблюдения и фиксации событий. Габариты прибора – 208×140×129 мм, вес – 1,8 кг. Размер получаемого негатива – 24×36 мм.

РК1565 – специальный фотоаппарат с объективом Pin Hole («игольное ушко»). Позволяет делать снимки через отверстия предельно малого диаметра без ухудшения качества изображения. Диаметр апертуры объектива – 3 мм, фокусное расстояние – 9 мм, угол зрения – 40°. Длина объектива – 120 мм, вес – 150 г.

РК340-S – автоматическая фотокамера, закамуфлированная под сумку-несессер, диапазон изменения времени экспозиции – от 1/750 до1 с. Светосила объектива – F 2,8, количество кадров – 110, вес – 360 г.

РК1690 – фотокамера с объективом Pin Hole, установленная в атташе-кейсе. Установка параметров экспозиции – полностью автоматическая, размеры кадра – 24×36 мм. **РК1690-S** дополнительно снабжена радиоканалом дистанционного управления съемкой.

РК335 – камера, закамуфлированная под папку-скоросшиватель. Полностью автоматическая. Количество кадров – 36.

РК1780 – стандартная автомобильная антенна с 5-мм встроенным объективом, снабжена поворотным устройством вокруг вертикальной оси. Изображение фиксируется на фотоаппарат с автоматической регулировкой фокусного расстояния и времени экспозиции. **РК1780-S** – то же устройство, но снабженное видеокамерой **РК5105** для прямой видеозаписи наблюдаемого изображения либо передачи его на дальность до 3 км. Мощность передатчика

видеосигнала – 1,5 или 10 Вт. **РК11930** или **РК1935** – специальные устройства для приема видеосигналов. Первый имеет размер экрана по диагонали – 23 мм, габариты – 83×167×49 мм, вес – 460 г и работает от автономного источника питания, второй имеет экран с диагональю 50 мм, габариты – 190×470×412 мм, вес – 4,4 кг и питается от сети 110/220 В.

РК1700 – устройство для чтения, фотографирования или снятия на видеокамеру **РК5105** текстов (писем), запечатанных в конверты. Представляет из себя специальный эндоскоп длиной 170 с мм фиксированным фокусным расстоянием и углом зрения 70°, его диаметр равен 1,7 мм. Устройство вводится в нераспечатанный конверт и перемещается вдоль текста, который можно прочесть, например, на экране монитора (23 см по диагонали). В устройство входит и специальный источник подсветки **РК1765** с напряжением питания 220 В и мощностью 150 Вт.

5.4. Технические средства получения видеоинформации

Наиболее совершенным способом получения конфиденциальной информации является скрытое телевизионное или видеонаблюдение. Применение специальных миниатюрных камер позволяет сделать это наблюдение абсолютно незаметным, информативным и безопасным.

Однако по своей структуре телевизионные камеры более сложны, чем рассмотренные выше приборы ночного видения. Это связано с необходимостью разложения получаемого изображения на составные части для их передачи к месту регистрации и последующего восстановления передаваемого изображения (дословно *телевидение* – это видение на расстоянии). В общем случае структурная схема телевизионной камеры имеет вид, показанный на рис. 89.

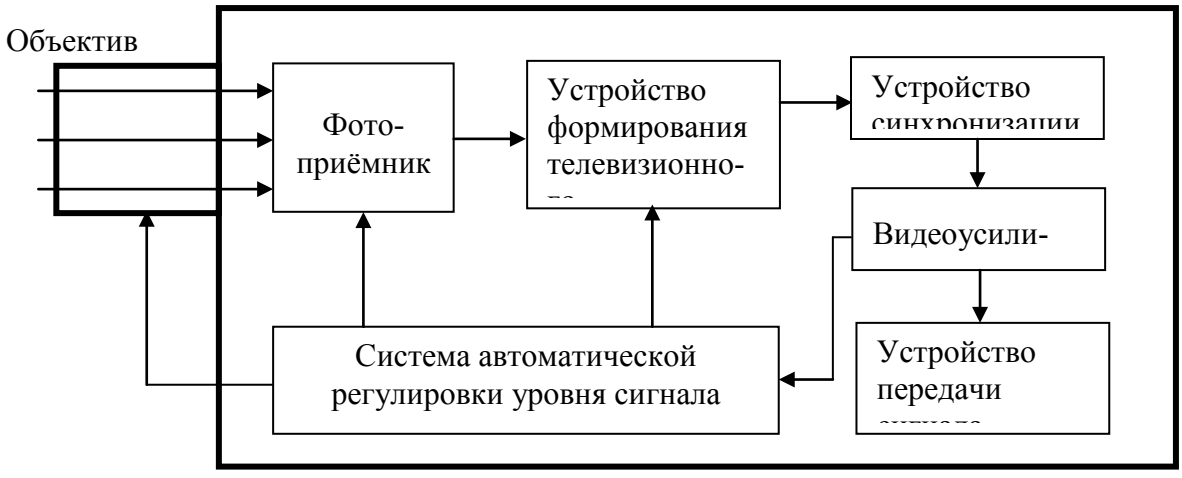

Рис. 89. Основные компоненты телевизионной камеры

Здесь *объектив* играет такую же роль, как и в рассмотренных выше оптических приборах, но конструкция его сложнее из-за необходимости решения задачи автоматической регулировки диафрагмы в зависимости от уровня освещенности объекта наблюдения. Характеристики некоторых современных телевизионных оптических систем приведены в табл. 13. В ряде стран существуют два типа стандартных конструкций узлов крепление объективов: тип «С» и тип «CS». Тип «С» имеет резьбу 2,54×0,8 и расстояние до опор ной плоскости ПЗС-матрицы 17,5 мм, тип «CS» имеет резьбу 2,54×0,8 и расстояние до опорной плоскости матрицы 12,5 мм. Объективы с узлом крепления типа «С» нельзя заменять типом «CS», так как матрица окажется не в фокусе объектива и изображение получится нечетким. В то же время объективы с «CS» можно использовать вместо объективов типа «С» при наличии специального адаптера (переходного кольца).

Таблица 13.

Тип объектива	Диаметр апертуры, мм	Светосила	Фокусное расстояние, мм	Угол поля зрения, град	Установочная резьба
iVi-1,0	14	F1.8	3,6	110	M12
iVi-2,0	13	Fl,8	4,1	90	M12
iVi-3,0	3,4	Fl,8	6,6	50	M12
iVi-4,0	4,6	Fl,6	7,7	40	M12
iVi-7,0	1,2	F2.8	3,5	110	-
iVi-10	6,5	F2,8	19,5	16	
HS3 166-X	3,7	F 1,6-64	-	-	CS/АРД
HS4 166-X	4,2	F 1,6-64	-	-	CS/АРД
HS614 HX	2,6	F 1,6-300	-	-	CS/АРД

Фотоприемник предназначен для преобразования светового потока, отраженного объектом в электрические сигналы. В подавляющем большинстве современных телевизионных камер для этих целей используют так называемые, ПЗС-матрицы.

Устройство формирования сигнала, устройство синхронизации и видеоусилитель обеспечивают формирование полного телевизионного сигнала заданной структуры и амплитуды.

Система автоматической регулировки уровня сигнала, управляя электронной диафрагмой объектива (АРД), временем накопления электронного заряда в ПЗС-матрице (временем срабатывания электронного затвора) и параметрами усиления, поддерживает выходной видеосигнал в заданных пределах при изменении условий освещенности.

Некоторые камеры дополнительно оснащены функцией компенсации заднего света (КЗС), которая устанавливает указанные параметры по некоторому фрагменту изображения (как правило, по центру). Она может оказаться незаменима при работе в условиях с большим перепадом освещенности или при съемке в условиях, когда в поле зрения аппарата вместе с объектом попадает яркий источник света. Например, если ведется наблюдение в затененном помещении за входящими с улицы посетителями, то в яркий солнечный день на экране видеоконтрольного устройства вместо четкого изображения входящего может оказаться только темный силуэт. Достоинство функции КЗС заключается в том, что она настраивает камеру именно по слабоосвещенному объекту в центре, обеспечивая его четкое изображение.

Устройство передачи сигнала – это радиопередатчик, аналогичный применяемым в радиозакладных устройствах, полупроводниковый лазер или электрический кабель в зависимости от способа применения телевизионной системы наблюдения.

Современные телевизионные камеры характеризуются большим числом различных параметров, однако, с точки зрения скрытого наблюдения, наибольший интерес представляют следующие:

- мгновенный угол поля зрения;
- разрешающая способность;
- чувствительность телевизионной камеры.

Мгновенный угол поля зрения полностью определяется конструкцией оптической системы. Его значения для различных типов объективов приведены в табл. 13.

Разрешающая способность включает в себя два понятия: разрешающую способность объектива и разрешающую способность фотоприемника.

Разрешающая способность объектива, $\Delta\ell$ – это тот предел, к которому стремится любая система фиксации изображения. Она зависит от диаметра D, входного зрачка объектива и расстояния R от телекамеры до объекта наблюдения и соответствует минимальному линейному разносу двух точек на объекте, при котором они воспринимаются еще раздельно. Значение $\Delta\ell$ может быть определено из соотношения

$$\Delta\ell = 1{,}22\frac{\lambda}{D}R, \qquad (5.8)$$

где ℓ – среднее значение длины волны оптического излучения (для видимой области спектра 0,54 мкм, а для ИК-области – 0,9 мкм).

Разрешающая способность фотоприемника хуже (больше) разрешающей способности объектива, поэтому ее величина и определяет разрешение телевизионной системы в целом. Она зависит от числа чувствительных элементов ПЗС-матрицы (пикселей), из выходных сигналов которых складыва-

ется изображение. Их число обычно лежит в пределах от 270 000 до 440 000. Чем больше число пикселей в матрице, тем больше дискретных точек образует изображение, тем выше его четкость и качество. Однако на практике часто пользуются не понятием «число чувствительных элементов матрицы», а апеллируют к однозначно связанной с ней характеристике – максимальному количеству переходов от черного к белому и обратно. Она называется числом телевизионных линий и указывается, как правило, только по горизонтали.

Некоторые фирмы в технических характеристиках на свои телевизионные камеры дополнительно указывают размер матрицы оптического приемника. В большинстве представляемых на российском рынке камерах используются датчики изображения (матрицы) с размером: 1 дюйм; 2/3 дюйма; 1/2 дюйма; 1/3 дюйма; 1/4 дюйма. Последние, как правило, применяются только в сверхминиатюрных камерах, используемых для скрытого наблюдения.

По *чувствительности* к уровню освещенности телевизионные камеры делятся на пять классов:

- I – камеры, которые могут работать только при нормальном дневном освещении (при уровне освещенности E ≈ 50 лк).
- II – камеры, способные работать при низкой освещенности вплоть до наступления сумерек (E ≈ 4 лк).
- III – камеры, предназначенные для работы при лунном свете, соответствующем уровню освещенности от четверти луны в безоблачную ночь (E ≈ 0,1-0,4 лк).
- IV – камеры, способные работать при уровне освещенности, создаваемой безлунным звездным небом в безоблачную ночь (E ≈ 0,0007-0,002 лк).
- V – камеры, предназначенные для работы с дополнительными источниками ИК-излучения в условиях полного отсутствия видимого излучения.

Следует еще раз обратить внимание на то, что телевизионные камеры, предназначенные для работы в условиях низкого уровня освещенности отличаются от приборов ночного видения более сложным представлением сигнала. Это связано с необходимостью передачи его на расстояние, в то время как приборы ночного видения позволяют только фиксировать информацию, например, глазом или фотоаппаратом.

Выбирая класс телевизионной камеры, необходимо знать, что чувствительность E ее телевизионного приемника должна отвечать условию

$$E \le E_o \times R \times K, \qquad (5.9)$$

где E_O – общий уровень освещенности в зоне нахождения объекта наблюдения [лк]; R – коэффициент отражения объекта наблюдения; K – коэффициент

пропускания объектива камеры. Значения параметров R и K приведены в табл. 14 и 15. Зависимость уровня освещенности E_o от времени суток и состояния атмосферы представлена на рис. 90.

Таблица 14.

Отражающая поверхность	Коэффициент отражения, R
Кожа человека	0,15-0,25
Ткань серого цвета	0,2-0,6
Ткань желто-коричневого цвета	0,3-0,4
Ткань ярко-голубого цвета	0,35-0,6
Ткань ярко-зеленого цвета	0,5-0,75
Ткань желтого цвета	0,6-0,75
Ткань цвета слоновой кости	0,75-0,8
Ткань грязно-белого цвета	0,75-0,85
Ткань белого цвета	0,8-0,9

Таблица 15.

Светосила объектива	Относительное отверстие объектива	Коэффициент пропускания
F 0,8	1.0,8	0,31
F 0,95	1:0,95	0,2
F 1,2	1:1,2	0,14
F 1,4	1:1,4	0,1
F 2,0	1:2,0	0,05
F 2,8	1:2,8	0,025
F 4,0	1:4,0	0,0125
F 5,6	1-5,6	0,00625
F 8,0	1:8,0	0,003125

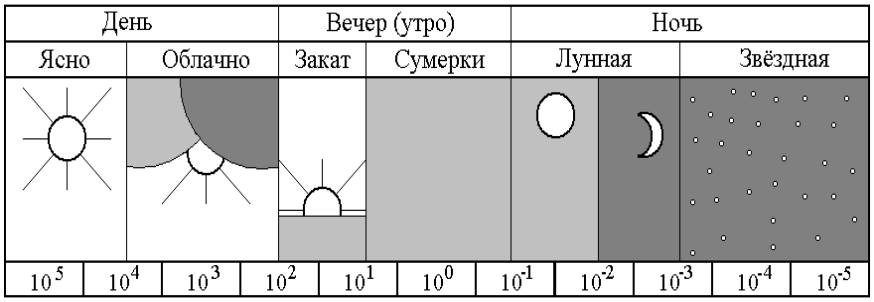

Рис. 90. Типовая зависимость уровня освещённости E_o [лк] от времени суток и состояния атмосферы

Для скрытой телевизионной (видео) съемки обычно используют малогабаритные камеры, которые могут быть выполнены как в обычном, так и закамуфлированном исполнении, например, в виде дверного «глазка» (см. рис. 91.).

Рис. 91. Видеокамера “дверной глазок” МВК-17(А)

Существует целое семейство малогабаритных бескорпусных телевизионных камер (см. рис. 92, 94), которые для осуществления наблюдения устанавливаются в элементы конструкций зданий, предметы интерьера помещений.

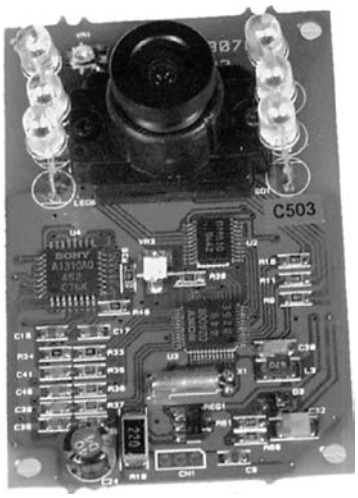

Рис. 92. Бескорпусная видеокамера С-503

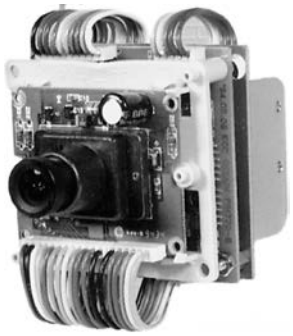

Рис. 93. Бескорпусная видеокамера С-770

Рис. 94. Бескорпусная видеокамера BHV-558Ex

Некоторые телевизионные камеры, например, **JT-241s** штатно оснащается следующими предметами камуфляжа:

- *элементы интерьера*: картина, мебель, цветочная ваза, статуэтка, светильник, электророзетка;
- *одежда и ее элементы*: куртка, костюм, заколка для галстука, пуговица, пряжка ремня;
- *носимые предметы*: кейс, сумка, радиоприемник, магнитофон.

Один из вариантов скрытой установки камеры **JT-241s** «за плоским укрытием» показан на рис. 95. Важным достоинством этой камеры является наличие специального передатчика телевизионного сигнала **JR-500**, позволяющего передавать изображение и звук на расстояние до 500 м. Передатчик работает в диапазоне дециметровых волн, имеет габариты 120×120×25 мм и массу 200 г. Питание – от элемента с напряжением 12 В. Предусмотрено закрытие передаваемой информации. Дополнительно камера оснащается выносным проводным микрофоном **JM-004** и оптико-волоконными жгутами для выне сения объектива, прожектором инфракрасной подсветки, диктофоном и видеомагнитофоном. В зависимости от комплектации эта камера может использоваться как носимое средство либо как закладное устройство.

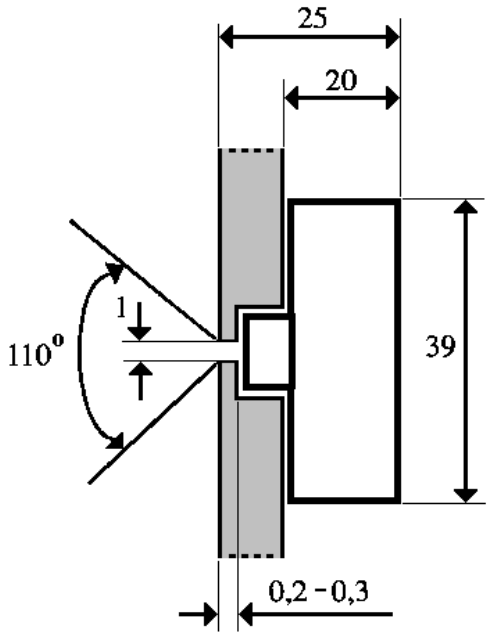

Рис. 95. Скрытая установка камеры **JT-241s**

С целью увеличения времени автономного функционирования в качестве закладки телевизионная камера может оснащаться приемником сигналов дистанционного управления. Время непрерывной работы в зависимости от комплектации и режима функционирования изменяется в пределах от 30 минут до 30 часов.

Для приема телевизионных и аудиосигналов от передатчика JR-500 применяется специальный приемник **JD-500**, обеспечивающий уверенный прием на указанной дальности – до 500 м. Основные технические характеристики телевизионной камеры JT-241s, а также некоторых других приведены в табл. 16.

Таблица 16.

Тип камеры (фирма - страна производитель)	Мин. освещенность, лк	Горизонтальное разрешение, телевизионных линий	Размер чувствительного элемента	Параметры объектива	Время срабатывания электронного затвора, с	Габариты, мм; масса, г; др. особенности
JT-241S (Тайвань)	0,04	400	1/3"	D =0,3-1,2 мм; F 2.8; θ =110°	1/100000	32×32×20 20 г
MYTHOS (Bisset - Франция, Ю. Корея)	0,3	380	1/3"	D = 4 мм; F 1.6	-	Аудиоканал
ПКС-504С (ЭВС-Россия)	0,08	380	1/3"	F l,4; CS	1/50-1/10000	-
ПКС-504Н (ЭВС-Россия)	0,005	380	1/3"	F 1.4; CS	1/50-1/10000	-
ПКС-754СМ (ЭВС-Россия)	0,05	380	1/3"	F l,4; CS	-	Аудиоканал
ДО-1 (ЭВС-Россия)	0,005	380	1/3"	F l,4; θ = 90°; CS	-	АРД
FC-65 (Computer – Япония)	0,3	380	1/3"	F l,4	1/50-1/100000	55×40×102
XC-41 (Computer – Япония)	10	320	1/3"	D = 4 мм; F 2,0	-	55×60×30 бескорп.
BHV-558Ex (Sony – Япония)	0.1	480	1/3"	D = 3,6 мм; F 1,4; θ = 70°	1 - 1/100000	38×38×25 бескорп.

6. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

6.1. Нежелательные излучения радиопередающих устройств систем связи и передачи информации

По своему функциональному назначению радиопередающие устройства формируют в определенной полосе частот радиочастотные сигналы, модулированные в соответствии с передаваемой информацией. Требования к ширине этой полосы определяются видом передаваемой информации, скоростью и качеством передачи. Минимальная полоса частот данного класса радиоизлучения, достаточная для передачи сигнала с требуемыми скоростью и качеством, называется необходимой полосой радиочастот [32]. Излучение радиопередающего устройства в необходимой полосе радиочастот, предназначенное для передачи сигнала, называется основным радиоизлучением.

Преобразование модулированных колебаний, формируемых передатчиком, в электромагнитное поле осуществляется в антенной системе радиоэлектронного средства. Наряду с основным излучением любое радиопередающее устройство осуществляет формирование в окружающем пространстве электромагнитных полей, соответствующих нежелательным радиоизлучениям. В соответствии с [32] к нежелательным радиоизлучениям радиопередающих устройств относят радиоизлучения за пределами необходимой полосы радиочастот. Эти излучения присущи любым радиопередающим устройствам. Они подразделяются на внеполосные, побочные и шумовые [9].

Нежелательные радиоизлучения в полосе частот, примыкающей к необходимой полосе радиочастот, являющиеся результатом модуляции, называются внеполосными излучениями. Такие излучения могут быть вызваны наличием нелинейностей в тракте формирования модулирующих сигналов, нелинейностей амплитудных и фазовых характеристик модулятора, применением модулирующих сигналов с большей шириной спектра, чем требуется для обеспечения нормальной работы, а также рядом других причин.

К побочным радиоизлучениям относятся нежелательные радиоизлучения, возникающие в результате любых нелинейных процессов в радиопередающем устройстве, кроме процесса модуляции. Различают побочные излучения на гармониках, субгармониках, паразитные, комбинационные и интермодуляционные. Эти виды излучений вызываются нелинейными процессами, имеющими место в передатчике, а также в фидере и антенне. В образовании интермодуляционных излучений, кроме того, принимают участие внешние электромагнитные поля, воздействующие на данное радиопередающее устройство [32].

Шумовое радиоизлучение радиопередающего устройства — нежелательное радиоизлучение, обусловленное собственными шумами и паразитной модуляцией генерируемого колебания шумовыми процессами радиопередатчика.

Нежелательные радиоизлучения передающих устройств систем информатизации и связи могут содержать передаваемую в радиолинии информацию вследствие их модуляции информационными сигналами. Излучение в окружающее пространство таких нежелательных электромагнитных полей создает дополнительную опасность утечки информации.

Необходимо отметить, что любая антенная система обладает наряду с основным лепестком своей диаграммы направленности боковыми и задними лепестками на основной частоте, а также диаграммами направленности на частотах нежелательных излучений. Вид этих диаграмм направленности зависит от типа антенны, частоты излучения, условий размещения и т.д., а уровни их боковых и задних лепестков могут быть достаточно высокими. Вследствие этого в различных направлениях окружающего пространства осуществляется излучение электромагнитных полей на частотах основного и нежелательных излучений, которые могут распространяться на значительные расстояния.

6.2. Нежелательные излучения технических средств обработки информации

Технические средства, не являющиеся радиопередающими устройствами, также могут быть источниками нежелательных электромагнитных излучений. Излучения таких технических средств обработки информации называются побочными электромагнитными излучениями. Существуют различные причины возникновения побочных излучений. В цепях различных устройств протекают переменные электрические токи, порождающие электромагнитные поля, излучаемые в окружающее пространство. Структура и параметры электромагнитных полей, создаваемых токоведущими элементами, определяются конструктивными особенностями систем и средств информатизации и связи, а также условиями их размещения и эксплуатации. Такие электромагнитные излучения, например излучения, возникающие при работе ПЭВМ (излучения дисплея, усилителей записи и считывания, кабельных соединений и т.д.), являются потенциальными носителями опасного сигнала.

Технические средства различного назначения могут иметь в своем составе устройства, которые для выполнения своих основных функций генерируют электромагнитные колебания (эталонные и измерительные генераторы, генераторы тактовых частот, генераторы развертки электронно-лучевых трубок, гетеродины радиоприемных устройств и т.д.).

В отдельных технических средствах, например в усилительных каскадах, могут возникать паразитные излучения, обусловленные их самовозбуждением за счет паразитных положительных обратных связей. Причины возникновения нежелательных обратных связей в усилителях могут быть различными. Параметры элементов радиоэлектронной аппаратуры — конденсаторов, резисторов, катушек

индуктивности, отрезков соединительных линий — вне полосы рабочих частот существенно отличаются от соответствующих параметров на рабочих частотах. Наличие конечной индуктивности выводов элементов, различных паразитных емкостей, проявление свойств цепей с распределенными параметрами, различные межэлементные соединения образуют большое количество паразитных колебательных систем и обратных связей, свойства которых невозможно предусмотреть и учесть заранее.

Причины возникновения нежелательных обратных связей в усилителях можно разделить на две группы [10]. Первая группа причин связана с наличием внутренних обратных связей через усилительный прибор (через проводимость обратного действия). Ко второй группе относят внешние обратные связи через паразитные индуктивности, емкости, цепи питания, регулировок и т.д. В многокаскадных усилителях существует большое количество каналов, по которым усиленное напряжение может поступать из точек с большим уровнем напряжения в точки с меньшим уровнем напряжения (рис. 96).

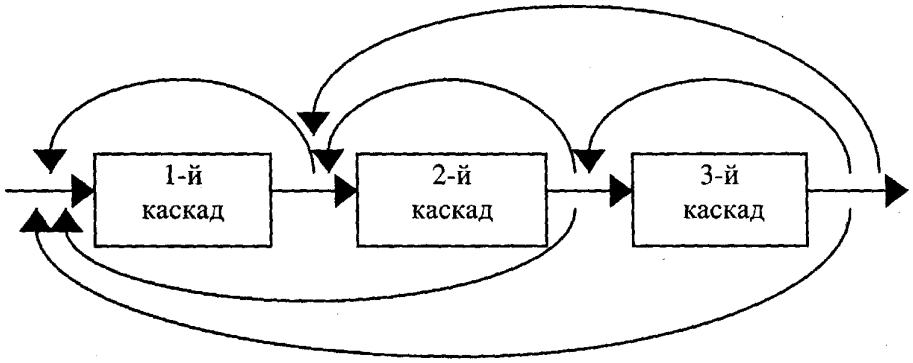

Рис. 96. Каналы утечки в многокаскадных усилителях

К таким каналам можно отнести все виды обратной связи между входной и выходной цепями, в пределах каждого отдельного каскада, в пределах двух, трех и более каскадов. Практически напряжение с выхода усилителя на его вход может передаваться в результате действия следующих основных видов внешних обратных связей:

1. Через емкость между выходной и входной цепями усилителя. Этот вид связи имеет место в тех случаях, когда провода входной цепи (см. рис. 97) проходят рядом с проводами выходной цепи (емкость C_1); когда отсутствуют экраны между каскадами или когда они недостаточно экранированы (емкость C_2); когда среди монтажных проводов имеются провода, не имеющие отношения к высокоточным цепям, но связанные с ними емкостями (емкости C_3 и C_4).

2. Через взаимоиндуктивности между выходным и входным контурами избирательного усилителя:

- через провода регулировок, подключенные к различным точкам усилительных каскадов;
- через провода питания активных элементов усилителя;
- через шасси и корпус усилителя, являющиеся общим проводом, соединяющим ряд его точек.

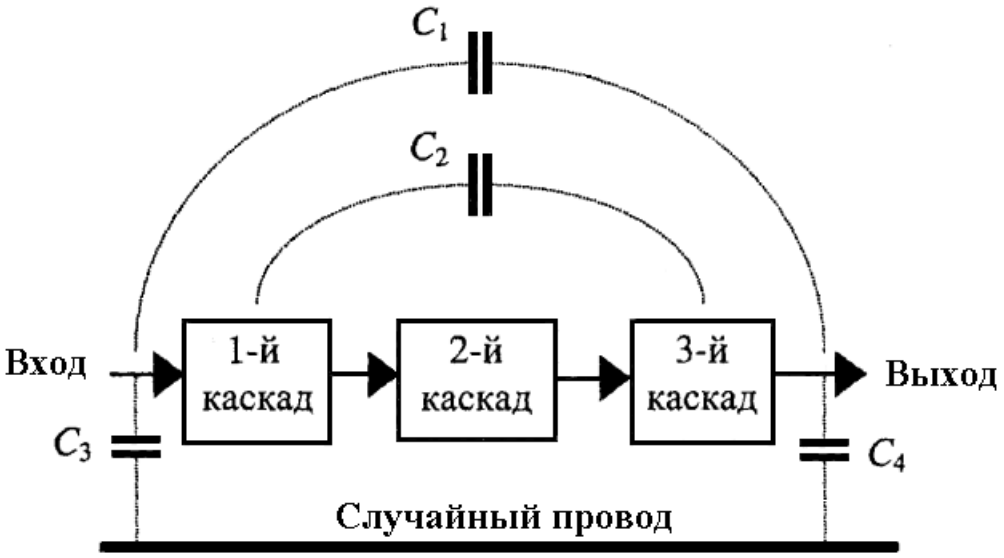

Рис. 97. Емкостные связи в усилителе

На какой-либо частоте нежелательная обратная связь может оказаться положительной, а условия самовозбуждения - выполненными. Это приводит к возникновению паразитной генерации устройства на этой частоте, предсказать которую заранее практически невозможно.

Причиной возникновения высокочастотных колебаний в транзисторных усилителях может стать их перегрузка за счет воздействия входного сигнала чрезмерно большого уровня. В этом случае нелинейность емкостей p-n переходов транзисторов приводит к параметрической генерации гармоник сигнала. Кроме того, при воздействии входных сигналов большого уровня может иметь место изменение внутренней обратной связи электронного прибора усилителя, что при определенных условиях вызывает его самовозбуждение.

В цифровых интегральных микросхемах в отличие от каскадов, выполненных на дискретных элементах, расстояния между элементами значительно меньше, а сами элементы расположены на подложке, проводимость которой выше проводимости воздуха. Это приводит к увеличению паразитных связей. В интегральных микросхемах возможна также паразитная генерация, возникающая из-за отражения сигнала от концов соединительных линий между этими микро-

схемами вследствие несогласованности сопротивлений источника и нагрузки с волновым сопротивлением соединительных линий.

Побочные излучения технических средств обработки информации могут иметь место в различных участках частотного диапазона. Низкочастотными излучателями электромагнитных колебаний являются, например, звукоусилительные устройства различного функционального назначения и конструктивного исполнения. На более высоких частотах наблюдаются излучения гетеродинов радиоприемных устройств, измерительных генераторов, генераторов тактовых частот электронно-вычислительной техники и т.д.

Нежелательные излучения различных устройств могут содержать опасные сигналы. В процессе функционирования технических средств обработки информации элементы" генераторов, усилителей и других излучающих электромагнитные поля устройств могут оказаться в зоне действия электромагнитных полей опасных сигналов. Воздействие электромагнитного поля опасного сигнала на рассматриваемые устройства может привести к изменению параметров отдельных элементов генератора или усилителя (например, крутизны S характеристики активного элемента, контурной емкости или индуктивности, емкостей p-n переходов транзисторов, сопротивления нагрузки каскада и т.п.). Результатом такого изменения является паразитная модуляция опасным сигналом нежелательных излучений технических средств. Вид и количественные параметры, характеризующие эту модуляцию, определяются конкретной ситуацией. Таким образом, внешнее воздействие электромагнитных полей опасных сигналов на элементы высокочастотных генераторов, усилителей и других технических средств может привести к амплитудной и угловой модуляции высокочастотных колебаний в этих устройствах. Следствием этого является появление в окружающем пространстве нежелательных излучений, модулированных опасными сигналами, т.е. создаются предпосылки для утечки информации, обрабатываемой техническими средствами.

6.3. Нежелательные электромагнитные связи

Между двумя электрическими цепями (элементами, узлами, средствами), находящимися на некотором расстоянии друг от друга, могут возникать нежелательные электромагнитные связи. Наличие таких связей приводит к тому, что сигналы, циркулирующие в одной цепи (в цепи источника наводки), появляются в другой электрической цепи (в цепи рецептора наводки). Основными путями возникновения нежелательных связей являются:

- ближнее электрическое поле;
- ближнее магнитное поле;
- электромагнитное поле излучения;
- соединительные провода, кабели и волноводы, цепи питания, заземления и другие токоведущие элементы и конструкции.

На малых расстояниях могут существовать все указанные виды нежелательной связи. С увеличением расстояния ослабляются и исчезают связи через ближнее электрическое и магнитное поля, а на больших расстояниях — и через электромагнитное поле излучения.

Связь через ближнее электрическое и магнитное поля

Теоретически полная независимость ближнего электрического и магнитного полей может наблюдаться только в статических условиях. Электростатическим называется поле неподвижных зарядов. При любом перемещении этих зарядов появляется магнитное поле. Точно так же магнитостатическим является поле постоянного магнита или электромагнита, питаемого постоянным током. При любом изменении этого поля появляется электрическое поле. Исчерпывающий анализ связи цепей с учетом взаимозависимости электрического и магнитного полей может быть выполнен с помощью уравнений Максвелла [33]. Вместе с тем приемлемые для практики результаты получаются при рассмотрении нежелательных связей между цепями в предположении полной взаимной независимости ближнего электрического и магнитного полей. В этом случае связь между источником и рецептором наводки через ближнее электрическое поле рассматривается как емкостная связь через малую паразитную емкость без учета появляющегося при этом магнитного поля. Связь через ближнее магнитное поле рассматривается как индуктивная связь между источником и рецептором наводки через малую паразитную взаимоиндуктивность без учета появляющегося при этом электрического поля.

Емкостная и индуктивная нежелательные связи могут появляться и при отсутствии непосредственной связи между источником и рецептором наводки. Рассмотрим случай размещения источника и рецептора наводки в отдельных экранированных отсеках. Через оба отсека проходит провод AB, не имеющий отношения ни к источнику, ни к рецептору наводки. Этот провод имеет емкость C1 (рис. 98) или взаимную индуктивность M1 (рис. 99) по отношению к источнику наводки и емкость C2 или взаимную индуктивность M2 по отношению к рецептору наводки.

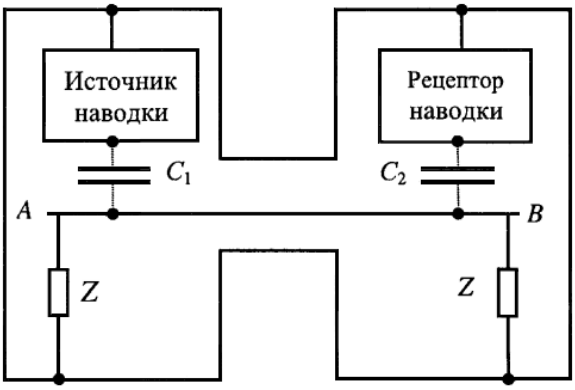

Рис. 98. Емкостная нежелательная связь через случайный провод AB

Таким образом, из-за наличия провода АВ источник и приемник наводки оказываются взаимно связанными. Величина этой связи определяется значениями Ср С2, mi,M2 и полного сопротивления ZAB постороннего провода относительно корпуса.

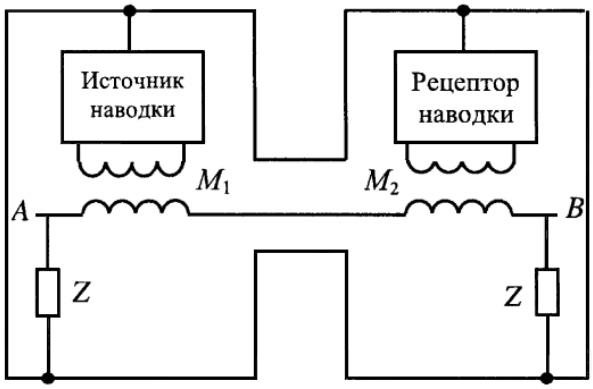

Рис. 99. Индуктивная нежелательная связь через случайный провод АВ

На рис. 100 представлена эквивалентная схема для случая емкостной связи, из которой следует, что элементы C_1 и Z_{AB} представляют собой делитель, плечи которого определяют величину напряжения, наводимого через емкость C_2 на рецепторе.

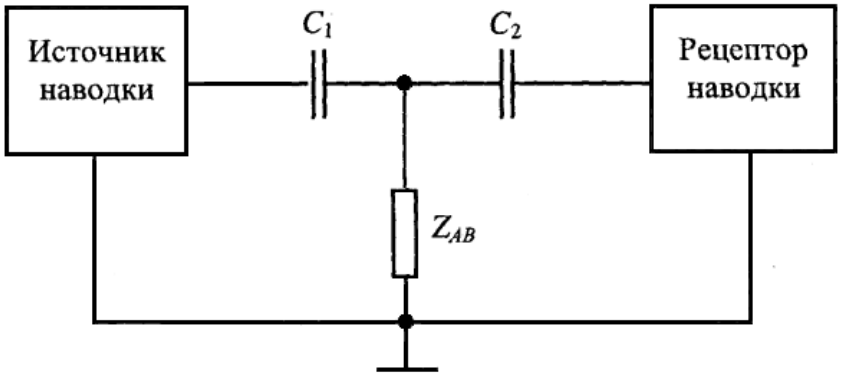

Рис. 100. Емкостная нежелательная связь по схеме делителя

Аналогичные эквивалентные схемы могут быть составлены для случаев индуктивной и смешанной связей.

Связь через электромагнитное поле

Электромагнитные излучения, сопутствующие работе технических средств систем информатизации и связи, распространяются в окружающее пространство. В зону действия этих излучений попадает большое количество токопроводящих элементов и конструкций, обладающих свойствами антенн. В таких случайных антеннах электромагнитное поле наводит ЭДС или ток опасного сигнала. Роль случайных антенн могут играть проводники монтажных схем технических средств, токоведущие элементы систем заземления, металлические

корпуса аппаратуры, металлоконструкции систем водоснабжения и канализации, посторонние протяженные проводники (например, провода открытой телефонной или громкоговорящей связи, сигнализации, часофикации, электропитания и т.д.). Токи опасных сигналов, наводимые электромагнитными полями, сопутствующими работе технических средств, распространяясь по токоведущим коммуникациям, создают реальные предпосылки утечки информации.

Связь через общее полное сопротивление

В конструкциях технических средств часто обнаруживаются общие сопротивления $Z_{общ}$, входящие одновременно в цепи источников и рецепторов наводки [10]. На рис. 101 представлена эквивалентная схема такого включения, из которой следует, что на входе приемника наводки формируется напряжение, комплексная амплитуда которого равна:

$$\dot{U}_н = \frac{\dot{E}_{ист} \cdot \dot{Z}_{общ}}{\dot{Z}_{ист} + \dot{Z}_{общ}} \qquad (6.1)$$

где $\dot{Z}_{ист}$ — внутреннее сопротивление источника наводки; $\dot{E}_{ист}$ — комплексная амплитуда ЭДС источника наводки.

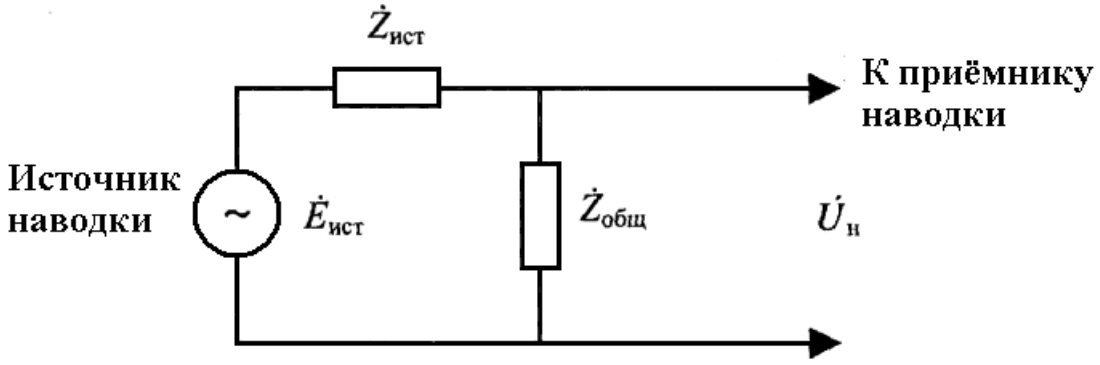

Рис. 101. Пример эквивалентной схемы включения

Так как обычно $\dot{Z}_{ист} >> \dot{Z}_{общ}$, то можно полагать, что:

$$\dot{U}_н = \dot{E}_{ист} \cdot \frac{\dot{Z}_{общ}}{\dot{Z}_{ист}} \qquad (6.2)$$

Связь через общее сопротивление проявляется чаще других встречающихся видов нежелательной связи. Это прежде всего связь через внутреннее сопротивление и соединительные провода источников питания или управления (рис. 102)

Через цепь источника питания протекают токи всех частот, составляющих спектр сигнала источника наводки. Эти токи создают падение напряжения на всех сопротивлениях, включенных в цепь питания.

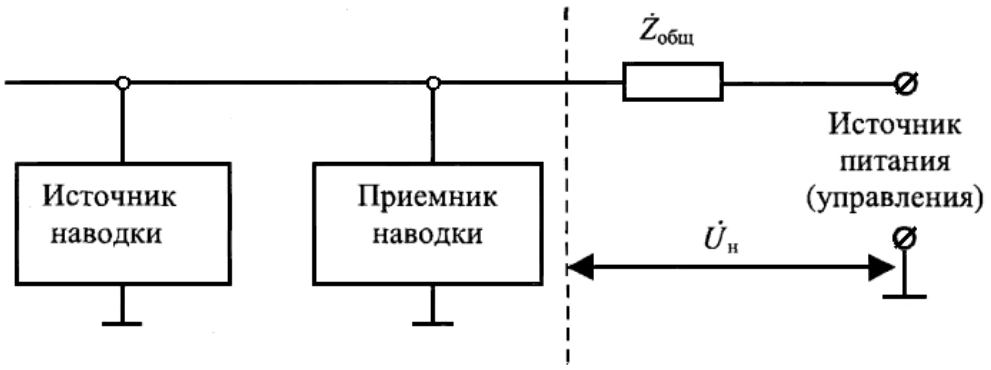

Рис. 102. Связь через общее сопротивление источника питания

Сопротивление $\dot{Z}_{общ}$ оказывается включенным в цепи приемника наводки, и напряжение $\dot{U}_н$, снимаемое с $\dot{Z}_{общ}$, является наводимым напряжением. Величина сопротивления $\dot{Z}_{общ}$ зависит от частоты наводимого напряжения. Для постоянного тока и очень низких частот — это в основном сопротивление дросселей фильтра и диодов выпрямителя или внутреннее сопротивление химических источников питания. Для звуковых частот — активное сопротивление проводов и емкостное сопротивление выходного конденсатора фильтра питания. На высоких частотах величина $\dot{Z}_{общ}$ зависит в основном от индуктивного сопротивления соединительных проводов и конденсаторов фильтра питания. Индуктивности проводов и распределенные емкости монтажа могут образовывать резонансные контуры. При неблагоприятном сочетании величин индуктивности и емкости величина $\dot{Z}_{общ}$ на некоторых высоких частотах может быть достаточно большой. К рассматриваемому виду нежелательной связи относится связь через общие отрезки проводов и общие участки корпуса, по которому протекают блуждающие токи. Вероятность проявления такой связи увеличивается с ростом частоты.

6.4. Излучатели электромагнитных полей

В состав систем и средств информатизации и связи входит большое количество различных устройств и соединительных линий, содержащих токоведущие элементы. Прохождение электрических сигналов и токов по *различным цепям* технических средств сопровождается возникновением в окружающей среде электромагнитных полей. Необходимым условием возникновения таких полей является наличие в технических средствах элементов, обладающих антенными свойствами, в которых и осуществляется возбуждение электромагнитного поля соответствующими токами и зарядами.

Структура и количественные параметры электромагнитных полей, сопровождающих работу различных технических средств, зависят от элементной базы, принципов построения, конструктивных особенностей и условий размещения этих

средств. Такие электромагнитные излучения технических систем и средств являются потенциальными носителями опасных сигналов и относятся к классу нежелательных излучений. Распространение этих нежелательных электромагнитных излучений в окружающем пространстве создает предпосылки для утечки информации за счет их перехвата техническими средствами разведки.

Электромагнитное поле излучающей антенны

Электромагнитное поле возбуждается в пространстве токами и зарядами излучающей системы — антенны. Излучатели электромагнитных полей можно разделить на две группы. К первой группе относятся передающие антенны различных радиотехнических средств, которые специально предназначены для преобразования подводимых к ним электромагнитных колебаний в электромагнитные поля с целью передачи информации по радиоканалу через свободное пространство. Вторая группа излучателей включает в себя элементы, обладающие свойствами антенн, но по своему функциональному назначению не предназначенные для возбуждения электромагнитных полей, т.е. случайные антенны.

В зависимости от соотношения между расстоянием r от излучателя до точки приема и длиной волны λ, излучаемого поля пространство вокруг излучателя может быть разделено на три области в которых свойства электромагнитного поля проявляются по-разному: ближнюю зону ($r << \lambda$); промежуточную зону ($r \approx \lambda$); дальнюю зону ($r >> \lambda$).

Излучатели первой группы предназначены для формирования поля в основном в дальней зоне. В настоящее время в радиопередающих устройствах различных систем передачи информации широко используются самые разнообразные антенны. По типу излучающих элементов антенны подразделяются на следующие три группы [38]: линейные антенны, апертурные антенны; антенны поверхностных волн.

К линейным относят антенны, у которых токи протекают по сравнительно узким каналам, с поперечными размерами, малыми по сравнению с продольными и с длиной волны. К таким антеннам прежде всего относят проволочные (симметричные и несимметричные), а также щелевые антенны. В настоящее время проволочные антенны используются в диапазонах километровых, гектометровых, декаметровых и метровых волн. Щелевые антенны главным образом применяются в диапазонах ультра- и сверхвысоких частот.

Апертурными называют антенны, излучение которых происходит через раскрыв, называемый апертурой. Такие антенны обычно используются в диапазонах ультра-, сверх- и крайне высоких частот. К апертурным антеннам относятся, в первую очередь, рупорные, линзовые и зеркальные антенны. Отличительной особенностью этих антенн является то, что электрические токи у них протекают по

проводящим поверхностям, имеющим размеры, соизмеримые или много больше по сравнению с длиной волны.

Антенны поверхностных волн возбуждаются бегущими электромагнитными волнами, распространяющимися вдоль антенны, и излучают преимущественно в направлении распространения. Примером такой антенны является стержневая диэлектрическая антенна, являющаяся продолжением открытого конца волновода и имеющая максимум излучения вдоль своей оси. Антенны поверхностных волн находят практическое применение главным образом в диапазонах очень высоких, ультравысоких и сверхвысоких частот.

Рассмотренные типы антенн могут применяться в качестве одиночных антенн, а также группироваться в многоэлементные решетки (например, фазированные антенные решетки). Кроме того, возможно создание и использование гибридных антенных систем, объединяющих свойства различных антенн. Решение задач определения и измерения параметров электромагнитного поля, формируемого различными антеннами в дальней зоне, осуществляется методами электродинамики, теории и практики антенных систем [33].

Случайные излучающие антенны

Случайные излучатели, роль которых при работе технических средств и систем играют отдельные элементы или соединительные линии, могут быть сосредоточенными (при их малых в сравнении с длиной волны λ излучаемых колебаний линейных размерах ($l << \lambda$)), соизмеримыми с длиной волны ($l \approx \lambda$) и распределенными ($l >> \lambda$).

В теории электромагнитного поля в качестве простейших излучателей широко используются элементарные электрические и магнитные диполи. Элементарным электрическим диполем называют прямолинейный излучатель длиной l много меньшей, чем длина волны λ, вдоль которого амплитуда и фаза тока неизменны (см. рис. 103).

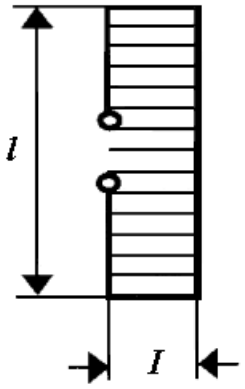

Рис. 103. Элементарный электрический диполь

Комплексные амплитуды напряженности поля, создаваемого элементарным электрическим диполем, расположенным в однородной неограниченной среде (без

потерь) вдоль оси Z сферической системы координат, в точке наблюдения на расстоянии r при изменении тока в излучателе по гармоническому закону $\dot{I} \cdot e^{j\omega t}$ определяются выражениями [33]:

- для ближней зоны (рис. 104):

$$\dot{H}_\varphi = \frac{\dot{I} \cdot l}{4\pi r^2} \sin\theta \tag{6.3}$$

$$\dot{E}_r = -j \frac{\dot{I} \cdot l}{2\pi\omega\varepsilon r^3} \cos\theta \tag{6.4}$$

$$\dot{E}_\theta = -j \frac{\dot{I} \cdot l}{2\pi\omega\varepsilon r^3} \sin\theta \tag{6.5}$$

- для дальней зоны (рис. 105):

$$\dot{H}_\varphi = j \frac{k \cdot \dot{I} \cdot l}{4\pi r} e^{-jkr} \sin\theta \tag{6.6}$$

$$\dot{E}_\theta = \frac{k \cdot \dot{I} \cdot l \cdot Z_в}{4\pi r} e^{-jkr} \sin\theta \tag{6.7}$$

где $k = 2\pi/\lambda = \omega\sqrt{\varepsilon\mu}$ — волновое число; λ — длина волны колебаний в рассматриваемой среде; ε, μ — абсолютные диэлектрическая и магнитная проницаемости среды; ω — угловая частота колебаний.

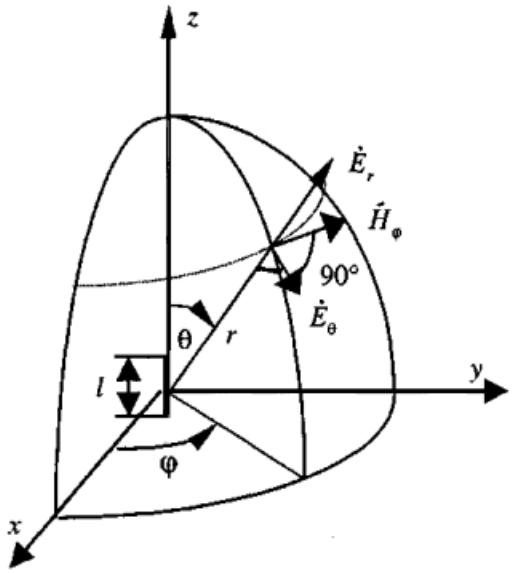

Рис. 104. Амплитуда напряженности поля для ближней зоны

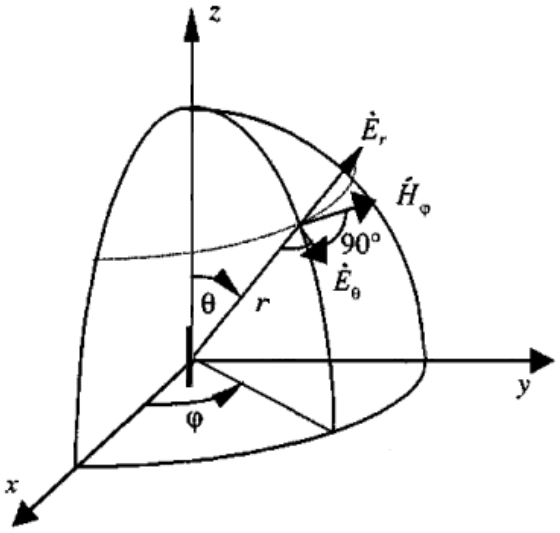

Рис. 105. Амплитуда напряженности поля для дальней зоны

Анализ выражений (6.3 - 6.5) показывает, что в ближней зоне составляющие вектора напряженности электрического поля изменяются обратно пропорционально г3 и отстают по фазе на 90° от составляющей вектора напряженности магнитного поля, которая изменяется обратно пропорционально г2. Взаимная ориентация векторов $\dot{E}$ и $\dot{H}$ в ближней зоне представлена на рис. 104.

Из выражений (6.6, 6.7) следует, что в дальней зоне векторы напряженности электрического и магнитного полей синфазны и убывают обратно пропорционально r. Взаимное расположение векторов напряженности поля в дальней зоне показано на рис. 105.

Векторы $\dot{E}_\theta$ и $\dot{H}_\varphi$ лежат в плоскости, перпендикулярной направлению распространения: вектор $\dot{E}$ лежит в плоскости, проходящей через ось диполя, а вектор $\dot{H}$ — в плоскости, параллельной плоскости XOY. Такая картина поля характерна для поперечной электромагнитной волны.

Плоская излучающая рамка

Другим простейшим излучателем является небольшой виток провода (плоская рамка в виде круглого витка радиуса а) с переменным электрическим током $\dot{I} \cdot e^{j\omega t}$. Предполагается, что во всех точках провода ток имеет неизменные амплитуду и фазу. Практически это условие реализуется при размерах рамки, малых в сравнении с длиной волны λ.

Комплексные амплитуды компонент поля элементарного магнитного диполя определяются в соответствии с общей теорией поля соотношениями [33]:

- для ближней зоны:

$$\dot{E}_\varphi = \frac{\dot{I} S \mu \omega}{4\pi r^2} \sin\theta, \tag{6.8}$$

$$\dot{H}_r = j\frac{\dot{I} S}{2\pi r^3} \cos\theta, \tag{6.9}$$

$$\dot{H}_\theta = j\frac{\dot{I} S}{4\pi r^3} \sin\theta, \tag{6.10}$$

- для дальней зоны:

$$\dot{E}_\varphi = \frac{\dot{I} k^2 S Z_в}{4\pi r} e^{-jkr} \sin\theta, \tag{6.11}$$

$$\dot{H}_\theta = -\frac{\dot{I} k^2 S}{4\pi r} e^{-jkr} \sin\theta, \tag{6.12}$$

где $S = \pi \cdot a^2$ — площадь рамки с током.

Таким образом, в ближней зоне электрическая компонента поля рамки изменяется обратно пропорционально r^2, а магнитные компоненты — обратно пропорционально r^3. В дальней зоне электрическая и магнитная компоненты поля изменяются обратно пропорционально.

Сравнительный анализ полей электрического и магнитного диполей

Сравнительный анализ выражений (6.3 - 6.5, 6.8 - 6.10) для компонент электромагнитного поля электрического и магнитного диполей показывает, что магнитное поле горизонтальной рамки идентично электрическому полю элементарного вертикального электрического диполя, а электрическое поле, горизонтальной рамки идентично магнитному полю вертикального электрического диполя. Следовательно, горизонтальная рамка создает такое же поле, как и вертикальный электрический диполь. Различие между этими полями состоит лишь в том, что векторы $\dot{E}$ и $\dot{H}$ меняются в пространстве местами. Поэтому горизонтальную рамочную антенну можно трактовать как фиктивный вертикальный магнитный диполь. Взаимная ориентация векторов $\dot{E}$ и $\dot{H}$ поля рамки в ближней зоне изображена на рис. 106.

Сравнивая выражения (6.11, 6.12) для компонент поля, создаваемого рамкой в дальней зоне, с соответствующими выражениями (6.6, 6.7) для компонент поля, создаваемого элементарным электрическим диполем, отметим, что при одинаковых фазах токов $\dot{I}$ электрического диполя и рамки поля излучения их будут сдвинуты между собой по фазе на 90° (на это указывает множитель j в выражениях для поля электрического диполя).

Векторы $\dot{E}_\varphi$ и $\dot{H}_\theta$ лежат в плоскости, перпендикулярной направлению распространения. Взаимное расположение векторов напряженности поля рамки в дальней зоне представлено на рис. 107.

Волновое сопротивление свободного пространства $Z_в$ в дальней зоне ($r >> \lambda/2\pi$) не зависит от расстояния и равно 377 Ом. Для оценки интенсивности электромагнитного поля в этой зоне достаточно определить одну из составляющих поля. Обычно осуществляют измерение напряженности электрического поля или плотности потока мощности.

Волновое сопротивление в ближней зоне при $r << \lambda/2\pi$ зависит от типа излучателя (электрический или магнитный) и от расстояния до него. Если излучатель представляет собой прямой короткий проводник (вибратор), в котором ток высокой частоты мал (сопротивление источника велико), то волновое сопротивление вблизи такого излучателя большое

$$\frac{\dot{E}_\theta}{\dot{H}_\varphi} = \frac{Z_в \lambda}{4\pi r} >> Z_в . \qquad (6.13)$$

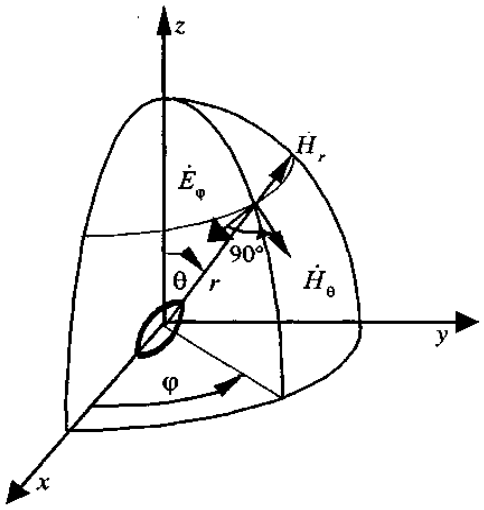

Рис. 106. Напряженность поля рамки в ближней зоне

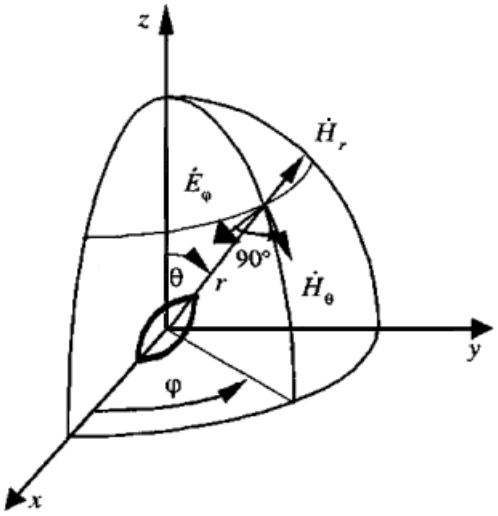

Рис. 107. Напряженность поля рамки в дальней зоне

В структуре поля преобладает электрическая составляющая, которая по мере удаления от излучателя уменьшается быстрее ($E_\theta \approx 1/r^3$), и, следовательно, уменьшается волновое сопротивление, асимптотически приближаясь к значению $Z_в$ в дальней зоне (рис. 108).

Если в роли излучателя выступает рамка (источник с низким сопротивлением), то волновое сопротивление в ближней зоне мало:

$$\frac{\dot{E}_\varphi}{\dot{H}_\theta} = \frac{Z_в 2\pi r}{\lambda} << Z_в, \qquad (6.14)$$

В этом случае в структуре поля в ближней зоне преобладает магнитная составляющая. По мере удаления от источника излучения волновое сопротивление растет и асимптотически приближается к значению $Z_в = 377$ Ом в дальней зоне (см. рис. 108).

Таким образом, если электрические цепи, технические средства или их элементы обладают значительным сопротивлением и для них характерны большие амплитуды напряжений и малые амплитуды токов, то по своим свойствам они подобны электрическим излучателям. К таким элементам можно отнести, например, телевизионные кинескопы.

Низкоомные электрические цепи и средства с большими амплитудами токов и малыми амплитудами напряжений - например, мощные транзисторные усилители - близки по своим свойствам к магнитным излучателям.

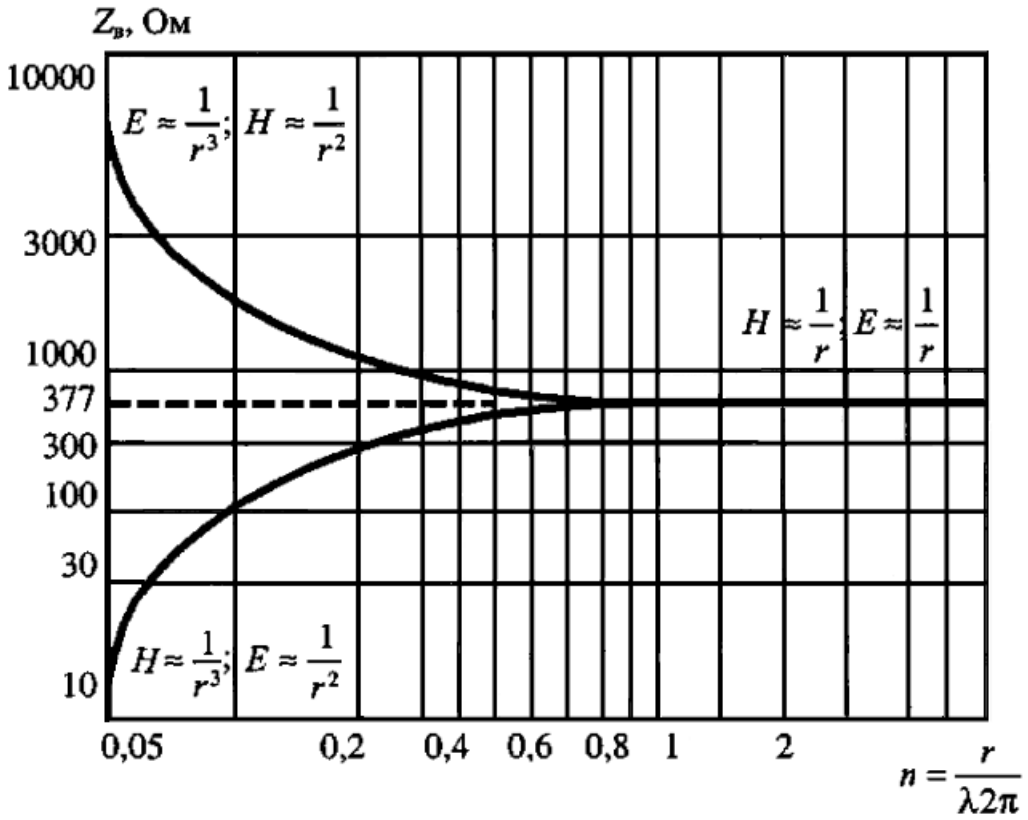

Рис. 108. Волновое сопротивление свободного пространства

В большинстве практических случаев результирующее электромагнитное поле создается группой разнотипных источников излучения. Поэтому характер изменения компонент этого поля существенно отличается от того, который свойственен одиночному излучателю, и обычно определяется экспериментально.

Анализ выражений (6.3 - 6.5, 6.8 - 6.14) позволяет сделать следующие выводы:

1. Структура поля элементарного электрического и элементарного магнитного излучателей отличается взаимным изменением положения в пространстве векторов $\dot{E}$ и $\dot{H}$.

2. Поля ближней зоны элементарного электрического и магнитного излучателей существенно неравномерны, а их интенсивность быстро убывает с расстоянием ($\sim 1/r^3$ и $\sim 1/r^2$).

3. Составляющие напряженности электрического и магнитного полей в ближней зоне сдвинуты по фазе на 90°. Поэтому вектор Пойнтинга оказывается чисто мнимой величиной со средним значением, равным нулю. Следовательно, рассматриваемые поля являются реактивными.

4. Вблизи элементарного электрического излучателя создается электромагнитное поле, основная энергия которого сосредоточена в электрической составляющей (электрическое поле).

5. Характеристическое сопротивление среды полю элементарного электрического излучателя в ближней зоне равно:

$$Z_E = \frac{\dot{E}_\theta}{\dot{H}_\varphi} = \frac{1}{j\omega\varepsilon_a r}, \qquad (6.15)$$

где ε_a — абсолютная диэлектрическая проницаемость среды.

6. Вблизи элементарного магнитного излучателя создается электромагнитное поле, основная энергия которого сосредоточена в магнитной составляющей (магнитное поле).

7. Характеристическое сопротивление среды полю элементарного магнитного излучателя в ближней зоне равно:

$$Z_н = \frac{\dot{E}_\varphi}{\dot{H}_\theta} = -j\omega\mu_a r, \qquad (6.16)$$

где μ_a — абсолютная магнитная проницаемость.

8. Характеристическое сопротивление среды полю электрического излучателя Z_E с увеличением расстояния от него уменьшается, а характеристическое сопротивление среды полю магнитного излучателя Z_H увеличивается, и оба стремятся к значению $Z_в = 120\pi$, достигая его в дальней зоне при $r >> \lambda / 2\pi$.

На практике часто встречаются случаи, когда однородные технические средства распределены на некоторой площади (например, группа видеоконтрольных устройств на пульте оператора, работающих с одинаковыми сигналами). Определение напряженности поля, создаваемого такими техническими средствами, осуществляется путем геометрического сложения отдельных составляющих, формируемых каждым излучателем. Анализ структуры электромагнитного поля, создаваемого группой однородных источников, показывает, что закон изменения компонент этого поля существенно отличается от того, который характерен для одиночного излучателя, и обычно определяется экспериментально.

6.5. Утечка информации по цепям заземления

Заземлением называется преднамеренное соединение объекта с заземляющим устройством. Заземление осуществляется путем создания системы проводящих поверхностей и электрических соединений, предназначенных для выполнения различных функций.

Защитное заземление

Защитное заземление предназначено для исключения поражения обслуживающего персонала электрическим током. Защитное заземление должно поддерживать элементы конструкции при одном и том же потенциале, равном или

близком к потенциалу «земли», и обеспечивать низкоомную нагрузку для больших токов, возникающих в системах при аварийных ситуациях. Как правило, защитные заземления должны иметь хороший низкоомный контакт с «землей», поэтому их часто называют наружными заземлителями [8]. Наружные заземлители осуществляют заземление силовых систем, радиочастотных антенн, молниеотводов, стекателей статического электричества и т.д.

Рабочие заземления включают в себя заземление силового оборудования (сильноточных цепей) и сигнальное или схемное заземление, которое обеспечивает формирование опорного потенциала, необходимого для работы электронных схем.

Заземление экранирующих поверхностей способствует ослаблению нежелательных связей и является составной частью системы экранирования. Проводящие поверхности и электрические соединения системы заземления экранов предназначены для протекания обратных токов в сигнальных цепях и цепях электропитания.

Попадание опасного сигнала в систему заземления

Одной из причин попадания опасного сигнала в систему заземления является наличие электромагнитного поля — носителя опасного сигнала в местах расположения элементов системы заземления. Это электромагнитное поле будет наводить в расположенной поблизости системе заземления ток опасного сигнала. Аналогичным образом опасные сигналы могут наводиться на цепь, образуемую нулевым проводом, через который ток опасного сигнала будет попадать в систему заземления и далее в грунт. Величина тока опасного сигнала в этом случае будет определяться интенсивностью воздействующего электромагнитного поля, сопротивлением цепей заземления и проводимостью почвы.

Проникновение опасного сигнала в цепи заземления может быть связано с образованием так называемых контуров заземления. Рассмотрим два устройства, соединенные парой проводников, один из которых является сигнальным, а другой служит для протекания обратных токов (рис. 109).

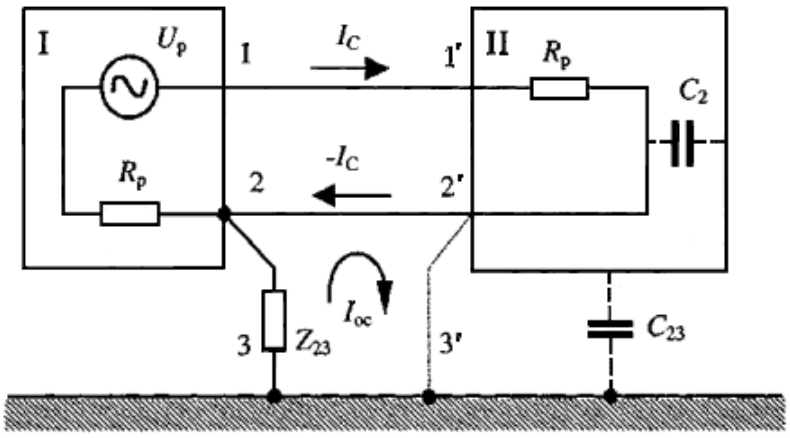

Рис. 109. Пример заземления двух устройств, соединенные парой проводников

Пусть возвратный проводник соединен с корпусом первого (I) устройства, а корпус — с землей. Если этот проводник соединен с корпусом второго (II) устройства, также имеющего электрический контакт с землей (соединение 2'— 3'), то образуется замкнутый проводящий контур 2—2'—3'—3—2. Внешнее электромагнитное поле источника опасного сигнала наводит в этом контуре ЭДС, вызывая протекание тока $I_{ос}$ который, в свою очередь, создает на участке 2—3 падение напряжения $U_{ос}$ равное:

$$U_{ос} = I_{ос} Z_{23}, \qquad (6.17)$$

где Z_{23} — сопротивление участка цепи 2—3.

Если отсутствует проводник 2'—3' или соединение проводника 2—2' с корпусом второго устройства, то возможность образования контура заземления полностью не исключается. В этих случаях контур может состоять из проводников 2—2', 3—3', земляной шины и паразитных емкостей между сигнальной цепью и корпусом второго устройства C_2, а также между корпусом второго устройства и землей C_{23}.

Еще одна причина появления опасного сигнала в цепи заземления связана с конечным значением величины сопротивления заземляющих проводников. По заземляющему проводнику протекает обратный электрический ток опасного сигнала (рис. 110).

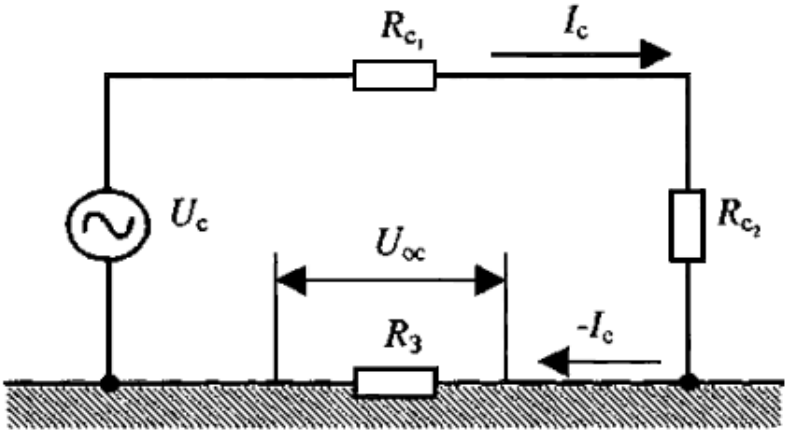

Рис. 110. Пример заземления с конечным значением величины сопротивления заземляющих проводников

Из-за конечного сопротивления R_3 земляной шины на этом сопротивлении создается падение напряжения:

$$U_{oc} = \frac{U_c R_3}{R_{c_1} + R_{c_2} + R_3}, \qquad (6.18)$$

где U_c — напряжение источника сигнала; R_{c_1}, R_{c_2} — внутреннее сопротивление источника сигнала и сопротивление нагрузки соответственно. При $R_{c_1} + R_{c_2} >> R_3$:

$$U_{oc} \approx \frac{U_c R_3}{R_{c_1} + R_{c_2}}, \qquad (6.19)$$

Например, при $R_{c_1} = R_{c_2}$ =100 Ом, $R_3 = 10^{-2}$ Ом и U_c = 5 В падение напряжения на сопротивлении R_3 составит:

$$U_{oc} \approx \frac{5 \cdot 10^{-2}}{200} = 250 \text{ мкВ}.$$

Напряжение опасного сигнала в цепи заземления будет тем больше, чем больше величина сопротивления R_3. Утечка информации за счет цепей заземления может также происходить вследствие того, что общая земля служит обратным проводом для различных контуров. Рассмотрим ситуацию, представленную на рис. 111.

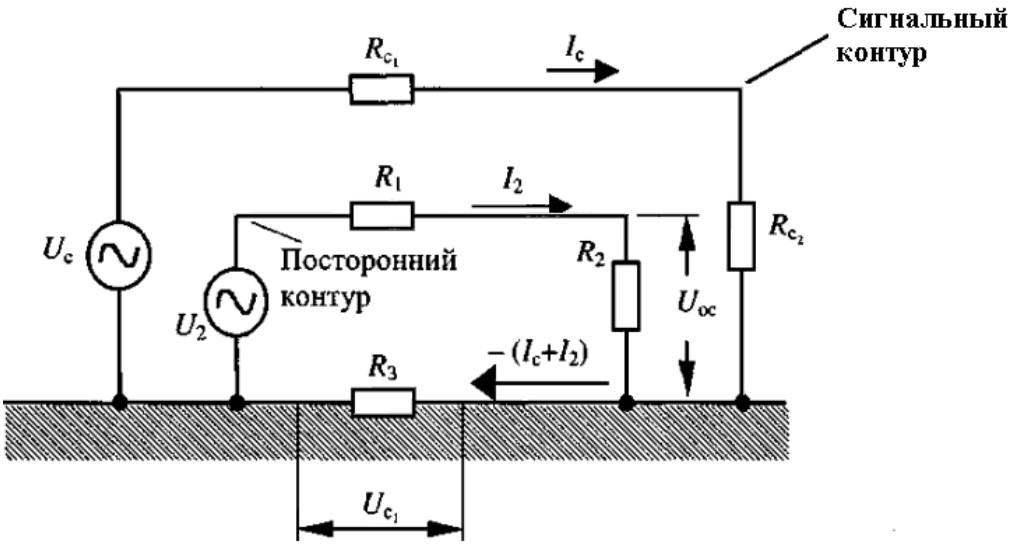

Рис. 111. Пример ситуации, когда земля служит обратным проводом для различных контуров

В этом случае для двух различных контуров — сигнального и постороннего — общая земля является обратным проводом с эквивалентным сопротивлением R_3. На эквивалентном сопротивлении земли R_3 возникает падение напряжения за счет протекания обратного тока опасного сигнала $-I_c$, равное:

$$U_{oc} = \frac{U_c R_3}{R_{c_1} + R_{c_2} + R_3} \approx \frac{U_c R_3}{R_{c_1} + R_{c_2}}, \text{ при } R_{c_1} + R_{c_2} >> R_3, \qquad (6.20)$$

где R_{c_1}, R_{c_2} — внутреннее сопротивление источника опасного сигнала U_c и сопротивление нагрузки в цепи сигнального контура.

На сопротивлении нагрузки R_2 постороннего контура имеет место падение напряжения $U_{ос}$, вызванное протеканием обратного тока опасного сигнала $-I_C$ по общей цепи заземления, которое равно:

$$U_{ос} = \frac{U_{c_1} R_2}{R_1 + R_2}, \text{ при } R_1 + R_2 >> R_3, \qquad (6.21)$$

где R_1 — внутреннее сопротивление источника напряжения U_2 в цепи постороннего контура. Подставляя (6.16) в (6.17), получим выражение для определения величины падения напряжения опасного сигнала на нагрузке постороннего контура:

$$U_{ос} = \frac{U_c R_2 R_3}{(R_{c_1} + R_{c_2})(R_1 + R_2)}, \qquad (6.22)$$

Пусть, например, $R_{c_1} = R_{c_2} =$ 100 Ом, $U_C =$ 5 В, R_1 = 100 Ом, R_2 = 10 МОм, R_3 = 0,2 Ом. В этом случае:

$$U_{ос} = \frac{5 \cdot 0{,}2 \cdot 10^7}{200 \cdot 10^7} = 5 \text{ мВ},$$

т.е. напряжение опасного сигнала на нагрузке постороннего контура будет достаточно велико.

Перехват электромагнитного поля опасного сигнала в грунте вокруг заземлителя

Возможность утечки информации, связанная с цепями заземления, обусловлена также наличием электромагнитного поля опасного сигнала в грунте вокруг заземлителя. Из-за большого затухания, вносимого грунтом, магнитное поле в землю практически не проникает. Электрическое поле в земле определяется величиной потенциала заземлителя и параметрами грунта, где происходит растекание тока опасного сигнала. С помощью дополнительных специально установленных заземлителей можно осуществить перехват опасного сигнала (см. рис. 112).

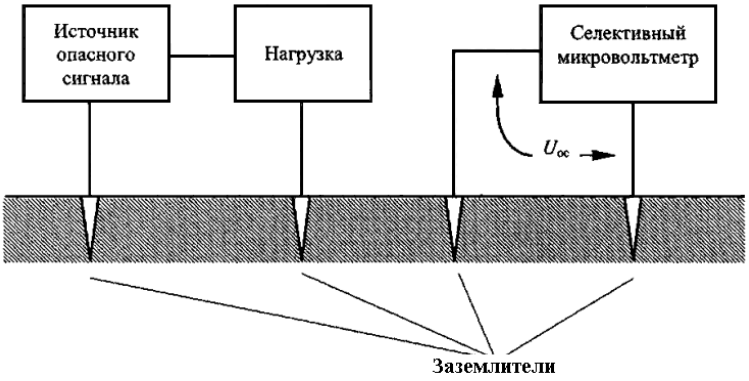

Рис. 112. Перехват опасного сигнала

6.6. Утечка информации по цепям питания

Утечка информации по цепям питания обусловлена различными причинами. Как правило, провода общей сети питания распределяются по различным помещениям, где расположены технические системы, и соединены с различными устройствами. Вследствие этого образуется нежелательная связь между отдельными техническими средствами. Кроме того, провода сети питания являются линейными антеннами, способными излучать или воспринимать электромагнитные поля. На практике значительная часть нежелательных наводок между удаленными друг от друга устройствами происходит с участием сети питания [10]. При этом возможны различные ситуации.

Асимметричная наводка

В случае асимметричной наводки, когда провода сети питания прокладываются вместе и имеют одинаковые емкости относительно источников и приемников наводки, в них наводятся напряжения, одинаковые по величине и по фазе относительно земли и корпуса приборов. Ниже представлены действительная (см. рис. 113) и эквивалентная (см. рис. 114) схемы нежелательной асимметричной связи двух устройств, питающихся от общей сети.

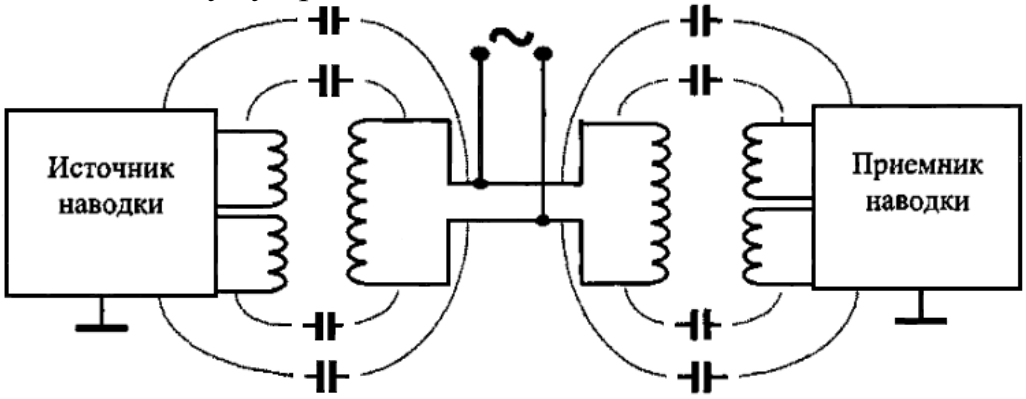

Рис. 113. Действительная схема нежелательной асимметричной связи

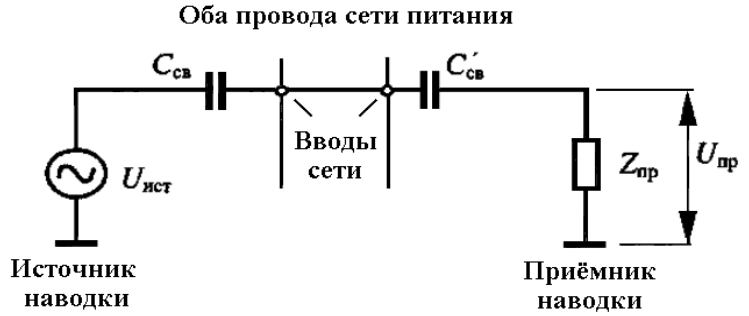

Рис. 114. Эквивалентная схема нежелательной асимметричной связи

На рис. 115 показан прием опасного сигнала через сеть питания, в которой наводятся напряжения за счет электромагнитного поля, излучаемого техническими средствами, а на рис. 116 показано излучение опасного сигнала через цепи питания источника наводки.

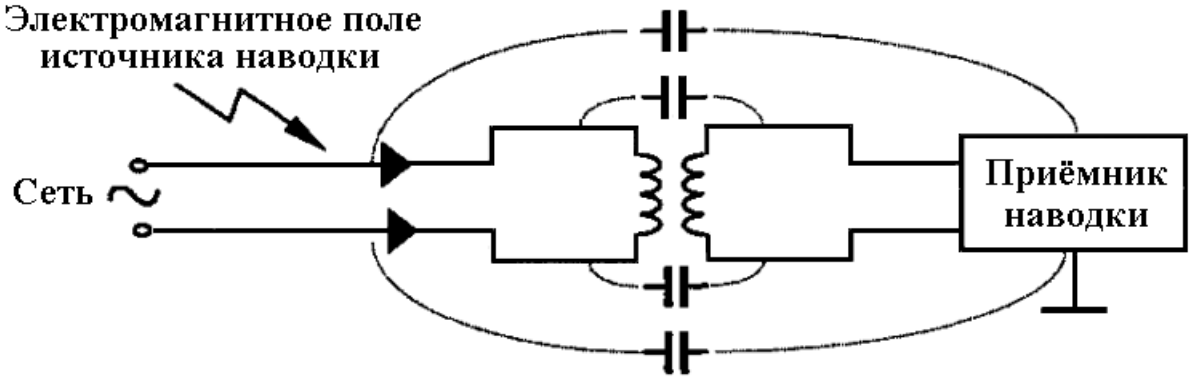

Рис. 115. Прием опасного сигнала через сеть питания

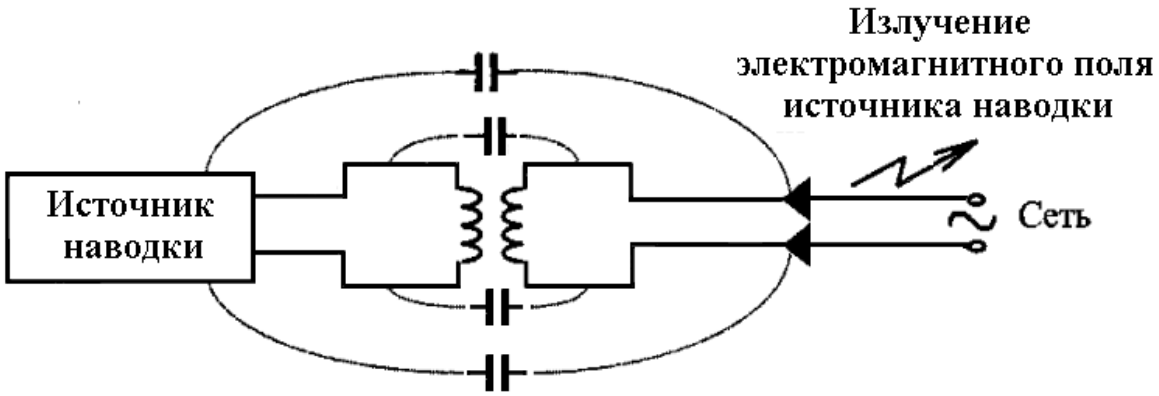

Рис. 116. Излучение опасного сигнала через цепи питания

Все эти виды распространения наводок по сети питания являются асимметричными или однопроводными, поскольку оба провода сети питания передают сигнал наводки в одном направлении. Обратным проводом является «земля».

Симметричная наводка

Симметричное распространение наводки имеет место в тех случаях, когда на проводах сети индуцируются различные напряжения относительно земли. Тогда между проводами образуется высокочастотная разность потенциалов, и по проводам сети проходят токи наводки в разных направлениях (рис. 117).

Вследствие этого в приемнике наводки индуцируются равные по величине и обратные по знаку напряжения. Поэтому симметрично распространяющаяся наводка не может проникнуть в высокочастотную часть приемника наводки. Проникновение симметричной наводки через силовой трансформатор путем передачи напряжения, наведенного в первичной обмотке, во вторичную маловероятно вследствие существенных отличий частот сети питания и сигнала наводки.

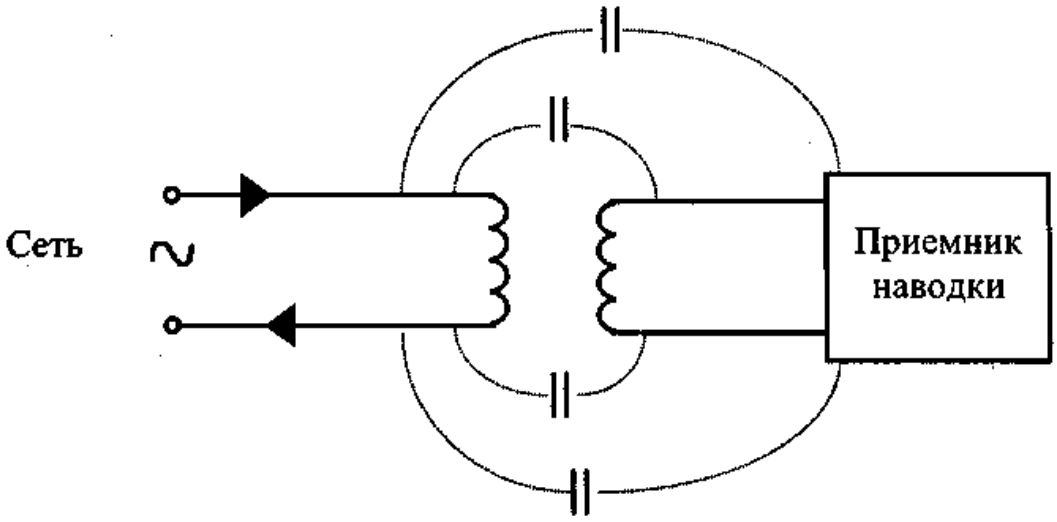

Рис. 117. Симметрично распространяющаяся наводка

Симметричное распространение наводки опасно только при асимметрии приемника наводки относительно проводов сети питания. Например, если в один из проводов сети питания ввести предохранитель, то провода сети будут иметь разные емкости относительно приемника наводки. Через них будут передаваться напряжения, разность которых приведет к наводке в приемнике [10].

Вторичный источник питания как источник утечки информации

Одними из основных устройств, без которых невозможна работа любого технического средства, являются вторичные источники питания. Эти источники предназначены для преобразования подводимой к ним энергии от сети переменного тока (например, напряжением 220 В с частотой 50 Гц) или постоянного тока (например, напряжением 27 В) в энергию постоянного или переменного тока с напряжением, необходимым для питания аппаратуры технических средств. При определенных условиях вторичные источники питания совместно с подводящими питающими линиями могут создавать условия для утечки информации, циркулирующей в техническом средстве. Несмотря на большое разнообразие конкретных технических решений схем построения таких источников питания, все они содержат в своем составе трансформаторы, выпрямители, сглаживающие фильтры, стабилизаторы и обладают конечным внутренним сопротивлением. При наличии в составе технических средств усилительных каскадов токи усиливаемых в них сигналов замыкаются через вторичный источник электропитания, создавая на его внутреннем сопротивлении падение напряжения $U_{ос}$, изменяющееся в соответствии с законом изменения усиливаемого (опасного) сигнала (см. рис. 118).

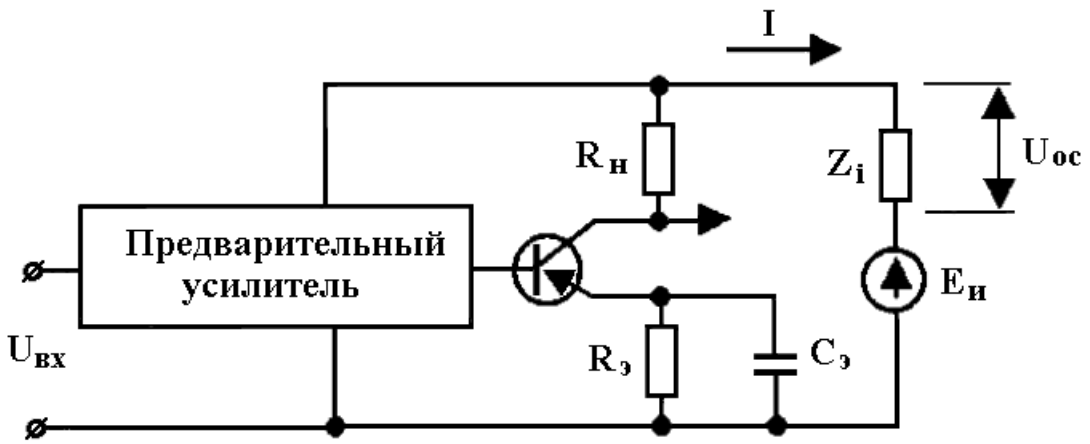

Рис. 118. Пример формирования опасного сигнала в сети питания

При недостаточном затухании в фильтре источника питания это напряжение может быть обнаружено в питающей линии.

Проникновение опасного сигнала в сеть электропитания может быть связано с тем, что среднее значение тока в оконечных каскадах усилителей технических средств в большей или меньшей степени зависит от амплитуды усиливаемых информационных сигналов. Это приводит к неравномерности потребления тока в цепи питания, которое может быть обнаружено.

При наличии трансформаторов в усилительных устройствах технических средств проникновение опасного сигнала в цепи электропитания может происходить из-за наличия магнитной связи между выходным трансформатором усилителя и силовым трансформатором вторичного источника электропитания.

6.7. Виброакустический канал

Воздействие акустических волн на поверхность твердого тела приводит к возникновению в нем вибрационных колебаний в результате виброакустического преобразования. Эти колебания, распространяющиеся в твердой среде, могут быть перехвачены специальными средствами разведки, а речевая информация, содержащаяся в акустическом поле, при определенных условиях может быть восстановлена. С этой целью используют специальные устройства, преобразующие вибрационные колебания в электрические сигналы, соответствующие звуковым частотам. Такие устройства называются вибродатчиками. Сигнал, снимаемый с выхода вибродатчика, после усиления может быть прослушан, зарегистрирован на магнитном или другом носителе или передан в пункт приема, находящийся на удалении от места прослушивания, по проводному, радио- или иному каналу передачи информации. Обобщенная структурная схема виброакустического канала утечки информации представлена на рис. 119.

В целях ведения разведки с использованием виброакустического канала широко применяются стетоскопы, т.е. устройства, содержащие вибродатчик (стетоскопный микрофон), блок обработки сигнала, осуществляющий его усиление и ослабление помех, и головные телефоны. В ряде таких устройств предусмотрена возможность записи сигнала на магнитный носитель.

Необходимо отметить, что чем тверже материал преграды на пути распространения акустических колебаний, тем лучше он передает вибрации, вызываемые ими. Поэтому, если стена помещения сделана из гипсолита, сухой штукатурки и т.п., необходимо вбить в нее металлический предмет (можно использовать обычный крупный гвоздь) и крепить датчик стетоскопа непосредственно к нему. Если стена бетонная или кирпичная, но покрыта штукатуркой или обоями, то желательно зачистить участок до твердого основания и стетоскоп крепить именно на это место.

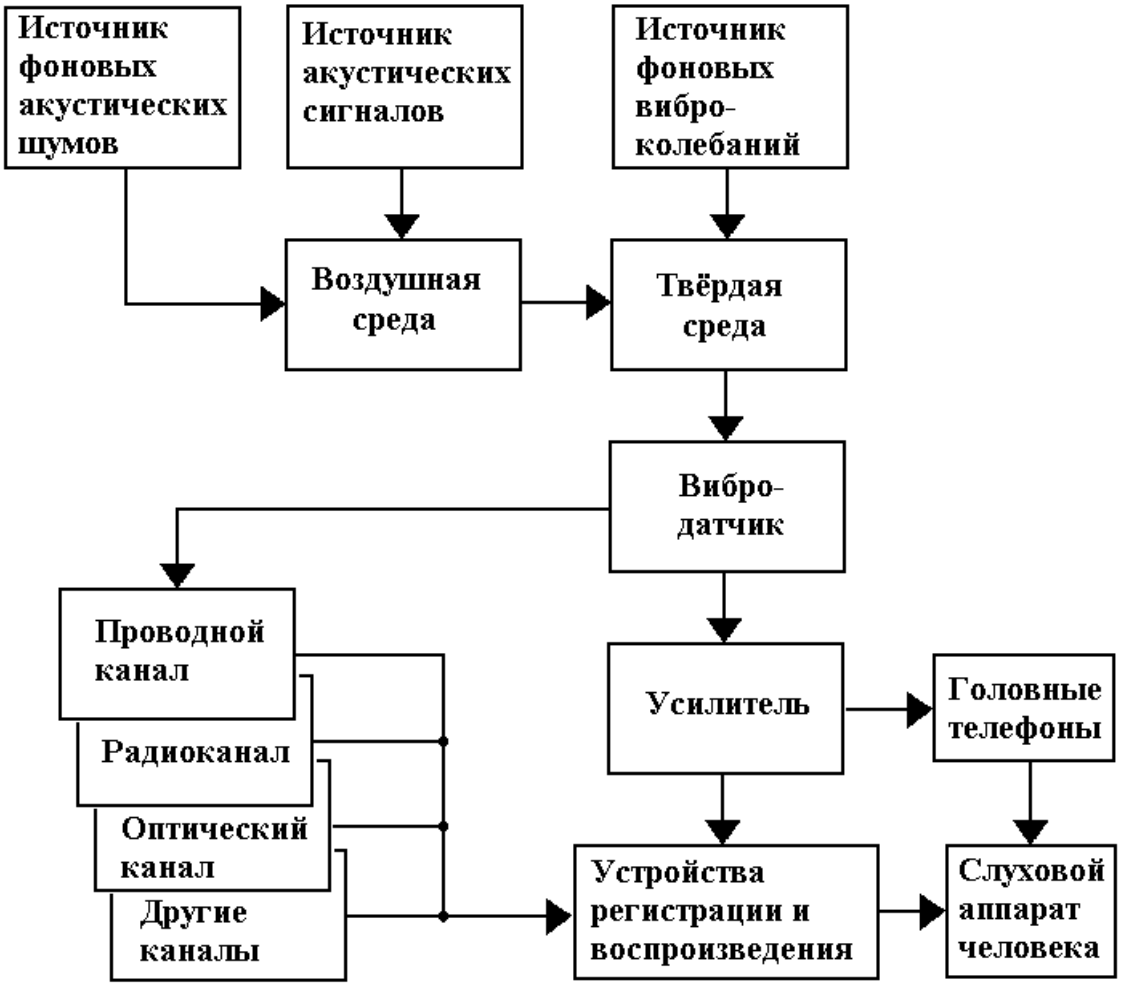

Рис. 119. Структурная схема виброакустического канала утечки информации

В качестве звукопровода можно использовать трубы водоснабжения, канализации, батареи отопления и т.д. Крепление вибродатчиков к элементам конструкции, по которой распространяются вибрации, может осуществляться с помощью специальных мастик, клеевых составов, магнитов и т.д. На качество приема вибросигналов кроме свойств вибродатчика и материала твердой среды влияют ее толщина, а также уровни фоновых акустических шумов в помещении и вибраций в твердой среде.

В ряде случаев, когда нет возможности разместить пункт прослушивания в непосредственной близости от места установки вибродатчика (стетоскопа), в состав аппаратуры прослушивания включают проводные, радио- и другие каналы передачи информации, аналогичные каналам, используемым в закладных подслушивающих устройствах. В табл. 17 приведены некоторые характеристики стетоскопных устройств, предназначенных для прослушивания информации.

Таблица 17.

№ п/п	Тип устройства	Максимальная толщина стены, см	Полоса частот вибродатчика, Гц	Диапазон частот передатчика, МГц. Дополнительные сведения.
1.	Стетоскопный микрофон UM 012	до 50	150-3500	Тип датчика: высокочувствительный вибромикрофон
2.	Изделие фирмы DTI	до 100	300-3000	То же с встроенным усилителем
3.	Стетоскопный микрофон UM 121	до 50		Тоже
4.	Радиозакладка-стетоскоп UM 006	до 50	150-5000	108-112,5 МГц Тип датчика: высокочувствительный вибромикрофон
5.	Радиозакладка-стетоскоп UM 006.1	до 50	150-5000	136-146 МГц Тип датчика: высокочувствительный вибромикрофон
6.	Радиозакладка SIPERS	до 50		Дальность действия передатчика до 250 м
7.	SIPE OPTO 2000			Ик-передатчик, до 500 м

6.8. Электроакустический канал

Образование электроакустического канала утечки информации связано с наличием в ТСОИ случайных электроакустических преобразователей, называемых случайными микрофонами. Эти элементы обладают способностью

преобразовывать акустические колебания в электрические сигналы, хотя и не предназначены для этой цели. Элементы технических средств обработки информации, обладающие свойствами случайных электроакустических преобразователей, могут подвергаться воздействию акустических полей с достаточными интенсивностью и звуковым давлением. Воздействие акустического поля на элементы ТСОИ может привести к изменению их взаимной ориентации, положения или к их деформации. В результате на выходах случайных электроакустических преобразователей могут либо возникнуть электрические заряды, токи или ЭДС, либо произойти изменения параметров токов и напряжений, формирующихся в цепях технических средств при их функционировании, обусловленные опасными сигналами (например, нежелательная модуляция).

Микрофонные свойства случайных электроакустических преобразователей проявляются в результате различных физических явлений, приводящих к появлению тока или ЭДС при перемещении элемента или его деформации под действием акустического поля. Большую группу случайных электроакустических преобразователей составляют индукционные (индуктивные) преобразователи. Например, если поместить рамку (катушку индуктивности) в магнитное поле, создаваемое постоянным магнитом (рис. 120), и изменять ее ориентацию относительно направления вектора магнитной индукции поля, то на выходе рамки появится ЭДС индукции. Перемещение рамки, изменяющее ее ориентацию, может быть вызвано воздушным потоком переменной плотности, возникающим при ведении разговора в помещении, где расположено техническое средство. К числу индуктивных случайных электроакустических преобразователей относят электрические звонки, громкоговорители, электромеханические реле, трансформаторы и т.д.

В состав телефонного аппарата входит вызывной звонок, который при положенной микротелефонной трубке подключен к линии через конденсатор. Этот звонок представляет собой электромагнитную систему (рис. 121), в которой под воздействием акустического поля происходит перемещение якоря, вызывающее появление ЭДС опасного сигнала $E_{м_э}$ на обмотке звонка и в линии, подключенной к телефонному аппарату.

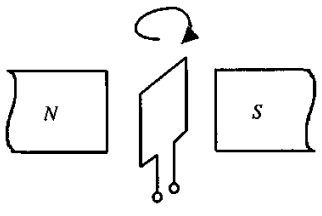

Рис. 120. Рамка в магнитном поле

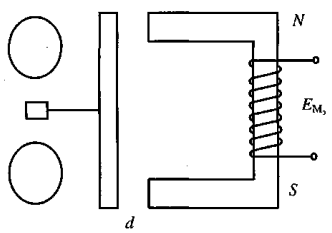

Рис. 121. Обмотка звонка

Величина этой ЭДС определяется выражением [15]:

$$E_{м_э} = \eta \cdot \rho, \qquad (6.23)$$

где η — акустическая чувствительность звонка; ρ — акустическое давление.

Акустическая чувствительность вызывного звонка может быть рассчитана по формуле [15]:

$$\eta = \frac{VS\mu\omega S_м}{d^2 Z_м}, \qquad (6.24)$$

где V — магнитодвижущая сила постоянного магнита; $S_м$ — площадь якоря;

μ — магнитная проницаемость сердечника; ω — число витков катушки звонка;

$S_м$ — площадь полюсного наконечника магнита; d — величина зазора в магнитной цепи якоря; $Z_М$ — механическое сопротивление акустико-механической системы звонка.

Акустическая чувствительность вызывного звонка телефонных аппаратов в среднем составляет 50 мкВ/Па - 6 мВ/Па. В состав телефонного аппарата кроме вызывного звонка входят и другие элементы, чувствительные к акустическому полю, например телефон и микрофон микротелефонной трубки, трансформатор.

Достаточно высокую чувствительность к акустическому воздействию имеют электродинамические громкоговорители, используемые в системах звуковоспроизведения или в радиотрансляционной сети (2-3 мВ/Па), а также исполнительные устройства вторичных электрических часов, работающих от системы единого времени (100-500 мкВ/Па).

Различные трансформаторы (входные, выходные, в сети питания и т.д.) также могут выполнять роль электроакустических преобразователей. Трансформатор состоит из замкнутого сердечника, сделанного из мягкой стали или феррита, на котором имеются, как минимум, две изолированные друг от друга обмотки с разным числом витков W_1 и W_2 (см. рис. 122).

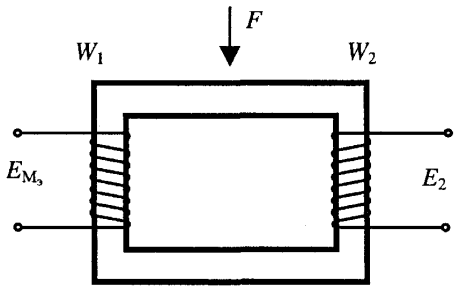

Рис. 122. Схема трансформатора

Акустическое воздействие на сердечник и обмотку трансформатора может привести к появлению микрофонного эффекта. Если ЭДС индукции $E_{м_Э}$ появляется в первичной обмотке, то во вторичной ЭДС изменится на величину коэффициента трансформации.

В электромеханических реле различного назначения появление микрофонного эффекта связано с теми же явлениями, которые имеют место при воздействии акустического поля на электромеханический вызывной звонок телефонного аппарата. В случайных магнитострикционных электроакустических преобразователях, например в подстроечных сердечниках катушек индуктивности, при воздействии акустического поля изменяется их намагниченность, что приводит к появлению низкочастотного напряжения на выводах этих катушек.

При воздействии акустического поля на технические средства обработки информации в отдельных их элементах могут проявляться свойства случайных электроакустических преобразователей. Например, в результате действия звукового давления акустических колебаний может происходить перемещение витков контурных катушек и изменение расстояний между ними, что приводит к изменению индуктивности и собственной емкости катушек. При определенных условиях воздействие акустического поля на ТСОИ вызывает случайные электроакустические преобразования, приводящие к нежелательной модуляции опасным сигналом электромагнитных колебаний, генерируемых или усиливаемых элементами технических средств.

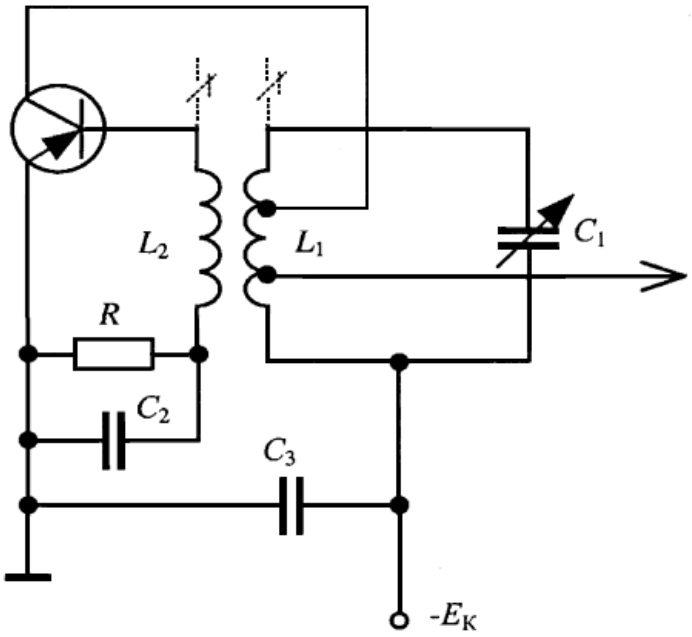

Рис. 123. Элементы колебательного контура

Например, при воздействии акустического давления на элементы гетеродина радиоприемного устройства (элементы колебательного контура: конденсатор с переменной емкостью C_1 и катушки индуктивности L_1 L_2 с подстроечными сердечниками, рис. 123) может изменяться расстояние между пластинами переменного воздушного конденсатора и витками катушек индуктивности. Это приведет к изменению их параметров С и L, следовательно, к изменению значения частоты гетеродина по закону изменения акустического давления.

Так осуществляется нежелательная модуляция частоты гетеродина опасным сигналом, соответствующим речевому сообщению.

Эффективность случайных электроакустических преобразователей определяется их свойствами и конструктивными особенностями, а также условиями их размещения относительно источника опасного акустического сигнала.

6.9. Утечка информации в волоконно-оптических линиях связи

Основные причины утечки информации в волоконно-оптических линиях связаны с излучением световой энергии в окружающее пространство. Причины этого излучения обусловлены процессами, происходящими при вводе (выводе) излучения в оптический волновод и распространении волн в диэлектрическом волноводе. Кроме того, утечка информации за счет оптического излучения может иметь место из-за наличия постоянных и разъемных соединений оптических волокон, а также изгибов и повреждений этих волокон [15, 21, 22].

Рассеяние излучения при вводе оптического сигнала в интегрально-оптический волновод связано с тем, что пучок излучения используемых источников имеет заметно большую ширину, чем толщина световодного слоя волновода [21]. Эффективность ввода излучения источника в световод зависит от степени согласования их характеристик: сечения и расходимости светового пучка с геометрическими размерами сердцевины и апертурного угла световолокна, количества волноводных мод и т.д. [21]. Увеличение эффективности ввода излучения в световод достигается применением оптического клея, микролинз и других средств фокусировки излучения. Наибольшее влияние на эффективность ввода излучения источника в световод оказывает поперечное рассогласование, меньшее - продольное и угловое [21]. В диэлектрическом волноводе [24] толщиной порядка длины распространяющейся в нем волны (1 - 10 мкм) в зависимости от соотношения показателей преломления волноводного слоя (сердцевины), оболочки и покровного слоя, а также от угла падения световой волны на границе раздела волна может либо канализиро-

ваться в волноводном слое (распространяться вдоль волокна путем многократных отражений от границы сердцевина - оболочка (луч 1, см. рис. 124), либо проникать в оболочку, распространяться вдоль неё и далее выходить в окружающую среду (лучи 2, 3).

В прямолинейных световодах излучение в окружающую среду незначительно. Однако в местах изгибов волноводов интенсивность излучения в оболочку или воздух увеличивается, и тем больше, чем сильнее эти изгибы. Интенсивность излучения в окружающее пространство увеличивается и при повреждении оболочки световода.

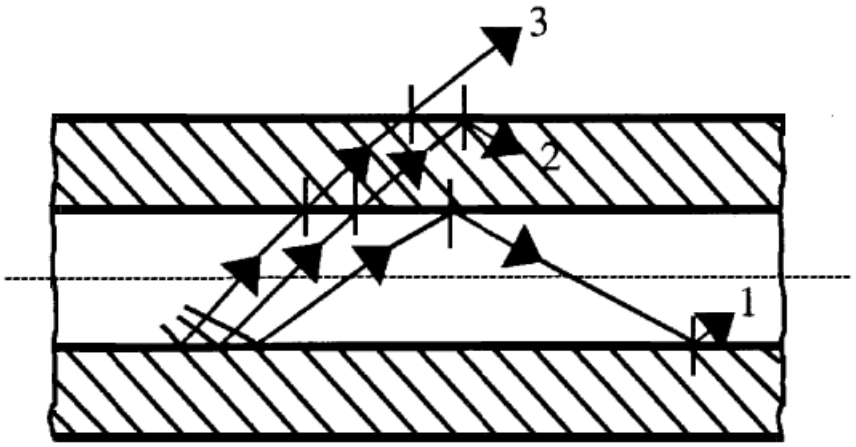

Рис. 124. Прямолинейных световод

Постоянные соединения отрезков оптических волокон между собой осуществляют свариванием, сплавлением или склеиванием в котировочном устройстве. Оптические разъемы (соединители) должны допускать многократные соединения-разъединения оптических волокон. Рассогласование волокон возникает из-за имеющихся различий в числовой апертуре, профиле показателя преломления, диаметре сердцевины или из-за погрешностей во взаимной ориентации волокон при их соединении. Основными причинами излучения световой энергии в окружающее пространство в местах соединения оптических волокон являются [15, 23]:

- Смещение (осевое несовмещение d) стыкуемых волокон (см. рис. 125).

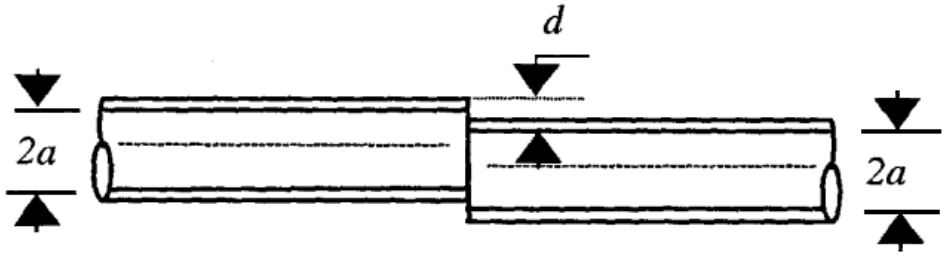

Рис. 125. Смещение стыкуемых волокон

- Наличие зазора шириной S между торцами стыкуемых волокон (см. рис. 126).

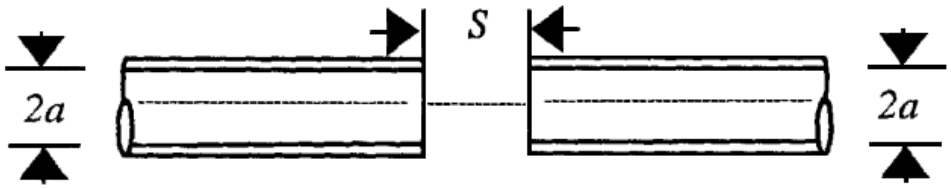

Рис. 125. Наличие зазора

- Непараллельность $\alpha > 0$ торцевых поверхностей стыкуемых волокон (см. рис. 126).

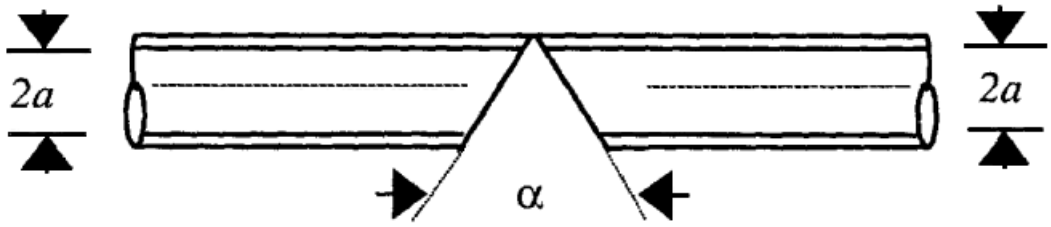

Рис. 126. Непараллельность торцевых поверхностей

- Угловое рассогласование осей стыкуемых волокон (см. рис. 127);

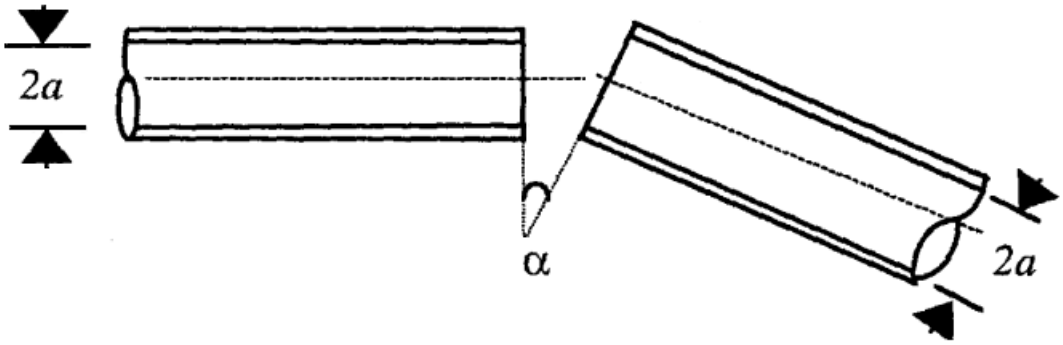

рис. 127. Угловое рассогласование осей

- Различие в диаметрах стыкуемых волокон (см. рис. 128).

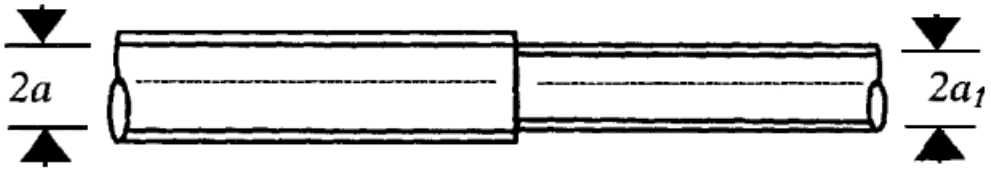

Рис. 128. Различие волокон в диаметрах

Исследования показывают [23], что наиболее интенсивное излучение в окружающее пространство наблюдается при наличии сдвига соединяемых волокон относительно друг друга.

Еще одна причина утечки информации в волоконно-оптических линиях может быть связана с возможным воздействием внешнего акустического поля (поля опасного сигнала) на волоконно-оптический кабель. Звуковое давление акустической волны может вызвать изменение геометрических размеров (толщины) или смещение соединяемых концов световодов в разъемном устройстве относительно друг друга. Вследствие этого может осуществляться амплитудная модуляция опасным сигналом излучения, проходящего по волокну. Глубина модуляции определяется силой звукового давления, конструкцией и свойствами волокна [15].

7. ПЕРЕХВАТ ИНФОРМАЦИИ В ЛИНИЯХ СВЯЗИ

В этой главе рассмотрим потенциальные возможности перехвата речевой информации, передаваемой по телефонным и телеграфным линиям.

7.1. Зоны подключения

Телефонную систему связи представляют в виде нескольких условных зон (см. рис. 95). К зоне «А» относится сам телефонный аппарат (ТА) абонента. Сигнал от аппарата по телефонному проводу попадает в распределительную коробку (РК) - зона «Б», и оттуда в магистральный кабель - зона «В». После коммутации на автоматической телефонной станции (АТС) - зона «Г» сигнал распространяется по многоканальным кабелям - зона «Д», либо по радиоканалу - зона «Е» до следующей АТС. В каждой зоне имеются свои особенности по перехвату информации, но принципы, на которых построена техника несанкционированного подключения, мало отличаются.

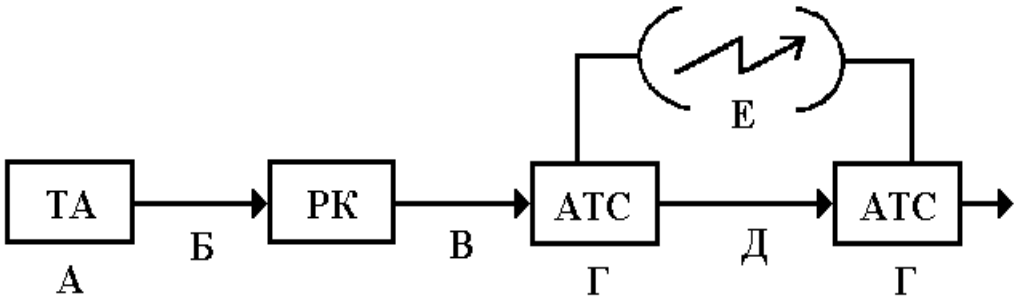

Рис. 95. Основные зоны перехвата информации в каналах телефонной связи

Наиболее опасными зонами, с точки зрения вероятности применения подслушивающих устройств, считаются зоны «А», «Б» и «В».

Что собой представляет зона «А» общеизвестно, поэтому рассмотрим состав только линейных сооружений связи городских телефонных сетей (ГТС), куда входят: абонентские линии, телефонная канализация со смотровыми устройствами и оконечное распределительное оборудование.

Телефонные линии служат для подключения аппаратов абонентов к городской АТС или телефонной подстанции и обычно состоят из трех участков (рис. 96): магистрального (от АТС до распределительного шкафа, РШ), распределительного (от РШ до распределительной коробки) и абонентского (от РК до телефонного аппарата).

Два последних участка (распределительный и абонентский) имеют сравнительно небольшую протяженность (80 % линий длиной до 3 км), но именно они являются наиболее уязвимыми с точки зрения возможного

перехвата информации. Вследствие чего рассмотрим их структуру более подробно.

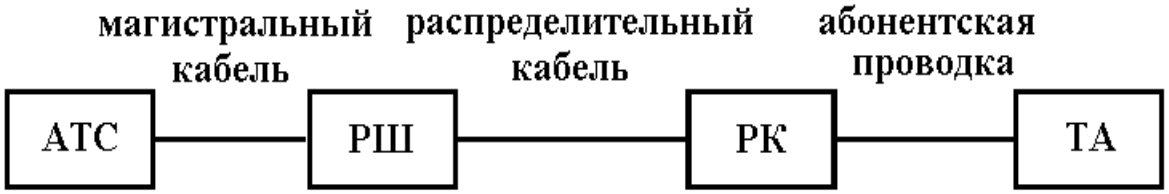

Рис. 96. Основные элементы сети АТС-абонент

По системе построения телефонные линии разделяют на шкафные и бесшкафные, а по условиям прокладки — на подземные в специальной телефонной канализации, подземные в коллекторах и тоннелях, подземные бронированные, подводные, воздушные стечные, воздушные столбовые, настенные открытой прокладки, настенные скрытой прокладки и т. д.

На телефонных линиях, построенных по шкафной схеме, применяют следующее оконечное распределительное оборудование: боксы распределительных шкафов и распределительные коробки. На линиях, построенных по бесшкафной схеме, обычно используют кабельные ящики. Выпускаются распределительные шкафы типа РШ для размещения боксов общей емкостью 600 и 1200 пар, которые устанавливаются вне зданий, и распределительные шкафы типа РШП для размещения боксов общей емкостью 150, 300, 600 и 1200 пар, устанавливаемые внутри зданий. Стандартные распределительные телефонные коробки типа РК емкостью 10 пар устанавливаются внутри зданий на лестничных клетках, в коридорах, специальных слаботочных совмещенных шкафах и нишах.

В сетях, построенных по бесшкафной схеме (что характерно для воздушных линий связи), используются кабельные ящики типа ЯКГ емкостью 10 и 20 пар, устанавливаемые непосредственно на опорах или чердаках одно- и двухэтажных зданий. Распределительные шкафы и кабельные ящики предназначены для соединения (кроссировки на боксах) магистральных и распределительных кабелей ГТС с целью наиболее экономичного построения и эффективного использования линейно-кабельной сети.

Знание структуры линии является определяющим при принятии решения об использовании того или иного типа аппаратуры перехвата.

7.2. Перехват телефонных переговоров в зонах «А», «Б», «В»

Способ непосредственного подключения

Это самый распространенный и простой способ подслушивания телефонных разговоров. Для негосударственных организаций, занимающихся

промышленным шпионажем, реально доступным местом подключения для перехвата информации являются зоны «А», «Б» и «В». Подключение бывает контактным и бесконтактным.

Шунт подслушивающего устройства в зонах «А» и «Б» может быть установлен в любом месте, где есть доступ к телефонным проводам или телефонному аппарату: в телефонной розетке или в любом другом месте телефонной линии на всем ее протяжении вплоть до распределительной коробки. В зоне «В», при использовании магистрального кабеля, подключение подслушивающего устройства маловероятно. Это связано с тем, что для этого необходимо проникать в систему телефонной канализации, то есть в систему подземных сооружений, состоящую из одной или нескольких объединенных в блоки труб и смотровых устройств (колодцев), предназначенную для прокладки кабеля, его монтажа и осмотра. Таким образом, необходимо не только разобраться в хитросплетениях подземных коммуникаций, но и определить в многожильном кабеле нужную пару среди сотен и сотен ей подобных. При использовании воздушной линии задача значительно упрощается. Поэтому, когда вы принимаете решение, что использовать для телефонизации, например, вашего дачного поселка: подземный кабель или дешевую «воздушку», то помните и о вопросах безопасности. Подземные кабели любителям да и многим спецслужбам пока не по зубам, однако, по мере роста профессионализма «шпионов» и улучшения качества защиты зон «А» и «Б», зона «В» со временем тоже станет достаточно активно использоваться для проведения разведывательных операций. В техническом плане самым простым способом незаконного подключения в зоне «Б» и «В» является контактное подключение (см. рис. 97).

Наиболее распространенный случай среди непрофессионалов — установка стационарного параллельного телефона. Возможно и временное подключение в любом месте абонентской проводки с помощью стандартного тестового телефона («монтерской» трубки) через обычный резистор номиналом 0,6-1 кОм с помощью двух иголочек. Еще проще произвести подключение к РК или РШ. Но это слишком примитивные методы. На практике такое подключение используют только непрофессионалы, поскольку очень велик риск быстрого обнаружения.

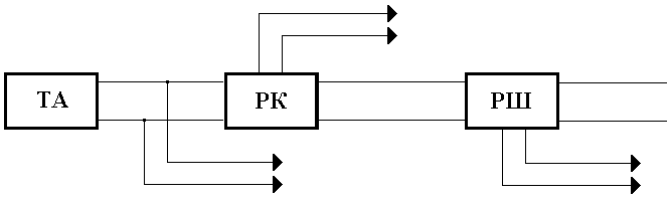

Рис. 97. Контактное подключение к телефонной линии

Подключение к воздушной линии гораздо безопаснее и может производиться следующим образом: прокладывается пара очень тонких (с человеческий волос) покрытых лаком проводов от телефонной жилы или от монтажа лепестков распределительного ящика вниз по трещине деревянного столба к соседнему арендованному заранее помещению, где находится оператор, осуществляющий перехват.

Однако подключение такого типа имеет существенный недостаток: его довольно легко можно обнаружить из-за сильного падения напряжения, приводящего к заметному ухудшению слышимости в основном телефонном аппарате, что является следствием подсоединения дополнительной нагрузки. В связи с этим более эффективным является подключение с помощью согласующего устройства (см. рис. 98). Такой способ меньше снижает напряжение в телефонной линии, что значительно затрудняет обнаружение факта подключения к линии, как самим абонентом, так и с помощью аппаратуры контроля.

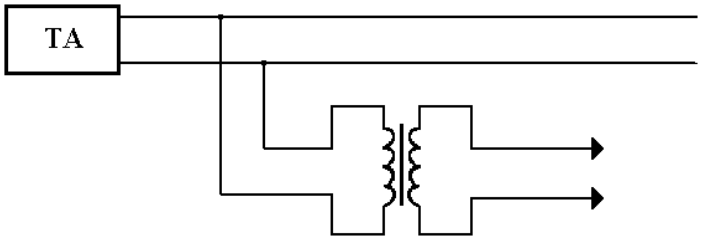

Рис. 98. Подключение к телефонной линии через согласующее устройство

Известен и способ контактного подключения к линиям связи с полной компенсацией изменения напряжения. Подслушивающая аппаратура и компенсирующий источник напряжения при этом способе должны подключаться к линии последовательно, как это показано на рис. 99. Общим недостатком всех видов контактного подключения является необходимость нарушения целостности провода и влияние подключенного устройства на характеристики линии связи.

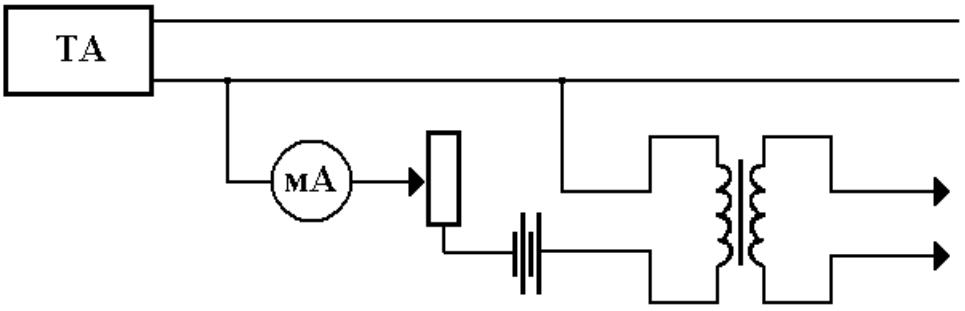

Рис. 99. Подключение к телефонной линии с полной компенсацией падения напряжения

Подключение бесконтактным методом

В целях устранения недостатка, связанного с влиянием подключенного устройства на характеристики линии связи, используют бесконтактный метод, при этом для съема информации обычно применяется индуктивный датчик, выполненный в виде трансформатора (см. рис. 100).

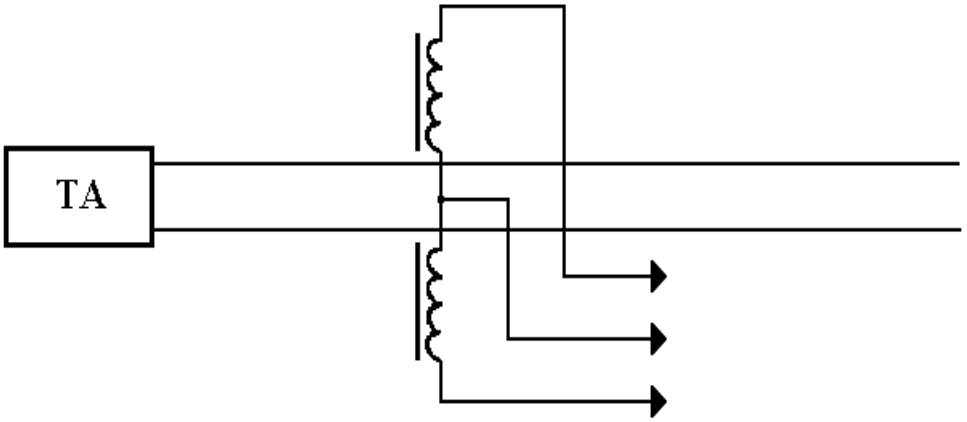

Рис. 100. Способ подключение к телефонной линии с помощью индуктивного датчика

При расположении такого устройства вблизи телефонной линии в нем будет наводиться напряжение, величина которого определяется мощностью передаваемого по линии сигнала и близостью обмоток датчика к проводам контролируемой линии. Однако в этом случае для нормальной работы устройства необходим усилитель звуковой частоты.

Иногда используются более сложные датчики, основанные на эффекте Холла (например, изделие **PRO 1219**). Датчик представляет собой тонкую прямоугольную пластину (площадью несколько квадратных мм) или пленку, изготовленную из полупроводника (Si, Ge, InSb, InAs) и имеет четыре электрода: два для подвода тока подмагничивания и два для съема информации. Чтобы избежать механических повреждений, пластинки монтируют (а пленку напыляют в вакууме) на прочной подложке из диэлектрика (слюда, керамика). Чтобы получить наибольший эффект, толщина пластины (пленки) делается возможно меньшей. Для повышения чувствительности датчик иногда монтируется в зазоре ферро- или ферромагнитного стержня. Внешний вид индуктивных датчиков показан на рис. 101 и 102.

Рис. 101. Датчик «КЛИПСА»

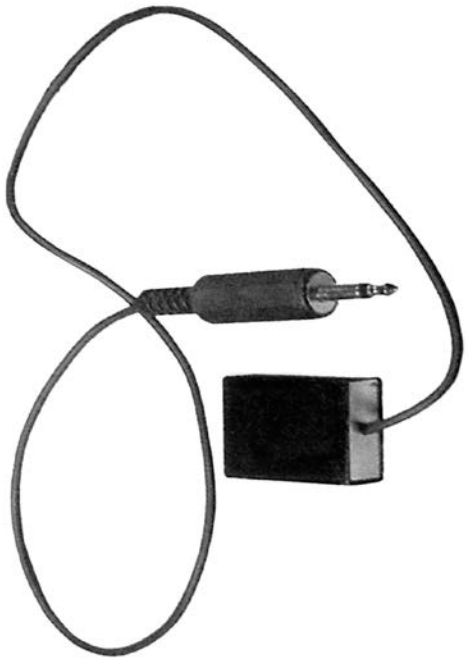

Рис. 102. Датчик «ТРАМПЛИН»

На рис. 103 и 105 показаны способы подключения индуктивных датчиков к кабелю.

Рис. 103. Подключение к телефонной линии в зоне «Б»

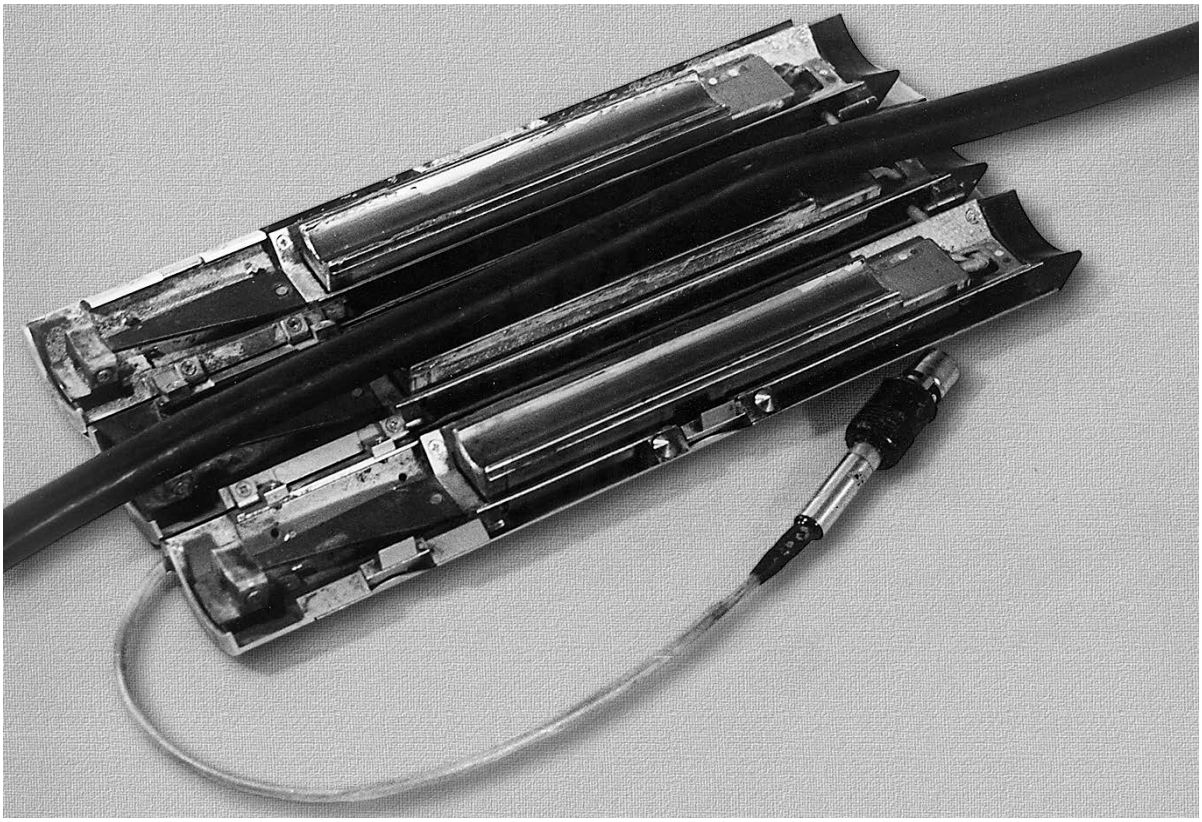

Рис. 104. Монтаж индуктивного датчика к телефонной линии в зоне «В»

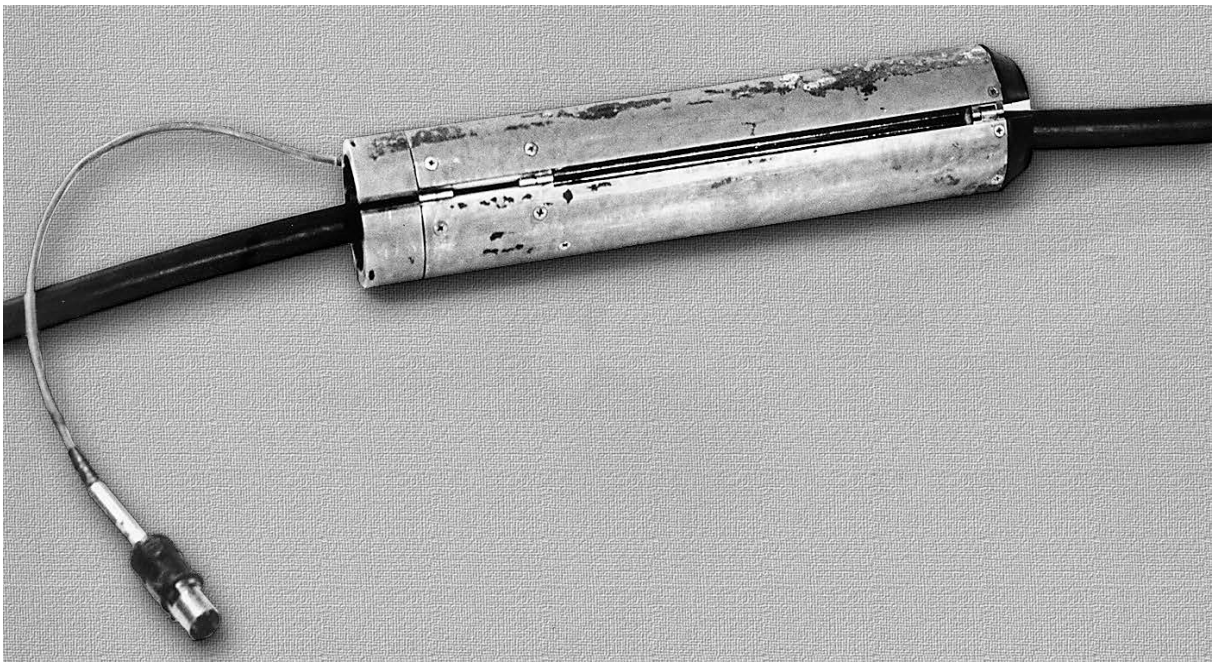

Рис. 105. Подключение к телефонной линии в зоне «В»

Качество принимаемого сигнала определяется не только подбором характеристик индукционного датчика, но также коэффициентом усиления и настройкой усилителя низкой частоты. При этом обязательно надо иметь регулируемую полосу пропускания. Это позволяет легко отфильтровать другие сигналы, наводки и помехи.

Подобные усилители в любом случае должны располагаться на выходе всех типов датчиков, что необходимо для оперативного прослушивания интересующего разговора. Должно быть предусмотрено и наличие гнезд для подключения магнитофона.

Впрочем, присутствие оператора совсем необязательно: в России имеется значительное количество датчиков для перехвата информации с телефонных линий в комбинации с диктофоном. Работа этой системы организована таким образом, что запись включается только при появлении сигнала в линии. Характеристики наиболее распространенных датчиков подобного типа приведены в табл. 17.

Таблица 17.

Марка	Габариты, мм	Питание	Дополнительные функции
ЛСТ-АД	45×35×5	Автономное	Автоматическое вкл./выкл.
ЛСТ- АД- 11	45×35×5	3 В / 220 В	Автоматическое вкл./выкл.
ЛСТ-АД-2	-	-	Автоматическое вкл./выкл.
ТТ-3	35×25×20	-	Автоматическое вкл./выкл.
БД-1	-	Автономное	Индуктивный датчик
PRO 1213	95×58×25	Автономное, 9 В	Индуктивный зонд
PRO 1213	95×58×25, 50×22×10	Автономное, 9 В	Эффект Холла
STG 4525	125×75×25	Автономное, 9 В	Индуктивный зонд
PRO 124	80×60×20	Автономное, 9 В	Регулируемая чувствит.
PK135S	16×35	Не требуется	Акустомат
UM 122	100×50×18	Автономное, 3 В	Контакт, Игла
УПМ-3	50×20×20	Автономное, 9 В	-

Стоимость подобных устройств колеблется от $20 до $250. В качестве записывающих устройств используются стандартные диктофоны типа SONY, Olympus и др. В них применяются 90-минутные микрокассеты, что позволяет на минимальной скорости записывать до 3 часов телефонных переговоров. Ряд фирм выпускает магнитофоны с встроенными адаптерами для подключения к линии (табл. 18).

Схемы последовательного и параллельного адаптеров приведены на рис. 106, 107. В обоих случаях оператору достаточно просто произвести подключение к линии (в некоторых моделях только положить прибор на провод) и нажать кнопку «Запись».

Таблица 18.

Марка	Габариты, мм	Питание	Время записи, ч	Дополнительные функции
ТТ-1	-	Автономное	2	Автомат, включение
PRO153	-	Автономное, 220 В	6	2 скорости, Акустомат
АД-3	220×160×50	Автономное, 220 В	12	Акустомат, перемотка с памятью
СМВ-500	-	Автономное	24	Акустомат

Главным недостатком указанных методов является необходимость иметь постоянный доступ в контролируемое помещение для смены кассет. Если это организовать невозможно, то применяют аппаратуру, передающую перехваченную информацию по радиоканалу.

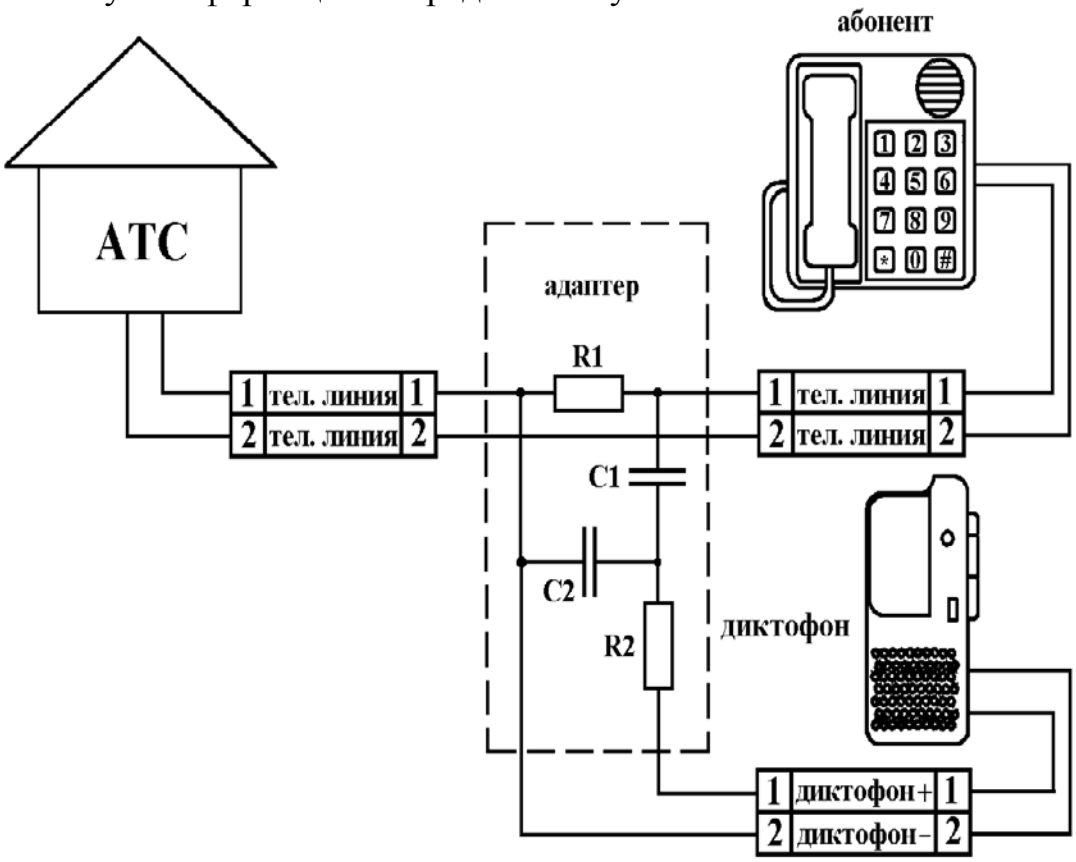

Рис. 106. Схема адаптера последовательного типа для подключения диктофона к телефонной линии связи, ток потребления не более 5 мА

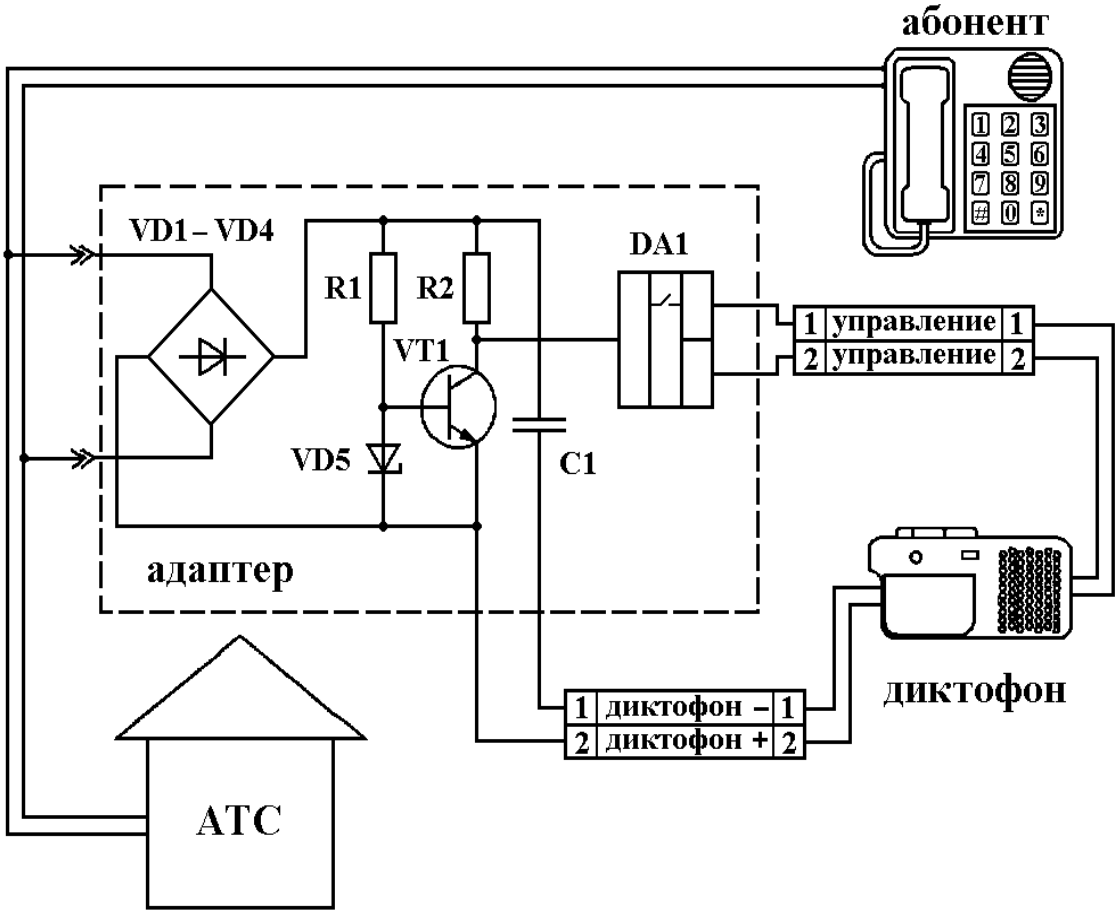

Рис. 107. Схема адаптера параллельного типа для подключения диктофона к телефонной линии связи, ток потребления не более 1 мА

7.3. Телефонные радиозакладки

Телефонные закладки подключаются в любом месте телефонной линии и имеют практически неограниченный срок службы, так как питаются от контролируемой сети. Эти изделия чрезвычайно популярны в промышленном шпионаже благодаря простоте и дешевизне (от $ 9 до $ 400).

Конструктивные особенности телефонных радиозакладок

Большинство телефонных закладок автоматически включаются при снятии трубки и передают по радиоканалу телефонный разговор на пункт перехвата, где он может быть прослушан и записан. Такие устройства используют микрофон телефонного аппарата и не имеют своего источника питания, поэтому их размеры могут быть совсем небольшими. Обычно в качестве антенны используется сама телефонная линия. Это связано с тем, что специальная антенна является демаскирующим признаком, а кроме того от ее длины, согласования и правильной ориентации при установке напрямую зависит вы-

ходная мощность передатчика. Схема простейшей телефонной радиозакладки приведена на рис. 108.

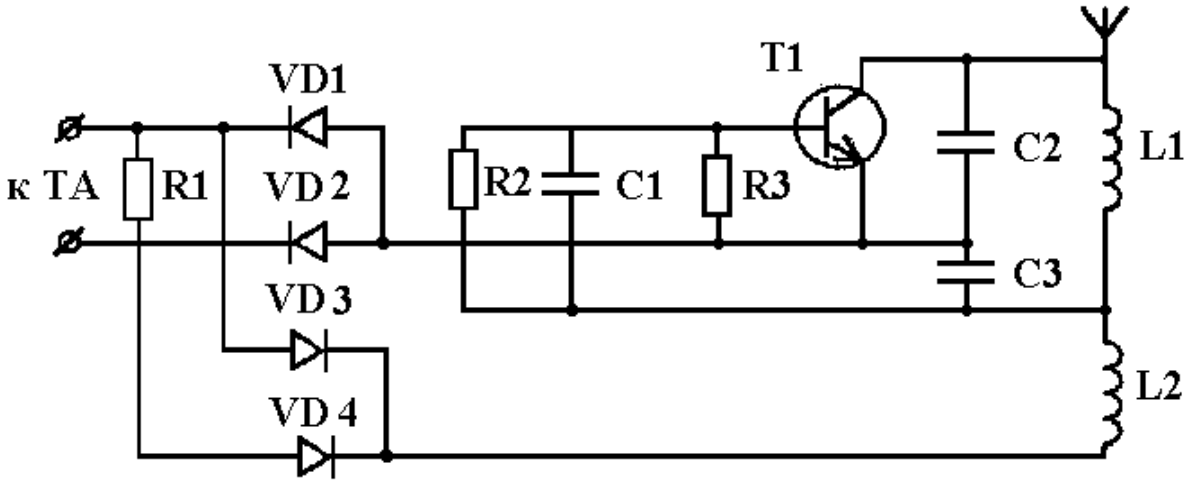

Рис. 108. Радиотелефонная закладка

Наибольшее распространение в России среди любителей получили дешевые изделия типа ЛСТ–5. При габаритах 22×14×13 мм эта закладка излучает сигнал на фиксированной частоте в диапазоне 60-170 МГц, который может быть принят на расстояние до 400 м, а при подключении внешней антенны – даже до 1000 м. Предусмотрена и возможность изменения частоты в пределах ± 10 МГц. Стоимость подобных изделий колеблется в районе $7-$30.

Параметры телефонных сетей в России имеют большой разброс и далеко не всегда соответствуют принятым стандартам. Поэтому из-за нестабильного напряжения питания возможно изменение частоты передатчика в пределах до 1% от номинала, что осложняет процедуру «вхождения в связь». Во избежание этого используются телефонные радиозакладки со стабилизацией несущей частоты. Для этого обычно применяются кварцевые резонаторы. Как правило, предлагаются изделия, работающие в диапазонах частот 100-150; 380-470 МГц. Конструкция прибора при этом существенно усложняется, стоимость вырастает до $40-$200, но потребительские качества значительно улучшаются. Не нужно судорожно «шарить в эфире» и гадать: ушла частота или выдерживается пауза в разговоре. В последние год - два телефонные радиозакладки с кварцевой стабилизацией частоты господствуют на рынке подобной спецтехники.

Выходная мощность передатчика в значительной степени определяется током потребления. Не рекомендуется увеличивать его более 2 мА, что определяется параметрами телефонной линии. Для большинства случаев развиваемой при этом мощности достаточно. Однако иногда возникают особые условия, например, возможна установка закладок внутри замкнутых металличе-

ских контуров (распределительных шкафов и т. д.), что приводит к снижению дальности перехвата в 2-7 раз. В этом случае возникает необходимость в использовании автономного питания. С целью упрощения подключений такого подслушивающего устройства и уменьшения его влияния на телефонную линию, а, следовательно, и снижения вероятности обнаружения, часто применяется индуктивный датчик съема информации. Характерной особенностью подобных устройств является наличие собственного источника питания, что побуждает применять и системы автоматического включения передатчика в режим излучения только при снятии трубки телефонного аппарата. Качество перехватываемой информации практически всегда значительно хуже, чем у закладок с прямым подключением.

Маскировка радиозакладок в зоне А

Для маскировки от обнаружения при визуальном контроле телефонные закладки, устанавливаемые в зоне «А», выпускаются в виде конденсаторов, фильтров, реле и других стандартных элементов и узлов, входящих в состав обычного телефонного аппарата. Некоторые изделия, например, CRISTAL фирмы SIPE, сделаны в виде действующего микрофона телефонного аппарата и могут быть установлены в трубку абонента за несколько секунд (см. рис. 109). Есть образцы, выполненные в виде телефонной розетки (см. рис. 110).

Рис. 109. Радиозакладка в виде телефонного микрофона

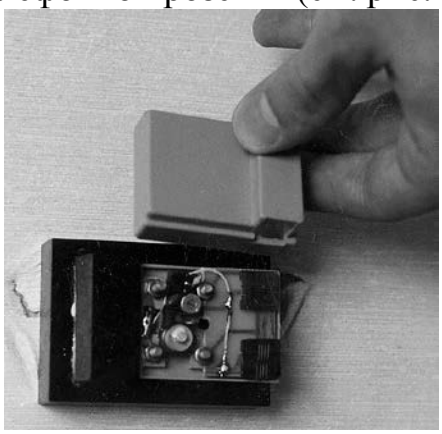

Рис. 110. Радиозакладка в переходнике на евроразъем

Серьезной проблемой при работе вне зоны «А» является выявление нужной телефонной линии. Для этих целей используются специальные тестеры, например, типа UM 011.

UM 011 – прибор с габаритами 280×60×20 мм, весом 200 г и напряжением питания 3 В. Для удобства использования он оборудован магнитной защелкой, которая позволяет установить корпус тестера на любом находящемся в месте работы металлическом предмете. В комплект входят иголки для прокалывания изоляции исследуемой проводки и специальные зажимы подклю-

чения провода тестера к этим иглам, а также светодиодный индикатор для определения состояния линии (красный — «занято», зеленый — «свободно»).

В случае, когда линия занята, прибор позволяет прослушивать разговор при помощи головных телефонов, подключаемых к гнезду «ТЛФ» тестера. А при необходимости позвонить предусмотрен номеронабиратель. Для этих же целей в комплект входит специальная перемычка для шунтирования линии в сторону контролируемого абонента, ее применение исключает возможность выявления подключения за счет случайных звуковых сигналов на телефоне абонента при работе номеронабирателя тестера.

Профессионалы стараются установить телефонные радиозакладки за пределами офиса, что существенно снижает риск. Так, по сообщениям прессы, домашний телефон главы областной администрации Воронежской области прослушивался при помощи устройства, расположенного в распределительном шкафу в подъезде дома, где живет губернатор.

Во избежание возможности случайного перехвата передаваемых по радиоканалу телефонных переговоров какой-нибудь радиоприемной аппаратурой, а значит обнаружения факта подслушивания, в профессиональных закладках используются два основных приема: шифрация сигнала и применение нетрадиционных видов модуляции.

Использование криптографической защиты существенно увеличивает стоимость и ухудшает некоторые технические параметры телефонной радиозакладки (растут габариты, энергопотребление, снижается разборчивость речи и т. д.). В связи с этим, более перспективным выглядит второй путь, то есть использование нетрадиционных для данной области видов модуляции. Например, амплитудная модуляция (АМ) с подавленной несущей или боковой полосой, использование поднесущих частот и т. д. Перспективным направлением можно считать использование шумоподобных сигналов, которые очень сложно обнаружить без знания их параметров.

Системы с ретранслятором

Одной из современных тенденций является использование системы с ретранслятором. При этом применяется простая радиозакладка с небольшим радиусом действия (обычно около 50 м). В безопасном месте устанавливается стационарный (или переносной) ретранслятор, переизлучающий сигнал закладки на значительные расстояния (до 10 км) часто на другой частоте и, возможно, в зашифрованном виде.

Для приема сигналов, излучаемых телефонными радиозакладками, используются устройства трёх основных типов: бытовые приемники и магнитолы; приемники различного назначения; специальные приемники.

Прием сигналов с помощью бытовых приемников и магнитол

К первому типу, как указано выше, относятся *обыкновенные бытовые приемники и магнитолы*. Преимущество магнитол заключается в возможности записи информации, передаваемой по радиоканалу. К плюсам таких систем можно отнести их низкую стоимость и двойное назначение, как правило, окружающие их не замечают. Обычно они не вызывают никаких эмоций даже у сотрудников служб безопасности. К минусам относятся: низкая чувствительность, что ограничивает дальность применения; использование общедоступного радиодиапазона (для отечественных приемников 62-74 МГц, для импортных 88-108 МГц), что может привести к случайному перехвату вашего канала съема информации каким-нибудь любителем «пошарить в эфире».

Частично эти недостатки возможно устранить. Для этого осуществляют перестройку входных и гетеродинных контуров, что приводит к изменению диапазона рабочих частот до 110-150 МГц у стандартных бытовых магнитол и пытаются несколько улучшить чувствительность. Другой путь связан с использованием конверторов, то есть устройств, осуществляющих перенос частоты принимаемого сигнала в рабочую область частот приемного устройства. В данном случае частотный диапазон может выбираться практически любой. При этом конверторы могут встраиваться непосредственно в приемное устройство (например, **ПРМ-450**), либо выполняться в виде отдельных блоков (например, **СО-01**, фирмы «Вече») и при работе располагаться в непосредственной близости от бытового приемника. При использовании конверторов чувствительность приемного комплекса зависит как от технических характеристик самого преобразователя частоты, так и от характеристик собственно приемника и может достигать 0,9-5 мкВ. Некоторое распространение получили конверторы с кварцевой стабилизацией частоты, которые не чувствительны к расположению окружающих предметов, в том числе, к касанию руками. В связи с этим отпала необходимость экранирования. К тому же, благодаря высокой шумовой и температурной стабильности кварцевого генератора, возможно «зафиксировать» настройку, а также значительно снизить шумы гетеродина.

Наиболее предпочтительно использование в качестве перестроенных магнитол изделия типа **Panasonic RQ-A160/A170**, **DAEWOO AHS-55W** и другой аналогичной продукции ведущих зарубежных фирм. Небольшие габариты (изделие свободно помещается в кармане куртки), относительно неплохой по чувствительности приемник и наличие возможности записи получаемой информации на стандартную кассету делают подобную аппаратуру достаточно удобной для работы с целым классом телефонных радиозакладок.

В качестве примера можно рассмотреть характеристики магнитолы AHS-55W.

AHS-55W (DAEWOO) – радиоприемное устройство, работающее в двух диапазонах частот: 88-108 МГц (FM) и 530-1605 кГц (AM). Его габариты – 112×82,5×29 мм, вес – 250 г (без батареек). В диапазоне AM используется встроенная магнитная антенна, а в диапазоне FM эту роль выполняет провод головных телефонов.

Цена подобных устройств во многом зависит от себестоимости базовой аппаратуры и колеблется в значительных пределах ($15-$400).

Хочется отметить следующее. При записи сигнала на магнитофон возможно вскрытие набираемого на телефонном аппарате номера, а при наличии установленных у абонентов средств АОН – вскрытие и номера звонящего. Для этого необходимо иметь соответствующий программно-аппаратный комплекс обработки сигналов, например, декодер телефонных номеров **РК100** (габариты – 220×140×50 мм; вес – 1,5 кг; питание – 220 В). Впрочем, при некоторых навыках определить набираемый номер можно и «на слух» притом в реальном масштабе времени.

Приемники различного назначения

Ко второму типу можно отнести *приемники различного назначения* с более широким, чем у стандартной бытовой аппаратуры, частотным диапазоном. В последнее время значительное распространение получили многодиапазонные дешевые приемники ($20-$150) производства Германии, Китая и Южной Кореи. Укажем характеристики подобных изделий на следующем примере.

Combicontrol 8000 Special (фирмы Pan International) – частотный диапазон – 54-176 МГц; габариты – 206×96×53 мм; вес – 500 г; выходная мощность низкочастотного блока – 350 мВт.

Специалисты не любят подобную технику из-за крайне низкой чувствительности и значительных габаритов. Непрофессионалов привлекает умеренность цены и простота в работе.

В конце 1991 года на отечественном рынке появились сканирующие приемники, в основном японского или немецкого производства. Сначала потенциальных покупателей отталкивала их достаточно высокая цена ($400-$2500). Однако несомненные достоинства подобной аппаратуры быстро сделали ее популярной. Имея небольшие размеры и высокую чувствительность, приемники могут использоваться с радиозакладками во всем возможном диапазоне частот и при любом виде модуляции. Наличие способности запоминать каналы и возможности сканирования по частоте позволяет работать одновременно с несколькими абонентами. Сканирование в заданной полосе по-

зволяют легко работать с изделиями, несущая частота которых нестабильна. Кроме того, открываются и другие возможности.

Технические характеристики некоторых сканирующих радиоприемников, применяемых для работы с телефонными радиозакладкамн приведены в табл. 19.

Таблица 19.

Модель	Диапазон, МГц	Вид модуляции	Чувствительность, мкВ (с/ш=12дБ)	Шаг перестройки, кГц	Количество каналов в памяти	Габариты, мм Вес, кг
IC-R1	2-905	AM, FM, WFM	0,4-3,2	0,5;1;5;8;9; 10; 12,5;15; 20;25	100	49×102,5×35 0,3
PRO-42	8-1300	AM, FM, WFM	0,5	5;10;12,5;50; 100	200	65×159×40 0,33
PRO-46	29-956	AM,FM	0,5-1,6	12,5	100	66×151×37 0,22
XR-100 STABO	0,53-1650	AM, FM, WFM, LSB, USB	0,5-10	0,05; 0,1; 1,5; 6,25; 9; 10; 12,5; 20; 25; 50; 100	1000	64,4×155×38 0,32
MVT-7000	8-1300	AM, FM, WFM	0,5-1	0,01; 0,1; 1; 5; 9; 10; 12,5; 20; 25; 100	-	159×64×40 0,33
MVT-7100	8-1300	AM, FM, WFM	0,5-1	0,01; 0,1; 1; 5; 9; 10; 12,5; 20; 25; 100	-	159×64×40 0,33
AR-1500	0,5-1300	AM.FM. WFM	0,5-3	5-995 (с шагом кратным 0,05)	1000	55×151×40 0,33
AX-700E	50-904	AM, FM, WFM	0.3-6	10; 25; 1000	100	- 2
TR-980	0,03-2000	AM, FM, WFM	0,5-2	5; 10; 12,5; 25; 30	125	154×55×41 0,27
Alan 1	26-512	AM, FM	0,2-5	-	50	210×158×52 1,2
Alan 1300	8-1300	AM, FM, WFM	0,5	5-995 (с шагом кратным 0,05)	100	170×35×65 0,3
AE39H	68-	AM, FM	1	-	200	58×42×145

	960					0,25
PRO-50	68-512	AM, FM	1	-	20	60×44×160 0,26
AE44H	68-137	AM.FM	1	-	50	58×42×145 0,25
BJ-200 MK	26-520	AM, FM	0,5-1,5	5; 12,5	16	185×80×37 0,47
DJ-X1D	0,1-1299,9	AM, FM, WFM	0,25-10	5; 9; 10; 12,5; 20; 25; 30; 50; 100	100	53×110×37 0,37

Специально разработанные приемники

Настоящие профессионалы обычно используют третий тип приемников — *специально разработанных*. В качестве примера рассмотрим приемник **ЛСТ-П-3** (**ЛСТ-П-5**). Чувствительность его — порядка 1 мкВ, диапазон рабочих частот – 110-160 МГц (или 400-.450 МГц). Возможно подключение внешней антенны, например, автомобильной. Выход перехваченного сигнала – и на наушники, и на магнитофон.

Большинство специальных приемников настроено на одну частоту (в крайнем случае на 2-5 частот). Это позволяет добиться высокой чувствительности (0,5-3 мкВ при отношении сигнал/шум 20 дБ), сохраняя небольшие габариты и низкую стоимость. При создании таких приемников часто используются специализированные микросхемы (например, К174ХА26) и микросборки (например, АК9401). Технические характеристики некоторых отечественных специальных приемников, применяемые для приема излучений телефонных радиозакладок, приведены в табл. 20.

Для записи телефонных переговоров часто используются специальные комплекты. Принцип их работы можно показать на примере изделия **«Телефонный секретарь»**. В состав комплекта входит телефонная радиозакладка, устанавливаемая в разрыв линии, и приемник с магнитофоном, смонтированные в «кейсе». При поднятии абонентом телефонной трубки происходит включение передатчика закладки, автоматический захват сигнала приемником и пуск (через 2 с) пишущего магнитофонного узла. Выключение магнитофона происходит мгновенно при пропадании сигнала. Удобство в работе подобного комплекта заключается в том, что нет необходимости в нахождении оператора на пункте контроля. Возможность питания комплекта от бортовой сети автомобиля 12 В позволяет осуществлять запись телефонных переговоров из машины, припаркованной недалеко от объекта контроля. Цена подобных изделий колеблется в пределах $100-$8000.

Таблица 20.

Модель	Диапазон, МГц	Чувствительность, мкВ (с/ш=20 дБ)	Тип антенны	Вид модуляции	Питание, В	Габариты, мм
ПРМ-М1	100-115	2-3	телеск.	ЧМ	3	135×60×18
ПРМ-1	100-115	1-3	штырь	ЧМ	4,5	-
UM100	105-108	0,5-1	штырь	ЧМ	6	-
UM101	108-112	0,5-1	штырь	ЧМ	9	-
ПРМ-М3	108-115	1	штырь	ЧМ	6	-
ЛСТ-П1	110-150	1	телеск.	ЧМ	9	140×60×20
ПРМ-2	115-130	1-3	штырь	ЧМ	4,5	135×60×18
ПРМ-3	130-150	1-3	штырь	ЧМ	4,5	-
ПРМ-К	130-170	1	штырь	УЧМ	6	150×60×20
ПРМ-М3	135-150	1	штырь	ЧМ	6	-
UM100,2	136-144	0,5-1	штырь	ЧМ	6	-
UM042,1	136-144	0,5	штырь	УЧМ, ЧМ	12	140×95×30
РП-Ш270	260-280	3	телеск.	ЧМ	9	-
RA-04	367-397	2	-	ЧМ	6	-
RA-05	375-385	2	штырь	ЧМ	10	-
RA-07	368-392	2	-	ЧМ	7	115×55×22
ПРМ	391 (417)	0,6-0,8	штырь	УЧМ	6	80×48×12
UM042,2	412-430	0,5	штырь	УЧМ, ЧМ	12	108×67×28

Значительное место на рынке занимают комбинированные системы типа **ЛСТ-4**, которые позволяют осуществлять перехват как телефонных переговоров при поднятой трубке, так и разговоров в помещении при положенной трубке. Питание производится от телефонной линии. Однако дальность передачи информации небольшая, так как нежелательно увеличивать потребление тока от телефонной линии.

Характеристики некоторых телефонных радиозакладок приведены в табл. 21.

Использование телефонных радиозакладок возможно и для перехвата информации, передаваемой по факсимильной или телетайпной связи. Отличие состоит только в специальном устройстве обработки сигналов. Например, портативная аппаратура **TRM 3700**, подключаемая к выходу радиоприемного устройства, позволяет записывать информацию, передаваемую по телексу, на встроенный кассетный магнитофон или распечатывать на матричном принте-

ре. Габариты системы – 475×395×180 мм, питание – 220 В, время непрерывной записи – 3 часа.

Таблица 21.

Марка	Частота, МГц	Дальность передачи, м	Габариты, мм	Вид модуляции
Телефонные радиозакладки в обычном исполнении				
ЛСТ-5	60-170	200-1000	25×13×10	ЧМ
ЛСТ-7	350-450	300	25×25×7	ЧМ
GQ-205	140-150	150	60×40×20	УЧМ
PRO 136	140-144	до 2000	40×24×12	УЧМ
PRO 139	135-180	до 500	36×12×10	УЧМ
Т1	90-118	до 300	14×13×8	ЧМ
UM 003	108-112	до 500	22×15×10	ЧМ
UM 008	136-145	до 700	22×15×10	ЧМ
РТМ-12	64-125	50	36×25×12	ЧМ
РТП-017	130	100	45×15×4	ЧМ
РТП-018	130	-	70×25×4	ЧМ
РТП-020	380-470	-	70×25×4	ЧМ
В закамуфлированном виде под конденсаторы и другие радиотехнические элементы				
НВ-ПТ	130-150	500	3×16×4	ЧМ
НВ-ПТ450	400-500	200-300		ЧМ
РК130	138	150	«рисовое зерно»	ЧМ
РК130-S	138	800	15×6×11	ЧМ
UM 008	136-145	до 700	35×15×15	ЧМ
Радиозакладки, установленные в капсулах телефонных трубок				
РК(CRISAL)	-	150	в габаритах камуфляжа	ЧМ
РК155	-	300	048×21	ЧМ
РК1 10-S	-	250	в габаритах камуфляжа	УЧМ
Комбинированные системы (телефон / микрофонные передатчики)				
ЛСТ-4	100-150	100	35×16×11	ЧМ
ЛСТ-8	350-450	200	25×25×5	ЧМ
STG-4315	115-150	100	26×22×15	ЧМ
STG-4317	395-415	100	66×27×14	УЧМ

ПТРМ	88-108 130-150	до 250 до 250	29×19×12 29×19×12	ЧМ ЧМ
PK125GHZ		500	25×20×10	-
PK125-SS	139	до 10000 с ретранслятором	-	-
Радиозакладки с индуктивным датчиком				
Ш01т	100-210	до 1000	70×38×20	ЧМ
Ш01ртм	100-210	до 1000	70×38×20	ЧМ
Ш01т	100-210	до 1000	70×38×20	ЧМ
111021т	100-210	до 1000	70×38×20	ЧМ
STG-4320	395-415	250	40×15×15	УЧМ

7.4. Перехват побочных электромагнитных сигналов и наводок

Любое электронное устройство при работе создает так называемые побочные электромагнитные излучения и наводки (ПЭМИН). Не является исключением и телефонный аппарат. Характерным примером являются широко распространенные аппараты с кнопочным номеронабирателем типа **ТА-Т, ТА-12, ТА-32** и т. д. При наборе номера и ведении переговоров, благодаря техническим особенностям блока питания, вся информация излучается на десятках частот в средневолновом, коротковолновом и ультракоротковолновом диапазонах. Это излучение может быть зафиксировано на расстоянии до 200 м. В случае применения подобного телефона радиозакладки совсем не нужны. Хочется отметить, что получившие широкое распространение телефонные аппараты с радиоудлинителем (Cordless Telephone) тоже значительно облегчают жизнь специалистам от промышленного шпионажа, так как дальность несанкционированного перехвата их довольно мощного сигнала достигает 400-800 м.

Конечно, приведенные примеры относятся к крайностям, но перехват излучений может осуществляться с помощью малогабаритного индуктивного датчика, позволяющего «улавливать» побочные электромагнитные колебания практически любого телефонного аппарата на расстоянии до метра. При этом кроме речевых сигналов регистрируются также и сигналы набора номера. В качестве датчика используется катушка индуктивности. Она может быть плоской и устанавливаться там, где ее никто искать не будет, например, под основанием телефонного аппарата или под настольным письменным прибором, а также параллельно телефонному проводу внутри стен, под карнизами и плинтусами. Недостаток способа — появление наводок от посторонних источников.

Кроме самого аппарата, телефонные провода и кабели связи тоже создают вокруг себя магнитные и электрические поля, образующие каналы утеч-

ки информации за счет наводок на другие провода и элементы аппаратуры в ближней зоне.

Влияние одной линии на другую, когда они имеют определенный параллельный пробег, известно довольно давно. Отмечен даже исторический факт, имевший место еще в 1884 году, за 11 лет до изобретения радио А. С. Поповым. В Лондоне было обнаружено, что в телефонных аппаратах на улице Грей-Стоун-Род прослушиваются телеграфные передачи из какой-то другой сети связи. Проверка показала, что виноваты заложенные неглубоко под землей телеграфные провода, идущие на большом протяжении параллельно проводам телефонным. Величина наводимой энергии на параллельные линии зависит главным образом от длины параллельного пробега и от расстояния между проводами (см. рис. 111).

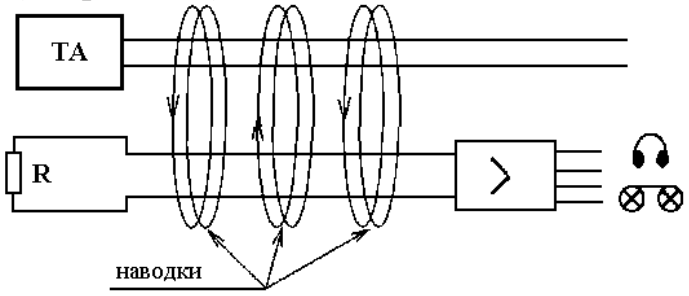

Рис. 111.Использование телефонной сети для прослушивания разговоров в помещениях

Отдельное место занимают системы, которые предназначены не для перехвата самих телефонных переговоров, а для акустического контроля помещений, где расположены телефонные аппараты или хотя бы проложены провода телефонных линий.

Поскольку именно эта тема особенно часто эксплуатируется авторами детективов, то рассмотрим этот вопрос достаточно подробно. Принципы и алгоритмы работы специальных устройств контроля помещения по телефонному каналу с дистанционным управлением проиллюстрируем на примере отечественных изделий **Elsy** и **UM 103**. «Телефонное ухо» (Elsy) подключается параллельно к телефонной линии (розетке) в контролируемом помещении (см. рис. 112).

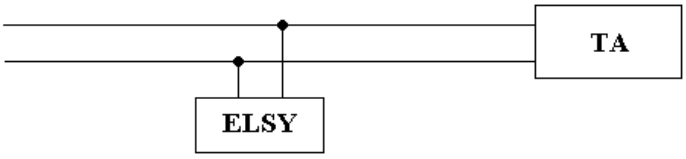

Рис. 112. Принцип применения закладного устройства типа Elsy

В принципе, наличия самого телефонного аппарата даже и не требуется, так как такая закладка может быть установлена в любом месте телефонной линии в пределах контролируемого помещения, например, в телефонной розетке. Поэтому те, кто, отсоединив свой аппарат от розетки, чувствуют себя в полной безопасности, могут жестоко ошибиться.

Для прослушивания помещения необходимо позвонить по номеру телефонного аппарата (что можно сделать даже из другого города), на линии которого установлено устройство акустического контроля. После одного-двух стандартных гудков АТС «абонент не отвечает» происходит изменение их тональности, теперь необходимо произнести несколько слов (или подать любой звуковой сигнал). Акустическая закладка активируется и начнет передавать информацию из помещения по телефонной линии, притом с достаточно хорошим качеством.

Положительным моментом является то, что система питается от телефонной сети. Недостаток этих комплексов очевиден: полная зависимость от поведения абонента телефонного номера, к которому осуществлено подключение. Сдерживает их широкое применение и довольно высокая стоимость.

К зарубежным аналогам можно отнести устройство **Tele-monitor.** Единственным его отличием от вышеописанного является возможность подключения до четырех датчиков к системе на одну линию для контроля различных помещений. Кроме того, на сам телефонный аппарат три первоначальных звонка вообще не проходят.

Изделие UM 103 подключается аналогично Elsy, но имеет выносной микрофон (рис. 113), что упрощает маскировку самого прибора в помещении.

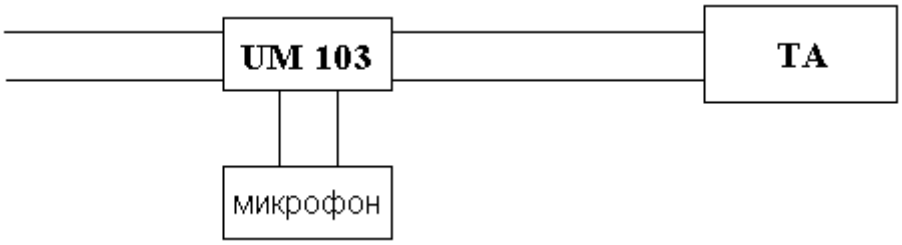

Рис. 113. Принцип применения закладного устройства типа UM 103

Алгоритм функционирования изделия следующий: при поступлении сигнала вызов на аппарат контролируемого абонента UM 103 «проглатывает» первые два звонка, после чего телефонный аппарат совершенно нормально работает. Для включения устройства необходимо позвонить контролируемому абоненту, подождать гудка станции, положить трубку, отсчитать нужное количество секунд (индивидуальный временной код доступа) и набрать его телефон снова. В трубке будет слышен сигнал «занято». Необходимо подож-

дать 45 с и UM 103 включится на прослушивание. Стоимость такого комплекта – порядка $5000.

Однако высокая цена «фирменной» аппаратуры не должна настраивать вас на мажорный лад: как это не покажется парадоксальным, но изготовить упрощенную версию прибора этого типа может даже радиолюбитель «средней руки». Устройство состоит из двух частей: приемно-передающего блока, устанавливаемого на контролируемом объекте, и мини-передатчика звуковых сигналов (бипера), включающего этот блок.

Принцип действия аппаратуры прост. Приемно-передающий блок в любом удобном месте подсоединяют параллельно к телефонной линии и подают на него напряжение питания от сети 220 В или от автономного источника +12 В. Теперь достаточно только позвонить по «зараженному» номеру с любого телефона и, услышав гудки «абонент не отвечает», прислонить к микрофону своей трубки включенный бипер. Дальше происходит следующее. В работу включается трансформатор *T1* (конденсаторы *C1* и *C2* в его первичной обмотке препятствуют шунтированию линии) и передает сигнал с обмотки *II* на трехкаскадный усилитель (транзисторы *VT1–VT3*). Усиленный сигнал следует на селективное реле *K1*. Последнее включает реле времени *K2*, определяющее промежуток времени, в течение которого устройство будет работать на передачу. Этот интервал устанавливается с помощью потенциометра *R10*. После включения реле *K2* блокирует себя контактами *K2.1*, контактами *K2.2* включает передатчик, а контактами *K2.3* имитирует снятие трубки, чтобы подключить на АТС к линии звонивший телефон. Передатчик состоит из микрофона *BM1* с двухкаскадным усилителем (транзисторы *VT8* и *VT9*), устройства коррекции, представляющего собой заградительный фильтр, и двухкаскадного оконечного усилителя (транзисторы *VT10 – VT12*). Нагрузкой выходного каскада, собранного по двухтактной схеме, служит обмотка *III* трансформатора *T1*, через которую сигнал с микрофона поступает в телефонную линию.

Детали, используемые в устройстве, – самые типовые, широко распространенные. Трансформаторы *T1* и *T2* идентичны промышленному Б-22. Реле легко изготовить из трех герконов, работающих на размыкание. Налаживание системы заключается в настройке передатчика на частоту 1000 Гц и доводке приемного устройства, которая сводится к регулированию селективного реле с помощью конденсатора *C10*. Что касается бипера, то он – не что иное, как типичный мультивибратор, нагруженный на динамик ДЭМ-4М.

Кроме того, возможно использование телефонной линии и для постоянной передачи информации с микрофона, установленного в помещении. Чтобы «не засветить» микрофон, используется несущая частота в диапазоне от десятков до сотен килогерц с целью не препятствовать нормальной работе телефонной связи. Одним из вариантов реализации подобной системы является

комплект **ST-01**, состоящий из приемника и датчика. Датчик типа **P10** устанавливается в телефонной розетке. Для передачи используется частота 100 ±10 кГц. Модуляция – частотная. Ток потребления – не более 2,5 мА.

Приемник сигналов **ST-01** имеет:

- систему автоматической регулировки уровня сигналов на выходе;
- ручную регулировку уровня сигнала на головных телефонах;
- регулятор тембра голоса;
- систему контроля состояния элементов питания;
- систему контроля наличия несущей частоты в телефонной линии;
- систему контроля наличия информационного сигнала.

Для регистрации информации к приемнику подключаются наушники или диктофон. Частотный диапазон приемника на линейном выходе по уровню 6 дБ и 300-3300 Гц. Дальность передачи не превышает 200 м, поскольку ВЧ-сигналы сильно затухают в телефонной линии.

Практика показывает, что в реальных условиях дальность действия подобных систем с приемлемой разборчивостью речи может быть еще меньше и существенно зависит от целого ряда факторов: качества телефонной линии; способа прокладки телефонных проводов; наличия в данной местности радио-трансляционной сети; наличия вычислительной и иной техники и т. д. Главным недостатком этого типа аппаратуры, помимо высокой стоимости, является большое количество времени, затрачиваемого на ее установку и необходимость проникновения в контролируемое помещение.

Для любого специалиста, работающего в области промышленного шпионажа с применением технических средств разведки, представляют наибольший интерес так называемые «беззаходовые» системы, то есть комплексы средств, позволяющие получать информацию из интересующих помещений без необходимости физического проникновения в них, которое зачастую просто невозможно. Телефонный аппарат предоставляет в этом плане определенные возможности. Неслучайно даже некоторые высокопоставленные чиновники опасаются вести компрометирующие разговоры в собственных кабинетах, кивая при этом на телефонный аппарат. Этот, конечно же, сильно преувеличенный страх нельзя считать совершенно беспочвенным, поскольку есть три потенциально возможных варианта прослушивания помещения с помощью телефона:

- телефонный аппарат содержит систему передачи информации, то есть в его конструкцию целенаправленно внесены соответствующие изменения или просто установлена специальная аппаратура типа описанной выше;
- используются определенные недостатки конструкции стандартного телефонного аппарата;

- производится такое внешнее воздействие на телефонный аппарат, при котором он превращается в канал утечки акустического сигнала из помещения.

Так как первый случай достаточно подробно уже рассмотрен, познакомимся с возможностями, которые дает применение второго варианта.

Причиной возникновения канала утечки информации в этом случае являются электроакустические преобразования, возникающие в некоторых узлах телефонного аппарата, например в катушке звонка. При разговоре акустические волны воздействуют на маятник звонка, который в свою очередь соединен с якорем электромагнитной катушки. Под этим воздействием якорь совершает микроколебания, а это вызывает колебание якорных пластин в электромагнитном поле катушки, что приводит к появлению в цепи звонка наведенных токов, модулированных речью. Как известно, цепь звонка при положенной трубке непосредственно включена в линию.

По данным специальных исследований, амплитуда сигнала, наводимого в линии, для некоторых типов телефонных аппаратов может достигать нескольких милливольт. Для приема этих наводок может быть использован обыкновенный усилитель низкой частоты (УНЧ) с диапазоном 300-3500 Гц, который просто подключается к абонентской линии (см. рис. 114). В качестве такого приемника возможно, например, использование многофункционального УНЧ типа **UM 053** с коэффициентом усиления порядка 7000. Батарея напряжением в 9 В обеспечивает непрерывную работу прибора, имеющего габариты всего 150×65×30 мм, в течение 50 часов.

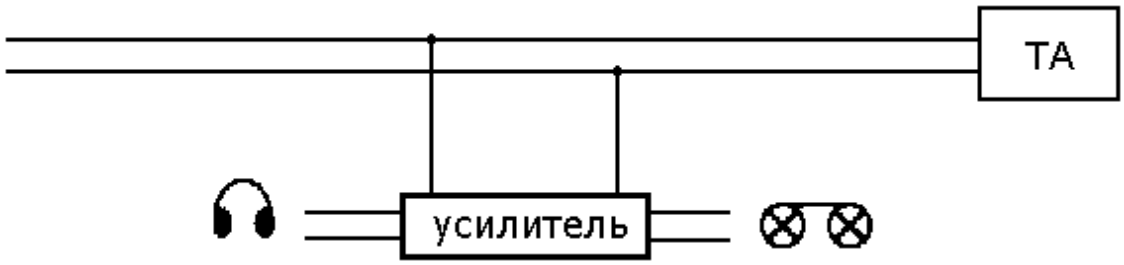

Рис. 114. Прием информационных сигналов, возникающих в результате акусто-электрического преобразования

Недостатком этого, на первый взгляд, очень перспективного, способа является то, что сигнал в большинстве случаев слишком слабый, и дальность действия подобной системы даже с хорошей аппаратурой не превышает нескольких десятков метров (зона «Б»). Данное обстоятельство существенно снижает практическую ценность второго варианта в реальных условиях.

Третий вариант получения информации связан с явлением так называемого ВЧ-навязывания. Работа системы показана на рис. 115.

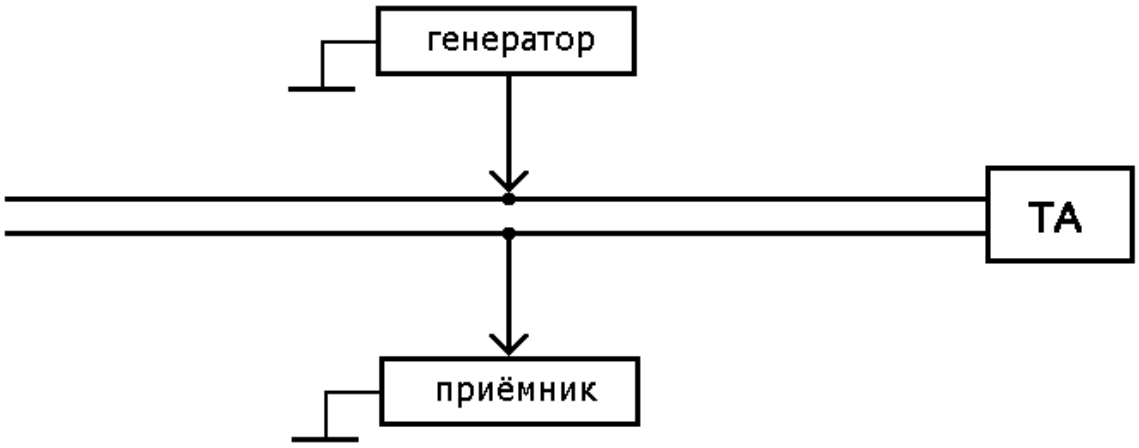

Рис. 115. Реализация принципа высокочастотного навязывания в телефонных линиях связи

Принцип заключается в том, что относительно общего корпуса (в качестве которого лучше использовать землю, трубы отопления и т. д.) на один провод подается ВЧ-колебание с частотой от 150 кГц и выше. Через элементы схемы телефонного аппарата, даже если трубка не снята, а значит отсоединена от сети, зондирующее ВЧ-излучение все-таки поступает на телефонный микрофон, где и модулируется речью. Прием информации производится относительно «общего корпуса» через второй провод линии. Амплитудный детектор позволяет выделить низкочастотную огибающую для дальнейшего усиления и записи. Очевидно, что для повышения качества перехватываемой информации желательно производить подключение как можно ближе к телефонному аппарату (опять зона «Б»), что существенно снижает эффективность применения системы.

7.5. Перехват телефонных переговоров в зоне «Г»

В этом случае наиболее безопасно организовать стационарное прослушивание телефонных разговоров, что достаточно просто сделать на телефонной станции (коммутаторе). В народе бытует мнение, что на телефонных станциях сутками напролет сидят представители спецслужб и прослушивают все переговоры. На самом деле это совсем не так. Во-первых, на станциях сидеть вовсе не обязательно – достаточно подключиться к единой системе АТС. Более того, прослушивать все телефонные разговоры нет необходимости. Контроль идет выборочно, по заданным номерам, так как анализ перехваченных телефонных разговоров и ведение соответствующих досье требует длительной, кропотливой работы. В связи с этим круг абонентов ограничен. Так, ЦРУ в многомиллионной Мексике контролировало в 60-е годы всего 40 телефонных номеров. При этом, наряду с дипломатами стран Варшавского Договора, прослушивались телефоны прокоммунистических организаций, мафи-

озных лидеров, а также политических деятелей и членов их семей. Кроме того, эпизодически контролировались переговоры деятелей науки и культуры с мировым именем.

Аналогичная ситуация складывалась и в бывшем СССР, где, по некоторым данным, прослушивались телефоны иностранных представительств, лиц, подозреваемых в совершении преступлений, различного рода диссидентов, а также руководителей различного ранга. Кроме того, иногда записывались разговоры родственников интересующих лиц и людей из их ближайшего окружения. Так, прослушивались переговоры парикмахера Р. М. Горбачевой, тренера Б. Н. Ельцина по теннису и т. д.

Прослушивание телефонных переговоров — достаточно дорогостоящее мероприятие. В связи с этим оно, как правило, не проводится на постоянной основе.

В качестве примера организации стационарного пункта можно привести операцию по прослушиванию телефонных разговоров, проводимую американской резидентурой совместно с полицейским управлением Монтевидео. Необходимые подключения к телефонным линиям на АТС производились инженерами телефонной компании по просьбе полицейского управления. Шестидесятижильный кабель протянули от центрального телефонного узла в деловой части города к полицейскому управлению, где на верхнем этаже размещался пункт прослушивания. Там находились исполнительные механизмы и аппаратура записи. Обслуживали пост два техника, которые передали записи в аналитический пункт.

В СССР до середины 80-х годов телефонные переговоры контролировались только спецслужбами и правоохранительными органами. Как утверждал бывший глава КГБ Вадим Бакатин, до августовского путча 1991 года 12-й отдел КГБ СССР прослушивал в Москве примерно 300 абонентов, в основном иностранных граждан и преступников. Контроль служебных переговоров велся и на особо режимных объектах, но здесь следили не за конкретным человеком, а за утечкой секретной информации. В этом случае использовались специальные системы контроля, работающие по ключевым словам и позволяющие прерывать (блокировать) или телефонный разговор в целом, или отдельные фразы. При этом легко устанавливались номера абонентов – нарушителей режима. Однако аппаратура для подобного контроля стоила очень дорого – порядка 200 тысяч рублей (в ценах 80-х годов) и применялась только на крупных объектах оборонной промышленности и в правительственных учреждениях.

Если верить уже упомянутому «Совместному решению по эксплуатационно-техническим требованиям к средствам и сетям электросвязи для обеспечения оперативно-розыскных мероприятий», то в России в состав се-

тей электросвязи вводятся аппаратные и программные средства, позволяющие проводить контроль из удаленного пункта управления. Кроме того, должна быть предусмотрена возможность по командам из пункта управления изменять на определенный период состав услуг, предоставляемых отдельным абонентам, а также осуществлять конспиративное подключение выделенных службе безопасности каналов и линий к любым абонентским линиям (каналам), в том числе уже находящимся в состоянии соединения.

Однако пока крайне редки случаи «коммерческого» прослушивания на городских АТС, так как это невозможно без наличия там «своего» человека из обслуживающего персонала.

Сейчас для обеспечения телефонной связью крупных организаций, гостиниц, предприятий и т. д. в них создается своя телефонная сеть, обслуживаемая самостоятельной учрежденческой АТС. Эта сеть предоставляет всем своим абонентам внутреннюю телефонную связь, а некоторой группе абонентов – право связи с абонентами ГТС, а через ГТС с междугородней телефонной станцией.

Как известно, значительное место службы безопасности «серьезных» предприятий уделяют контролю телефонных переговоров своих сотрудников. Идеальным местом подключения специального многоканального магнитофона как раз и является местная АТС. Там в миниатюре легко повторить действия спецслужб.

На отечественном рынке многоканальные магнитофоны еще представлены слабо. Пока многоканальность создается использованием большого числа стандартных или специальных одноканальных магнитофонов, характеристики которых приведены в табл. 22. За рубежом имеется значительное число образцов подобной техники. Как правило, это специально разработанное устройство предназначено для стационарной записи телефонных переговоров и рассчитано на значительное число каналов (от 10 до 100).

Таблица 22.

Марка	Количество каналов	Габариты, мм	Вес, кг	Время записи, ч	Дополнительные функции
РК115-S	10	500×360×150	9,8		Автоматическое вкл. Подключение принтера, Привязка ко времени
РК100-SS	1 10 50 100	205×1666×290 1100×550×380 110×890×660 2200×1890×600	2,9 60 220 430	4 10×4 50×4 100×4	Автоматическое вкл. Подключение принтера, метки даты и времени, сигнализация о сбоях

					в работе, и при переполнении кассеты
CU-1	10			Переменная	Регистрация времени, числа, номера абонента, подсчет числа звонков
AD-25	8	480×350×190	16		Метка времени, дистанционное управление
TM	9; 20; 31; 42			до 1000	Регистрация числа, времени, автоконтроль

Часто устройства имеют модульную структуру, которая позволяет наращивать их возможности до требуемого уровня.

Различные компании предлагают значительное количество дополнительных сервисных функций у такого рода аппаратуры. В качестве примера рассмотрим компьютеризированное устройство **DNR-600**, которое позволяет проводить анализ 2500 телефонных линий на предмет активности. При этом регистрируются время, дата, набираемый номер, продолжительность разговора и т. д. В памяти может храниться информация о 400 звонках на каждую линию.

Существует более простая аппаратура прослушивания и записи телефонных переговоров на 16 телефонных линий типа **WORLDSAFE**. Особенностью ее является то, что 24-часовая запись производится на обыкновенную видеокассету стандарта VHS. Внешнее управление аппаратуры возможно осуществлять с персонального компьютера через интерфейс RS 232. Записи распознаются по содержанию информации или по маркерам, установленным оператором. Два канала могут прослушиваться одновременно или раздельно через стереонаушники. К дополнительной возможности относится наличие индикатора занятости линии. Надежность записи обеспечивается механическим ключом, имеющим 4 уровня защиты.

Существует система, записывающая разговоры на медленно движущуюся стальную проволоку, которая по надежности превосходит обычную магнитную ленту. Как правило, это две бобины, с одной из которых на другую перематывается несколько сот метров проволоки. Система фиксирует как время переговоров, так и номера абонентов, с которыми шел разговор. Эта же система может распечатать содержание разговоров. Кроме того, в некоторых случаях предусматривается возможность срабатывания только по кодовым словам.

Широкое распространение офисных АТС привело к необходимости решения задач контроля их сигналов. Офисная АТС по сути своей является коммутатором внешних городских линий и «внутриофисных» линий связи. Сложность в осуществлении контроля внешних линий связи часто возникает

из-за того, что при входящих и особенно исходящих вызовах трудно определить линию, по которой идет информация. Это связано с динамическим распределением вызовов по линиям. Иногда эти проблемы решаются с помощью программ фиксированного распределения входящих звонков. Абонентские внутриофисные линии близки к внешним городским линиям по ряду основных параметров, а различие заключается в номинале напряжения (ГТС имеет 60 В, офисная сеть — 24 В) и способах его подачи на абонентские аппараты.

При включении в такие линии связи аппаратуры подслушивания с питанием от телефонной сети или входным сопротивлением менее 100 кОм съем информации становиться невозможен. В связи с этим датчики подключаемых устройств должны иметь высокое сопротивление как по постоянному, так и по переменному току.

Для удобства работы операторов таких многоканальных систем прослушивания создано целое семейство вспомогательных устройств. Например, прибор типа **РК10-04-005** позволяет осуществлять перезапись 120-минутной магнитофонной кассеты менее чем за 2 мин.

Существует мнение, что передача информации по факсу или телексу повышает безопасность информации. На самом деле это не так. В настоящее время разработаны десятки устройств перехвата факсимильных сообщений. Технически это не сложнее восстановления обычного телефонного разговора, да и способы подключения практически те же. В качестве примера рассмотрим устройство **FAX-MANager**. Будучи подключенным к телефонной сети, оно различает телефонные и факсовые сообщения и принимает их независимо друг от друга, а также автоматически копирует и хранит в памяти все послания, получаемые или отправляемые по факсу. При этом система может зафиксировать практически любое количество страниц и воспринимает информацию, передаваемую со скоростью от 300 до 9000 бит/с. Перехваченные послания распечатываются четко и с высоким разрешением. Прибор в принципе может быть установлен в любом месте на линии (в зонах «А», «Б», «В»), но обычно подобная аппаратура устанавливается именно в зоне «Г». При этом система работает в совершенно автономном режиме.

Более современная модель **FAX-MANager-2** позволяет осуществлять запись перехваченных сообщений на магнитофон. Подобные устройства предлагаются как в переносном, так и в стационарном вариантах. Разработаны и многоканальные системы прослушивания факсимильной связи тип **CD-3**. Эта система постоянно прослушивает 10 телефонных линий и делает печатные копии входящих и исходящих сообщений. Имеются индикаторы, показывающие, когда линия свободна, а когда используется для телефонной или факсимильной связи. Может комплектоваться системой дистанционного

управления наружным магнитофоном, прерывателем передачи информации и устройствами записи на компьютер.

Разработана и широко используется аппаратура и для прослушивания телексов. Например, система CD-3 одновременно контролирует до 10 телексных линий. Возможна распечатка перехваченных сообщений либо визуальный просмотр и распечатка только тех, которые представляют определенный интерес.

7.6. Перехват телефонных переговоров в зоне «Д»

Перехват информации с многоканальных линий связи как кабельных, так и волоконно-оптических, и выделение телефонных переговоров абонентов, за которыми ведется наблюдение, представляют собой очень сложную задачу, которая пока не под силу отечественным специалистам от промышленного шпионажа (по крайней мере, факты подобных подключений еще не известны, хотя интерес к подобной аппаратуре большой и стоит она относительно недорого).

Доступ к коаксиальным кабелям затруднен, поскольку они заглублены и, кроме того, во многих случаях заключены в герметическую оболочку, находящуюся под давлением. При этом нарушение целостности оболочки приводит к падению давления и срабатыванию тревожной сигнализации. В случае, если кабель не находится под давлением, необходимо наличие следующего оборудования для осуществления перехвата: гальванический отвод ($25); демультиплексор, соответствующий полосе модулирующих частот ($5000); смеситель ($50); устройство декодирования сигналов вызова ($1000); магнитофон ($100). Таким образом, полная стоимость подобного комплекта – более $6000. Плюс к этому необходимо иметь одного-двух специалистов по монтажу линий связи.

Более сложной и универсальной аппаратурой, которая может применяться для съема информации с любых кабельных линий связи, пользуются современные спецслужбы. Рассмотрим принцип ее действия на примере американской системы **«Крот».**

С помощью специального индуктивного датчика, охватывающего кабель, снимается вся передаваемая по нему информация. Для проникновения к кабелю используются колодцы. Датчик устанавливается на кабель в колодце и для маскировки проталкивается в трубу, что исключает его обнаружение при периодическом осмотре колодца монтером. Высокочастотный сигнал, идущий по кабелю, записывается на магнитный диск специального магнитофона. После заполнения диск заменяется новым. Запись с диска передается спецслужбе и обрабатывается приборами демодуляции и прослушивания. В целях упрощения задачи поиска устройства «Крот», что необходимо для за-

мены диска, оно снабжено сигнальной радиостанцией. Агент, проезжая или проходя в районе установки прибора-шпиона, запрашивает его с помощью своего портативного радиопередатчика, все ли в норме. Если аппаратуру не трогали, то она передает соответствующий сигнал. В этом случае при благоприятных условиях агент заменяет диск в магнитофоне и работа устройства продолжается. Аппарат может записывать информацию, передаваемую одновременно по 60 телефонным каналам. Продолжительность непрерывной записи на магнитофон составляет до 115 часов. Такие устройства находили в Москве в начале 90-х годов.

Более десяти аналогичных «Кротов» по просьбе сирийской стороны было снято нашими специалистами в Дамаске. Там все подслушивающие устройства были закамуфлированы под местные предметы и заминированы на «неизвлекаемость». Поэтому часть из них при попытке изъятия все-таки взорвалась.

Перехват информации с подводных линий связи – крайне сложное и дорогостоящее мероприятие. Тем не менее подобная аппаратура типа **«Камбала»** применяется разведкой США. «Камбала» — достаточно сложное устройство с ядерным (плутониевым) источником электропитания, рассчитанным на десятки лет работы, предназначено для съема информации с подводных бронированных кабелей связи.

Устройство «Камбала» выполнено в виде стального цилиндра длиной более 5 м, диаметром 1200 мм. В герметически закрытой трубе смонтировано несколько тонн электронного оборудования для приема, усиления и демодуляции снятых с кабеля сигналов. Запись перехватываемых разговоров осуществляется 60 автоматически работающими магнитофонами, которые включаются при появлении сигналов. Каждый магнитофон рассчитан на 150 часов записи. Таким образом, общий объем записи может составить около 9 тысяч часов. К моменту, когда пленки израсходованы, подводный пловец находит устройство подслушивания по гидроакустическому маяку, установленному на контейнере, снимает с кабеля индукционный датчик-захват, предварительный антенный усилитель и доставляет устройство на специально оборудованную подводную лодку. Это огромное устройство в воде имеет почти нулевую плавучесть. В лодке осуществляется замена магнитофонов, после чего устройство вновь устанавливается на линию связи. В контейнере смонтирована система приема, усиления и демодуляции ВЧ-сигналов, проходящих по кабелю. Специальный чувствительный индуктивный датчик способен снимать информацию с подводного кабеля, защищенного не только изоляцией, но и двойной броней из стальной ленты и стальной проволоки, плотно обвивающих кабель. Сигналы с датчика предварительно усиливаются антенным уси-

лителем, а затем направляются для демодуляции, выделения отдельных разговоров и их записи на магнитофоны.

Следует учесть, что для практического применения такой системы необходима еще специальная подводная лодка, оборудованная устройством для поиска подводных кабелей в морских глубинах. Понятно, что найти в море кабель даже в том случае, когда известна трасса его прохождения, – задача не простая. Для поиска кабеля нужны специальные электронные приборы с датчиками, находящимися вне лодки, приспособленными для работы на глубине.

«Камбала» опробована в деле для контроля наиболее важных каналов связи среди множества советских подводных кабельных коммуникаций. По признанию американцев, это были, пожалуй, самые опасные операции, когда подвергались риску жизни всех людей на борту подлодки, – экипажа и спецгруппы АНБ. Каждая операция утверждалась лично президентом. Атомная подводная лодка выходила в море, в заданном квадрате устанавливались звукозаписывающие устройства (их называли «коконы»), затем она уходила из этого квадрата и выжидала несколько недель. Потом возвращалась в тот же квадрат, чтобы снять пленки с установленного на кабеле записывающего устройства.

Директор ЦРУ признавал: «Иногда подлодка возвращалась с довольно богатым урожаем сведений о советских вооруженных силах. Как и при других подобных операциях, все строилось на ошибках другой стороны. Русские считали, что подводные кабели прослушивать невозможно, и поэтому использовался сравнительно несложный шифровальный код, а иногда обходились и без него».

Операция в Охотском море успешно осуществлялась до 1981 года. Но однажды на фотоснимке с американского спутника было отмечено большое скопление советских судов как раз в том участке Охотского моря, где к кабелю было прикреплено подслушивающее устройство. Один из советских кораблей был оборудован подводной спасательной техникой. Ранее было зафиксировано участие этого судна в спасательных операциях в различных районах мирового океана. Позднее, когда американская подводная лодка прибыла для замены пленок, она обнаружила, что устройство исчезло. Была создана комиссия по расследованию, которая установила, что поскольку русские точно вышли к месту, то они знали, что делают, значит у КГБ есть агент.

Провал операции подхлестнул активную деятельность американской разведки. Предлагалось скрытно провести из Гренландии глубоководный кабель и с его помощью подслушивающие устройства подсоединить к советским подводным коммуникационным линиям в северных прибрежных водах. В этом случае информация сразу же попадала бы в Агентство национальной безопасности (АНБ) в реальном масштабе времени. Расстояние между Грен-

ландией и советским побережьем составляет около 1200 миль. При всей заманчивости от этого плана отказались: кабель пришлось бы укладывать на дно океана при цене около 1 млн доллоров за милю. По другому проекту, стоимостью уже несколько миллиардов долларов, предлагалось, используя такую же технологию, прослушивать все коммуникационные кабели мира.

Таким образом, в настоящее время имеется целое семейство спецсредств перехвата информации с кабельных линий связи: для симметричных ВЧ-кабелей – устройства с индуктивными датчиками, для коаксиальных и НЧ-кабелей – с системами непосредственного подключения и отвода малой части энергии для целей перехвата. Для кабелей, внутри которых поддерживается повышенное давление воздуха, применяются устройства, исключающие его снижение, в результате чего предотвращается срабатывание специальной сигнализации. Некоторые приборы снабжаются радиостанциями для прямой передачи перехваченных разговоров в центр обработки. Однако из-за их колоссальной стоимости данные системы применяются только спецслужбами очень богатых стран.

Значительный интерес представляет возможность перехвата информации с волоконно-оптических линий связи (ВОЛС). По некоторым данным, в настоящее время до 10% всех линий передачи информации, а к 2000 году – почти все вновь вводимые линии будут волоконно-оптическими. Уже разработан и опробован оптический телефон и проводится работа по созданию принципиально новых АТС.

Считается, что использование оптических волокон в качестве физической среды для передачи большого объема информации по сравнению с существующими электрическими кабелями в части, касающейся защиты информации, имеет следующие преимущества:

- высокая помехозащищенность (устойчивость к воздействию окружающей среды, электромагнитным и оптическим помехам);
- гальваническая развязка по питанию различных элементов сети;
- отсутствие излучений и наводок на соседние информационные линии и устройства;
- сложность несанкционированного подключения.

Сутью несанкционированного доступа к оптическому волокну является создание (или использование природной) неоднородности, на которой происходит рассеяние части сигнала. Далее с помощью оптического приемника осуществляется перехват информации.

Примером природной неоднородности является место соединения ВОЛС. Причинами возникновения излучения в разъемных соединениях волоконных световодов являются: радиальная несогласованность стыкуемых волокон; угловая несогласованность осей световодов; наличие зазора между

торцами световода; наличие взаимной непараллельности поверхностей торцов волокон; разница в диаметрах сердечников стыкуемых волокон. Все эти причины приводят к излучению световых сигналов в окружающее пространство.

По мнению специалистов фирмы Dell Communication Research (США), возможен перехват информации с ВОЛС. Для этого требуется длительный контроль линий с помощью приборов, широко применяемых для неразрушающего контроля качества волоконно-оптического кабеля (ВОК) при его производстве и испытаниях.

В одном из способов перехвата используется свойства ВОК излучать небольшое количество энергии в месте его изгиба. ВОК зажимается между двумя пластинами, одна из которых имеет рифленую поверхность, предназначенную для деформации волокна. На другой пластине размещается фотодетектор и устройство регистрации информации. Стоимость такого комплекта – $1000.

При другом варианте схеме подключения в качестве элемента съема светового сигнала используется стеклянная трубка, заполненная жидкостью с высоким показателем преломления и с изогнутым концом, жестко фиксированная на оптическом кабеле, с которого предварительно снята экранная оболочка. На отогнутом конце трубки устанавливается объектив, фокусирующий световой поток на фотодиод, а затем на усилитель звуковых сигналов подается уже электрический сигнал с фотодиода.

В самом простом варианте подключения (так называемое контактное подключение) идут еще дальше: просто удаляют защитные слои кабеля, светоотражающую оболочку и изгибают его на необходимый угол. Даже при таком грубом подключении к ВОК обнаружить утечку информации за счет ослабления мощности бывает очень трудно. Так как при существующих приемных устройствах аппаратуре несанкционированного доступа достаточно отобрать всего 0,001% передаваемой мощности, чтобы уверенно подслушать переговоры, а дополнительные потери при изгибе кабеля составляют всего 0,01-1 дБ в зависимости от его угла.

7.7. Перехват телефонных переговоров в зоне «Е»

В последнее время большой популярностью среди бизнесменов пользуются радиотелефоны и радиостанции различных типов. Среди них, наряду с импортными, появляются и отечественные образцы. Как это ни странно, но существует расхожее мнение, что при разговоре по обычному телефону возможность его прослушивания существенно выше, чем при разговоре по радиотелефону. Увы, мы вынуждены развеять эти иллюзии, но сначала необходимо описать принцип работы самих радиотелефонов.

Радиотелефон – это в сущности комплекс из двух радиостанций, одна из которых является базовой, устанавливается стационарно и подключается к телефонной сети, вторая – подвижная. От обычной радиостанции они отличаются тем, что пользователь выходит непосредственно в ГТС.

Следовательно, осуществлять прослушивание радиотелефонных разговоров, с одной стороны, в принципе можно теми же способами, что и обычных телефонных. Однако с точки зрения съема информации радиотелефоны, в том числе сотовые системы, и радиостанции объединяет то, что при работе они сами используют радиоволны. Следовательно, достаточно приобрести качественный приемник с соответствующим диапазоном частот, хорошую антенну, устройство звукозаписи и без всякого риска «подключиться» к разговору. При этом дальность радиоперехвата будет не меньше дальности работы радиотелефона, а при использовании хорошей аппаратуры – в несколько раз больше. Так, если радиус действия базовой станции сотовой связи составляет от 5 до 15 км, то перехват при определенных условиях возможно осуществлять на расстоянии до 50 км. Дальность будет зависеть от многих факторов, в первую очередь от высоты расположения антенны, ее направленных свойств и от чувствительности приемника.

Мобильные сети связи для «узкого круга» существуют в России уже много лет, примерно с 60-х годов. До сих пор в некоторых городах России действует система **«Алтай»**. В Москве, например, у нее около 6 тысяч пользователей. Различие между системой «Алтай» и современными системами в том, что первая не является сотовой.

Сотовой называется система связи, состоящая из множества ячеек, которые, связываясь между собой, образуют широкую сеть. Система «Алтай» работает с единственной ячейкой, к которой подключены все абоненты. Именно потому, что сотовые сети имеют возможность наращиваться и соединяться между собой, они и стали так популярны.

Система «Алтай» работает в диапазоне 150 и 300 МГц, сотовые системы используют диапазон 450, 800 и 900 МГц (стандарты NMT, AMPS, GSM). Кроме того, некоторое распространение в России получили телефонные интерфейсы, предназначенные для удобной и надежной связи между радиокоммуникационным оборудованием и стандартными телефонными системами. Подобные средства, например **TW5800,** позволяют отдаленным радиостанциям устанавливать связь с телефонными абонентами и наоборот. Часто абонент и не предполагает, что его переговоры транслируются на десятки и сотни километров и становятся легкой добычей «радиолюбителей». Известно немало случаев, когда осуществлялся перехват информации в этих каналах с коммерческими целями. Так, у немецкой фирмы «Шмидтунд Фольке», которая конкурировала с другими компаниями в разработке месторождений на

дне моря, был похищен ее самый ценный секрет: точное географическое положение обследуемого района. Агенты прослушивали радиосвязь плавучей конечной станции фирмы с ее вычислительным центром на суше и затем обрабатывали полученную информацию. Результаты своих трудов они продавали конкурирующей фирме, которая благодаря этому сэкономила значительную сумму, так как разведка месторождений полезных ископаемых на больших глубинах всегда связана с весьма крупными затратами.

Наиболее скандальный случай – прослушивание переговоров по сотовому телефону короля Испании Хуана Карлоса испанскими же спецслужбами (кстати, в Испании в спецподразделениях по контролю телефонной связи всего шесть человек). Заодно прослушивали премьер-министра, министра иностранных дел и высокопоставленных гостей страны, и без счета «обычных» бизнесменов, журналистов и т. д.

Кроме того, необходимо помнить, что по излучаемым сигналам можно установить местоположение подвижных объектов, оборудованных радиотелефоном.

Одним из наиболее универсальных разведывательных приемников является **Miniport** фирмы «Роде и Шварц» с диапазоном рабочих частот 20-1000 МГц. С его помощью можно без труда осуществлять перехват всех радиостанций и радиотелефонов. Данный приемник имеет небольшие габариты (188×71×212 мм), универсальное питание (от аккумуляторной батареи и от сети 220 В) и может успешно применяться как в стационарных, так и в полевых условиях. Управление приемником осуществляется цифровым способом через встроенный процессор. Визуальное считывание значения частоты производится с цифрового дисплея с шагом 1 кГц. Запоминающее устройство микропроцессора может хранить в памяти до 30 фиксированных частот и осуществлять сканирование в заданном диапазоне с переменным шагом. Возможности приемника могут быть существенно расширены за счет совмещения с малогабаритным анализатором спектра, специально для него разработанного, – типа **EPZ100**. Для удобства применения комплекса аппаратуры в полевых условиях поставляются укладочные кейсы, где отдельно размещается аккумулятор, приемник с анализатором спектра и набор антенн.

Известно, что определение местоположения (пеленгация) работающих на излучение радиостанций производится с помощью вращающихся в горизонтальной плоскости специальных антенн направленного действия. Для определения точного местоположения источника сигнала необходимо иметь несколько, по крайней мере два пеленгатора, чтобы сделать «засечку» в месте пересечения двух пеленгов одного источника с разных мест. В последнее время появились более совершенные пеленгаторы доплеровского типа, у которых нет механически вращающихся антенн, а есть одна антенная мачта, на

которой установлено более десяти идентичных дипольных антенн. За счет специальной обработки сигнала производится мгновенная пеленгация излучателя. При совмещении подобной антенны с описанным выше приемником возможно за 0,1 с обнаружить радиосигнал, измерить его параметры и определить пеленг. С учетом необходимости передачи данных на другой пост пеленгации, с целью однозначного определения местоположения источника излучения, требуется около 1–2 с для точного определения места. Таким образом, не успев сказать несколько слов по радиотелефону, абонент точно указывает местоположение своего автомобиля.

Современные передающие устройства могут использовать перестройку частоты в ходе сеанса связи по случайному закону, осуществлять передачу с использованием специальных видов модуляции, что затрудняет перехват информации.

Фирма Telefunken System technik проектирует, разрабатывает и производит радиопеленгаторы серии **Telegon** в частотном диапазоне 10 кГц-1 ГГц. Данные пеленгаторы отличаются высокой чувствительностью и могут перехватывать кратковременные и слабые сигналы при перегруженности диапазона частот. При этом предусмотрена возможность перехвата сигналов и с перестройкой частоты.

Иногда, для упрощения контроля за перемещением объекта, используются специальные радиомаяки, которые скрытно устанавливаются в автомобилях, а в некоторых случаях вшиваются в одежду, монтируются в портфеле, калькуляторе и других вещах объекта наблюдения. Подобное устройство было установлено в печатной машинке одного бывшего сотрудника ЦРУ, благодаря чему отслеживались все его перемещения с квартиры на квартиру. Известны случаи установки подобных устройств в полостях каблуков обуви, возвращенной после ремонта.

Обычно подобные маяки имеют режим прослушивания разговоров, ведущихся объектом наблюдения.

Значительное распространение сотовой связи и особенности ее организации привели к необходимости создания специальной, гораздо более сложной аппаратуры для осуществления ее контроля. Дело в том, что телефоны этого типа не привязаны к фиксированным частотам, а могут работать на любой свободной частоте в пределах своего поддиапазона, что значительно затрудняет перехват.

Рассмотрим работу систем перехвата сообщений из каналов сотовой связи на примере **STG 4610** и **STG 4615**. Основой подобных устройств являются специальные радиоприемные устройства с декодером сигналов сотовой связи. Используя технику цифровой обработки сигналов для расшифровки неслышных служебных сообщений, идущих между сотовым телефоном и со-

товой станцией, декодер позволяет оператору настраиваться на частоту телефонов и автоматически прослушивать разговор через свой аппарат без перерывов в приеме. Подобные системы обычно оснащаются индикаторными устройствами отображения частоты и уровня принимаемого сигнала, встроенными магнитофонами, специальными антеннами, комбинированными источниками питания и другими необходимыми устройствами. На российском рынке предлагается весьма эффективная аппаратура контроля сотовых сетей стандартов **NMT-450** и **AMPS** по цене до 20 тысяч долларов.

Проблема перехвата существенно усложняется, если в сотовой сети предусмотрена криптографическая защита речевой информации. Однако даже и в этом случае полной гарантии (как это делают телефонные компании) дать нельзя, поскольку существуют специальные комплексы радиоперехвата с возможностью анализа зашифрованных сигналов, например **Sigint/Comint Spectra** фирмы Hollandes Signal. Подобная аппаратура чрезвычайно дорога (более 100 тысяч долларов) и может использоваться только организациями, обладающими очень большими средствами. Данных о наличии подобных систем в России в частном владении нет, но надо помнить, что, потратив определенную сумму, вас вполне могут слушать «заинтересованные лица».

Большую популярность получила пейджерная связь, которая осуществляется следующим образом. Абонент городской АТС набирает один из номеров пейджерной компании и передает сообщение диспетчеру, который вводит его в компьютер. Дальнейшая передача сообщения осуществляется автоматически по радиоканалу. Существуют и полностью автоматические системы. Через 2 года после появления данного вида связи в России были разработаны и предлагаются покупателям программно-аппаратные системы перехвата. В состав подобной системы входят: специально доработанный сканер (**AR-3000A**, **IC-7100** и т. д.); устройство преобразования; ПЭВМ и специальное программное обеспечение. Система позволяет осуществлять прием и декодирование текстовых и цифровых сообщений, передаваемых в каналах радиопейджинговой связи, и сохранять все принятые сообщения (с датой и временем передачи) на жестком диске ПЭВМ. При этом может производиться входная фильтрация потока сообщений, выделение данных, адресованных конкретным абонентам (с помощью априорно известных или экспериментально определенных кеп-кодов). Возможно осуществление поиска, распечатки и русификации перехваченных сообщений.

Как и в обычной телефонной сети, здесь тоже предусмотрен государственный контроль, который организован следующим образом. Министерство связи России обязало всех операторов мобильной телефонной и пейджинговой связи обеспечить доступ российских спецслужб к своим сетям. Эти требования сформулированы в приказе Минсвязи № 9 от 31 января 1999 года

«Об организации работ по обеспечению оперативно-розыскных мероприятий на сетях подвижной связи». В соответствии с техническим приложением к приказу система предназначена «для оперативного контроля соединений и местоположения определенных пользователей оперативной связи». То есть с ее помощью можно не только прослушивать разговоры, но и определять местоположение абонента телефона, даже если по нему не ведется разговор. Предусматривается создание баз данных передаваемой по мобильным сетям информации и точных адресов пользователей. Приказ также подразумевает контроль за всеми номерами, на которые переадресуется вызов, и всеми дополнительными услугами, предоставляемыми абонентам операторами мобильной связи. В документе расписаны виды, методы контроля, а также способы защиты информации от несанкционированного доступа.

Значительно более сложной задачей является перехват междугородных телефонных переговоров, ведущихся с привлечением радиорелейных линий связи. Используемые в России радиорелейные линии являются многоканальными системами передачи (до 3600 каналов), что усложняет задачу съема. Расстояние от радиорелейной станции, с которого возможно осуществление перехвата информации, совсем невелико, так как передающая антенна имеет узкую диаграмму направленности. Впрочем, можно располагаться вблизи приемного (передающего) пункта либо вдоль линии трассы в главном лепестке антенны. Комплект для перехвата информации с микроволновых линий связи включает:

- параболические антенны (2 шт. - $1000);
- радиоприемники с частотными демодуляторами (2 шт. - $10000);
- демодуляторы, соответствующие полосе модулирующих частот (2 шт. - $10000);
- управляющий процессор со сканированием ($1000);
- осциляторы с цифровой настройкой (2 шт. - $700);
- устройство декодирования сигналов вызова (2 шт. - $1500);
- смеситель ($50);
- магнитофон ($100).

Таким образом, полная стоимость подобного комплекта приближается к $40000, что делает его совсем непривлекательным для «рядовых» шпионов. Хотя, в принципе, могут быть использованы типовые разведывательные приемники с дополнительными выходными устройствами разуплотнения и демодуляции принимаемых сигналов. В приемном устройстве многоканальный сигнал селектируется, детектируется и усиливается до уровня, достаточного для нормальной работы записывающих устройств. При этом к системе предъ-

являются жесткие требования по стабильности частоты, нелинейным искажениям и появлению комбинационных частот.

В качестве примера рассмотрим систему **РК445**, предназначенную для перехвата телефонных переговоров, факсимильных сообщений и т. д. Диапазон рабочих частот – 0,1-18,5 ГГц. Точность настройки – 100 Гц. Возможно детектирование сигналов с АМ, ЧМ и импульсной модуляцией. Перехваченные сигналы снабжаются меткой времени с датой и могут быть записаны на встроенный магнитофон либо распечатываться на принтере. Управление системой осуществляется с ноутбука 486 SL25.

Серьезные задачи под силу организациям типа национальной АНБ. Эта правительственная организация насчитывает в 6 раз больше служащих, чем ЦРУ. Она занимается электронной разведкой, причем на ее долю приходится большая часть американских ассигнований на нужды разведки. Имеется 4120 мощных центров прослушивания, размещенных на многочисленных военных базах в Германии, Турции, Японии и других странах, а также на борту американских кораблей, подводных лодок и самолетов.

АНБ имеет возможность собирать и анализировать почти повсеместно радиограммы, телефонные переговоры, идущие по радиорелейным и спутниковым каналам связи, электронные сигналы любого типа, включая излучения систем сигнализации в квартирах и противоугонных устройств автомобилей. Достаточно сказать, что Агентство ежедневно «перерабатывает» до 40 т секретной документации.

Аналогичной деятельностью занимается британский Штаб правительственной связи (ШПС). У АНБ и ШПС имеется список лиц и организаций, все переговоры которых перехватываются автоматически. Этот список включает в себя ряд нефтяных компаний, банков, газет, имена известных дилеров на товарных рынках и лидеров ряда политических и общественных организаций. Для обработки перехваченной информации используются быстродействующие компьютеры, которые ведут поиск ключевых слов со скоростью до 4 млн знаков в секунду. Это означает, что они способны прочитать среднюю по объему газету быстрее, чем человек пробежит глазами ее заголовок. Когда компьютер наталкивается на определенное слово, означающее, что данный текст представляет интерес для АНБ или ШПС, изготовляется его печатная копия для дальнейшего изучения, причем тексты распечатываются устройствами, выдающими 22 тысячи строк в минуту. Таким образом, информация о событии, сообщении или переговорах, представляющих особое политическое или военное значение и называемых на специальном языке «критическими», ляжет на стол президента США в среднем через 10 минут.

Участники международных проектов вполне могут стать объектом внимания спецслужб, часто действующих в интересах национальных корпо-

раций. Действительно, как отмечает западная печать, американская радиоразведка, которая становится «свидетелем» многих коммерческих сделок, в состоянии выявить «узкие места» в развитии экономики многих стран, в том числе и России. Известно, например, что АНБ получило большие дивиденды, осуществляя перехват сообщений газовых и нефтяных компаний на Ближнем Востоке, финансовых и торговых организаций в Европе и Японии и передавая эту информацию американским фирмам. По некоторым данным, перед АНБ ставятся задачи о целенаправленном контроле за конкретными компаниями.

К зоне «Е» возможно отнести и сравнительно молодой вид связи — уникальную систему действующей в России внутригосударственной спутниковой связи с разветвленной сетью наземных станций «Орбита», «Экран», «Москва». Через спутники «Горизонт» вместе со спутниками «Молния-3» и «Радуга» обеспечивается телефонная и телеграфная связь по территории всей страны. Большинство спутниковых линий связи использует диапазон 4-6 ГГЦ. Интересно, что в ФРГ в свое время в законе о борьбе с преступностью предусматривалась возможность подслушивания международных телефонных переговоров именно по спутниковым каналам связи.

Даже в проект системы глобальной спутниковой связи для мобильных абонентов **Iridium** (инициирован фирмой Motorola) Центр им. Хруничева по настоянию Минсвязи согласился внести некоторые коррективы. В частности, был определен четкий порядок размещения в будущей сети аппаратуры спецслужб, чтобы они без труда могли проводить так называемые оперативно-розыскные мероприятия.

Группа радиоэлектронного контроля (Франция) имеет в своем распоряжении около 100 технических постов, в том числе за рубежом, и ведет перехват информации радиоэлектронными средствами, а также обеспечивает прослушивание телефонных переговоров. При этом в последние годы руководители Франции настойчиво говорят о важности усиления разведывательной деятельности именно в экономической области, подчеркивая особое значение обеспечения экономических интересов в условиях острой конкурентной борьбы с другими странами.

Таким образом, практически все страны мира контролируют телефонные переговоры в зоне «Е» (по крайней мере, имеют такую возможность при необходимости).

Для перехвата сообщений по космическим каналам связи также могут использоваться спутники-разведчики. Первые спутники радиоэлектронной разведки, вероятно, запускались в конце 60 – начале 70-х годов. Известно, что первый спутник типа **Rhyolit** вышел на орбиту в марте 1973 года. В 1979 и в 1981 годах были запущены два усовершенствованных спутника радиоэлектронной разведки **Shalet.** В 1985 году был запущен спутник типа **Magnum.**

Запуск космических аппаратов продолжался с помощью многоразовых аппаратов типа «Шатл». В качестве примера современного космического разведчика можно описать спутник «**Аквакейд**», осуществляющий прослушивание каналов радиосвязи в диапазоне частот 0,5-40 000 МГц. Спутник имеет две параболические антенны диаметром около 23 м и обладает весьма высокой чувствительностью и точностью привязки обнаруженного излучения объекта к местности. Он перехватывает от 300 до 3000 каналов связи одновременно и через спутники-ретрансляторы типа TDRSS передает информацию на наземные пункты, где проводится демодуляция сигналов и определение с помощью ЭВМ по дескрипторным словам тех сообщений, которые представляют интерес для спецслужб. Особое внимание уделяется перехваченным частным разговорам.

Спутники радиоразведки стоят порядка 300 млн. долларов и выводятся на геостационарные орбиты. Они предназначены для перехвата переговоров как по военным и дипломатическим каналам радиосвязи, так и по каналам, имеющим коммерческое значение. Группировка спутников радиоэлектронной разведки обычно состоит из 10-20 аппаратов, а 5-6 из них постоянно ведут перехват информации с радиорелейных, тропосферных, спутниковых и других линий связи. Эта информация также может быть передана заинтересованным организациям, имеющим бизнес в России.

Таким образом, существуют десятки методов и средств перехвата информации, циркулирующей в телефонной сети. В связи с этим представляет существенный интерес анализ возможности сохранения конфиденциальности сообщений от частных компаний. Чтобы оценить реальные возможности крупных фирм, приведем небольшой пример. 13 июля 1982 года АНБ перехватило направленное в Японию коммерческое сообщение из представительства компании «Мицубиси» в Вашингтоне. В перехваченном АНБ 29 июля 1982 года втором сообщении японской компании давались обширные цитаты из национальной разведывательной сводки от 26 июля.

7.8. Перехват телеграфных разговоров

В настоящее время доля телеграфных разговоров непрерывно снижается уступая место другим видам связи. Поэтому не вдаваясь в детали проиллюстрируем один из способов контактного подключения при перехвате низкоскоростной телеграфной передачи (см. рис. 116) посредством включения в линию связи низкоомного чувствительного реле. При низких скоростях телеграфирования в схеме могут применяться механические реле, а на высоких — электронные [15].

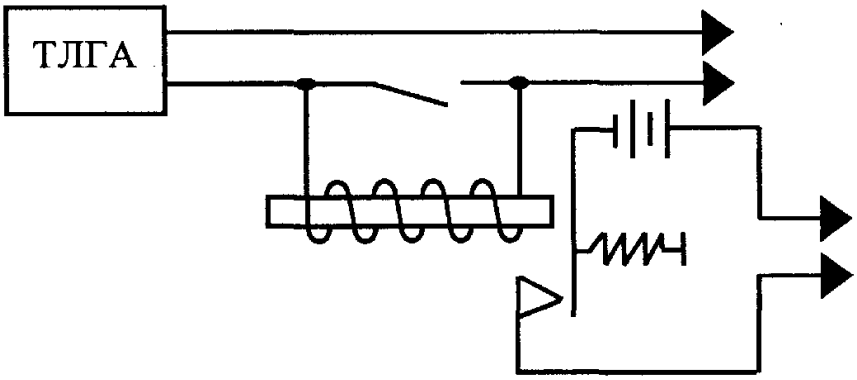

Рис. 116. Контактного подключение к телеграфной линии связи с использованием механического реле

Перехват сигнала от телеграфного аппарата (ТЛГА) осуществляется последовательным подключением к телеграфному проводу. Недостатком описанного контактного способа несанкционированного подключения к телеграфной линии является нарушение целостности проводов и влияние подключаемого устройства на характеристики линии связи.

8. ПЕРЕХВАТ СООБЩЕНИЙ В КАНАЛАХ СОТОВОЙ СВЯЗИ

В настоящее время мобильная связь является привычным атрибутом жизни. В этой главе будут описаны угрозы и недостатки защиты мобильной связи. А также представлены способы защиты от этих угроз. В качестве основной технологии будет рассматриваться технология стандарта GSM. GSM (англ. Global System for Mobile Communications) – глобальный стандарт цифровой мобильной сотовой связи, с разделением каналов по времени (TDMA) и частоте (FDMA) разработанный в конце 80–х годов прошлого века. В развитии GSM можно выделить несколько этапов. На первом этапе (phase 1, 1982–1992 гг.) поддерживал всего пять услуг. На втором этапе (phase 2, 1993–1997 гг.) появились дополнительные услуги (в т.ч. SMS) и добавился диапазон 1900 МГц. Следующий этап (phase 2+) не имеет четких границ внедрения. Среди наиболее заметных нововведений можно выделить появление GPRS (пакетная передача данных) и системы передачи данных по коммутируемым каналам HSCSD (High Speed Circuit Switched Data).

GSM относится к сетям второго поколения (2 Generation) (1G – аналоговая сотовая связь, 2G – цифровая сотовая связь, 3G – широкополосная цифровая сотовая связь). GSM пришел на смену таким аналоговым стандартам как NMT–450 и AMPS–800. Не вдаваясь в технические подробности можно сказать, что перехват разговоров в этих сетях был доступен простому радиолюбителю без специальной подготовки. Забегая вперед, необходимо отметить, что хотя перехватывать разговоры в GSM сети можно, сделать это (на декабрь 2012 года) далеко не просто, вопреки распространенному мнению. В дальнейшем мы покажем почему. Важно отметить, что рассматриваемые способы перехвата не используются спец. службами, по крайней мере, России. При регистрации любой фирмы занимающейся, в каком либо виде связью (в том числе при организации дата–центра) ее обязывают поставить (за свой счет) на своей площадке СОРМ, который может перехватывать данные в незашифрованном виде, в случае мобильной связи это звонки и смс. Более того, при получении санкции на прослушивание, уполномоченные органы даже не оповещают оператора о проводимых действиях. В сети можно найти видео с обзором дата–центров сотовых операторов, где прекрасно видно установленные СОРМы. Поэтому рассматриваемые способы скорее могут использоваться либо для промышленного шпионажа, либо для негласной «прослушки» абонента. Дополнительную информацию о СОРМ можно найти в Интернет.

8.1. Архитектура GSM сети. Особенности работы

Перед тем как приступить к рассмотрению способов перехвата, необходимо понимать архитектуру сети и понимать принципы ее работы.

Архитектура сети GSM

Архитектура сети GSM похожа на архитектуру обычных телефонных сетей, но в ней есть некоторые особенности. Сеть состоит из трех основных подсистем:

– подсистема базовых станций (BSS – Base Station Subsystem),

– подсистема сети и коммутации (NSS – Network Switching Subsystem), которая является “ядром” (core network) системы,

– центр технического обслуживания (OMC – Operation and Maintenance Centre).

В отдельный класс оборудования выделены мобильные (сотовые) телефоны (MS – Mobile Station).

Также для обеспечения сервисов пакетной передачи существует также расширение GPRS. Это позволяет мобильным телефонам получать доступ к Интернет.

Архитектура сети GSM представлена на рис. 117. Для однозначности интерпретации будем использовать термины и обозначения, принятые в рекомендациях GSM.

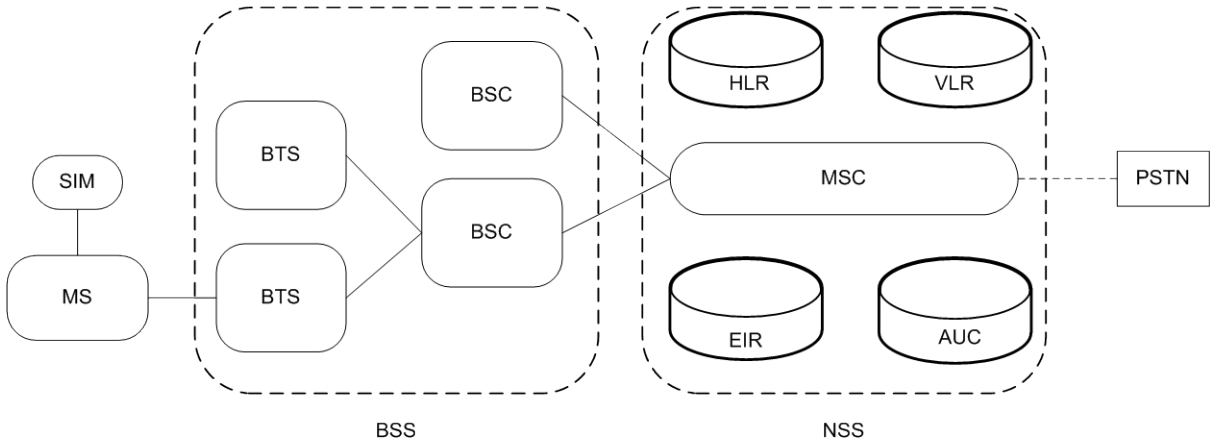

Рис. 117. Архитектура GSM сети

SIM (Subscriber Identification Module) – модуль идентификации абонента.

MS (Mobile Station) – мобильная станция (мобильный (сотовый) телефон).

PSTN (Public Switched Telephone Network) – телефонная сеть общего пользования, в которой используются обычные проводные телефонные аппараты, мини–АТС и оборудование передачи данных.

BSS состоит из BTS (англ. Base Transceiver Station), т.е. самих базовых станций и контроллеров базовых станций (BSC – Base Station Controller). Об-

ласть, которую покрывает одна BTS называют сотой. Сигнал от станции имеет теоретический радиус 120 км, но на практике составляет от 400м до 50 км. Области покрытия соседних станция перекрываются, тем самым обеспечивается возможность передачи обслуживания MS при перемещении ее из одной соты в другую без разрыва соединения (handover). Сигнал от каждой станции распространяется, покрывая площадь в виде круга, но при пересечении с областями покрытия соседних станций получаются правильные шестиугольники. При разработке стандарта были учтены задачи оптимального размещения станций при минимальном перекрытии зон. В итоге каждая станция имеет 6 соседей и именно поэтому при перекрытии зон получаются шестиугольники, которые похожи визуально на пчелиные соты (в разрезе). Отсюда происходит альтернативное название «сотовая» связь.

Основная задача контроллера базовых станций (BSC) заключается в контроле соединения между BTS и подсистемой коммутации. Также он управляет очередностью соединений, скоростью передачи данных, распределение радиоканалов, производит сбор статистики и контроль различных радиоизмерений, управляет процедурой handover.

Ядро (NSS) состоит из центра коммутации (MSC), домашнего(HLR) и гостевого(VLR) регистров местоположения, регистра идентификации оборудования(EIR) и центра аутентификации(AUC).

Центр коммутации (MSC – Mobile Services Switching Centre) контролирует определенную географическую зону с расположенными на ней BTS и BSC. Он осуществляет установку соединения к абоненту и от него внутри сети GSM, обеспечивает интерфейс между GSM и PSTN, другими сетями радиосвязи, сетями передачи данных(GPRS). Также выполняет функции маршрутизации вызовов, управление вызовами, эстафетной передачи обслуживания при перемещении MS из одной зоны в другую. После завершения вызова MSC обрабатывает данные по нему и передает их в центр расчетов для формирования счета за предоставленные услуги (биллинг), собирает статистические данные. MSC также постоянно следит за положением MS, используя данные из HLR и VLR, что необходимо для быстрого нахождения и установления соединения с MS в случае ее вызова.

Домашний регистр местоположения (HLR – Home Location Registry) содержит базу данных абонентов, приписанных к нему. Здесь содержится информация о предоставляемых данному абоненту услугах, информация о состоянии каждого абонента, необходимая в случае его вызова, а также Международный Идентификатор Мобильного Абонента (IMSI –International Mobile Subscriber Identity), который используется для аутентификации абонента (при помощи AUC). Каждый абонент приписан к одному HLR. К дан-

ным HLR имеют доступ все MSC и VLR в местной GSM–сети, а в случае межсетевого роуминга – и MSC других сетей.

Гостевой регистр местоположения (VLR – Visitor Location Registry) обеспечивает мониторинг передвижения MS из одной зоны в другую и содержит базу данных о перемещающихся абонентах, находящихся в данный момент в этой зоне, в том числе абонентах других систем GSM – так называемых роумерах. Данные об абоненте удаляются из VLR в том случае, если абонент переместился в другую зону. Такая схема позволяет сократить количество запросов на HLR данного абонента и, следовательно, время обслуживания вызова.

Регистр идентификации оборудования (EIR – Equipment Identification Registry) содержит базу данных, необходимую для установления подлинности MS по IMEI (International Mobile Equipment Identity, международный идентификатор мобильного абонента (индивидуальный номер абонента)). Формирует три списка: белый (допущен к использованию), серый (некоторые проблемы с идентификацией MS) и черный (MS, запрещенные к применению). У российских операторов (и большей части операторов стран СНГ) используются только белые списки, что не позволяет раз и навсегда решить проблему кражи мобильных телефонов.

Центр аутентификации (AUC – Authentification Centre). В задачи этого компонента входит обеспечение аутентификации и защиты информации в GSM сетах. Работа этого компонента подробней рассмотрена в следующем разделе.

Обновление местоположения

Важной процедурой работы в сети GSM является обновление местоположения (Location update, LU). Для того чтобы в момент звонка BSS не искала абонента на всей зоне покрытия она должна хотя бы примерно представлять, где в настоящий момент находится каждый MS. Информация о текущем местоположении предоставляется самим MS с помощью процедуры, называемой «location update». BSS объединяются в логические группы, называемые location area (LA)(рис. 118). Все LA пронумерованы, у каждой есть определенный числовой код – Location Area Code (LAC). Текущий «адрес» телефона в сети представляет собой пару (LAC, CellID), где CellID – числовой идентификатор «соты». Пара (LAC, CellID) уникальна в пределах всей сети.

В каждый момент времени телефон слушает до 16 широковещательных каналов (broadcast channel, BCH) от 16 сот. На основании услышанного он выбирает 6 «лучших» сот, с которыми (по мнению телефона) у него будет максимально устойчивая связь с минимальными затратами энергии. Из этих шести сот телефон выбирает одну «самую лучшую» на основании так назы-

ваем «критериев C1 и C2» (технические детали этих критериев нам здесь не важны). Именно эту соту телефон постарается использовать для получения или совершения звонка.

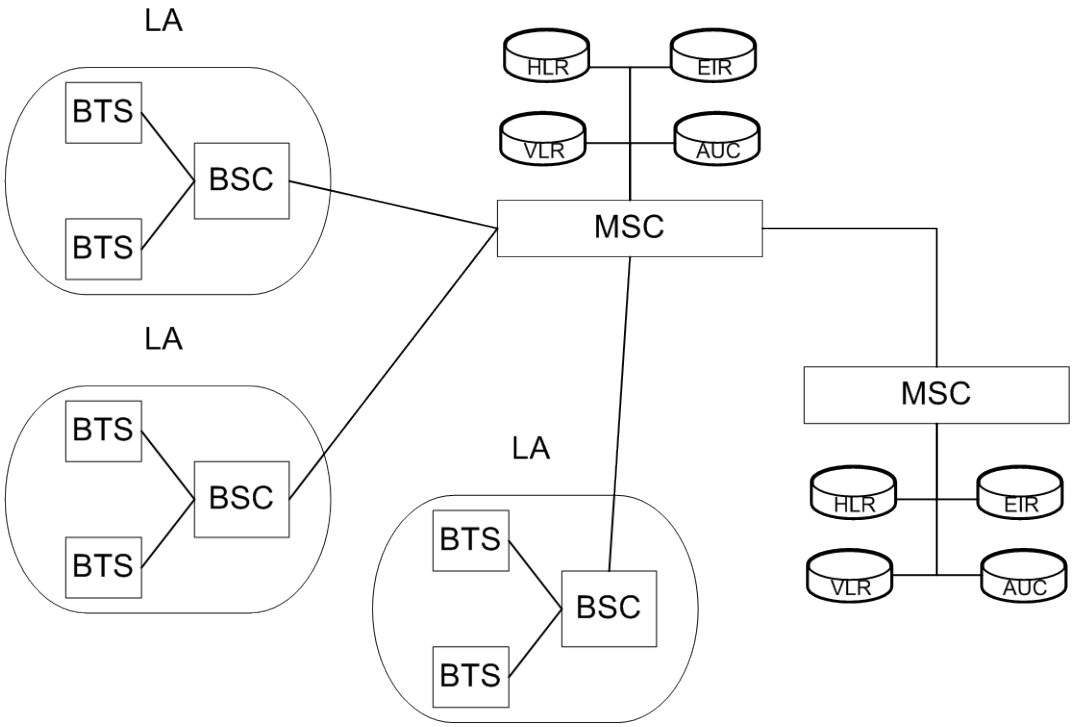

Рис. 118. Структура LA

После включения телефон пытается зарегистрироваться в сети. В процессе телефон формирует список 6 соседних сот, выбирает из них лучшую, и использует «общий канал доступа» (RACH) этой соты, чтобы сообщить о том, что его текущее местоположение – тут, в это самой соте. Эта информация (пара LAC+CellID) попадает в контроллер базовых станций (BSC), а от него – передается коммутатору (MSC), который обслуживает эту часть сети. Коммутатор сохраняет информацию о текущем местоположении телефона в специальном кэше, называемом VLR (Visitor Location Register). В дальнейшем телефон периодически (обычно раз в час, но зависит от настроек сети) будет выполнять LU. Либо же, если абонент передвигается, то телефон будет выполнять LU при переходе в зону покрытия соты из другого LA. В быту это проявляется в виде специфических звуковых наводках, если телефон находиться рядом с колонками (наушниками).

Выделение каналов

В заключение рассмотрение особенностей функционирования GSM сети кратко опишем реализацию выделения каналов в радиодиапазоне. Это важно для понимания особенностей перехвата сигналов в сети GSM.

Для GSM выделен спектр определенной частоты, поэтому необходимо оптимально распределить ширину полосы между всеми возможными пользователями. Как уже упоминалось ранее, GSM использует комбинацию методов множественного доступа TDMA и FDMA (Time– and Frequency–Division Multiple Access).

Сначала полоса частот в 25 МГц делится на полосы в 200 Кгц. Каждой станции соответствует своя полоса (или несколько полос). Абоненты полосы разделены во времени, каждый из каналов делиться между 8 абонентами. Каждому абоненту соответствует один кадр. Восемь кадров объединяются во фрейм (TDM – кадр). 26 фреймов, в свою очередь, образуют мультифрейм, который повторяется циклически. Длина мультифрейма – 120 миллисекунд. На один кадр приходится 1/200 мультифрейма, т.е. около 0.6 миллисекунды (рис. 119). Как видно из рис. 1, позиция 12 в мультифрейме занята для целей управления, а 25–я зарезервирована для будущих применений.

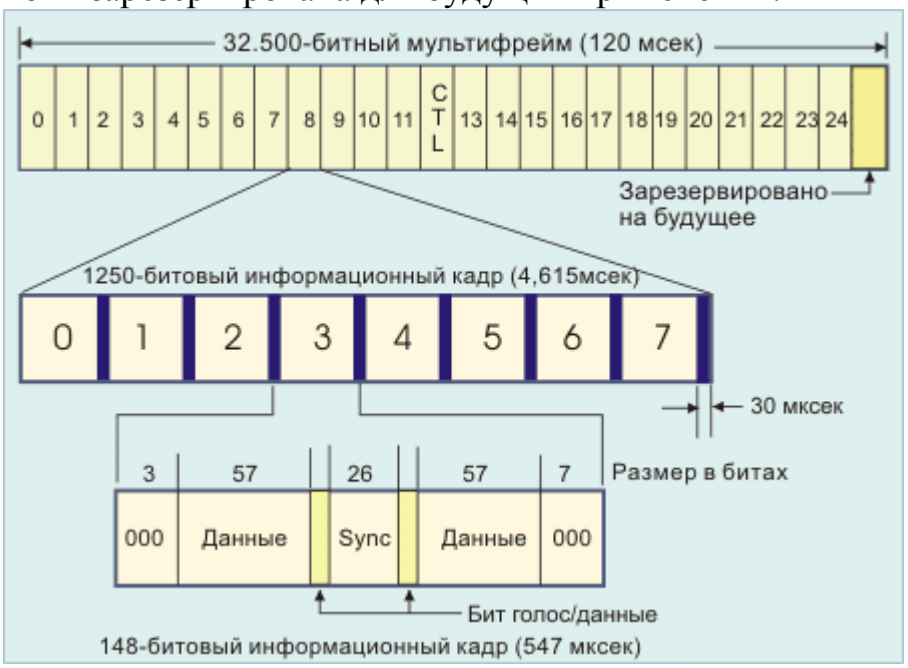

Рис. 119. Структура кадров в GSM

Каналы определяются числом и позицией соответствующих им циклличных кадров, и вся палитра повторяется приблизительно каждые 3 часа. Они делятся на предписанные каналы (dedicated channels), или каналы трафика, каждый из которых соответствует одной MS (mobile station, телефон), и общие каналы (common channels), или каналы управления, используемые MS в пассивном режиме.

Каналы трафика применяются для переноса речевого потока и потока данных. Эти каналы для восходящего и нисходящего звеньев разделены во

времени тремя кадрами, так, чтобы MS мог осуществлять прием и передачу информации в разное время. Это позволяет упростить электронное оборудование MS и сделать его более компактным.

Общие каналы используются свободными MS при обмене сигнальной информацией, необходимой для перехода в режим занятости. MS, находящиеся в режиме занятости, оповещают близлежащие базовые станции о перемещении в другую ячейку и передают необходимую информацию.

8.2 Безопасность GSM

В стандарте GSM следующие механизмы безопасности:

– аутентификация;

– секретность передачи данных;

– секретность абонента;

– секретность направлений соединения абонентов.

Защита сигналов управления и данных пользователя осуществляется только по радиоканалу. Режимы секретности в стандарте GSM определяются Рекомендациями, приведенными в табл. 23.

Таблица 23.

GSM 02.09	Аспекты секретности	Определяет характеристики безопасности, применяемые в сетях GSM. Регламентируется их применение в подвижных станциях и сетях
GSM 03.20	Секретность, связанная с функциями сети	Определяет функции сети, необходимые для обеспечения характеристик безопасности, рассматриваемых в рекомендациях GSM 02.09
GSM 03.21	Алгоритмы секретности	Определяет криптографические алгоритмы в системе связи
GSM 02.17	Модули подлинности абонентов (SIM)	Определяет основные характеристики модуля SIM

Аутентификация

Как было отмечено ранее в описании архитектуры, аутентификацией в GSM занимается подсистема AUC. Рассмотрим работу этого компонента подробнее.

В процессе производства SIM–карт производитель заносит в ROM каждой карты случайное число, называемое «K_I» (Key for identification). Это число будет служить секретным ключом для данной SIM–карты. Когда SIM–

карты доставляются мобильному оператору, с ними передаются данные о K_I каждой новой SIM–карты. Эти данные (в виде пар (IMSI, K_I)) заносят в «центр аутентификации» мобильной сети (AUC).

При регистрации телефона в сети, его IMSI передается в AUC, который передает обратно случайное число (RAND). Дальше SIM–карта и AUC параллельно выполняют одно и то же вычисление: (SRES, K_C) = A3/A8(RAND, K_I), где «A3/A8» – название стандартных алгоритмов вычисления SRES (Signed RESponse) и K_C (Key for ciphering) соответственно.

Телефон передает вычисленное SIM–картой значение SRES обратно в AUC, который сравнивает его со своим SRES. Если результаты совпали, то SIM–карта является подлинной.

Вычисленное значение K_C сохраняется в AUC/HLR/VLR и энергонезависимой памяти SIM–карты до следующей регистрации карты в сети и используется для шифрования голосового траффика, идущего по радио интерфейсу. Расшифровкой занимается BTS и дальше (по наземным каналам) в сторону BSC поток данных идет оцифрованным, но нешифрованным. Фраза «возможен перехват до 16/256/1024 одновременных разговоров на интерфейсе Abis» в описании устройств перехвата GSM трафика означает что речь идет именно о интерфейсе между BTS и BSC, где голосовой поток уже расшифрован. Организация собственно физической «врезки» в этот интерфейс оставляется на откуп пользователю этого устройства.

Исходя из схемы можно понять, что основу системы безопасности GSM составляют 3 секретных алгоритма (официально не раскрытые до сих пор, сообщаемые только тем, кому это требуется – поставщикам оснащения, операторам связи и т.д.):

A3 – алгоритм аутентификации, защищающий телефон от клонирования;

A8 – алгоритм создания криптоключа, однонаправленная функция, которая берет фрагмент выхода от A3 и превращает его в сеансовый ключ для A5;

A5 – собственно алгоритм шифровки оцифрованной речи для обеспечения конфиденциальности переговоров. В GSM применяются 2 главные разновидности алгоритма: A5/1 – полноценная версия шифра для избранных стран (в основном ЕС и США) и A5/2 – ослабленная для всех прочих.

В основе алгоритма A5 лежит разработанный французскими военными специалистами–криптографами поточный шифр. Этот шифр обеспечивал достаточно хорошую защищенность потока, что обеспечивало конфиденциальность разговора. Изначально экспорт стандарта из Европы не предполагался, но вскоре в этом появилась необходимость.

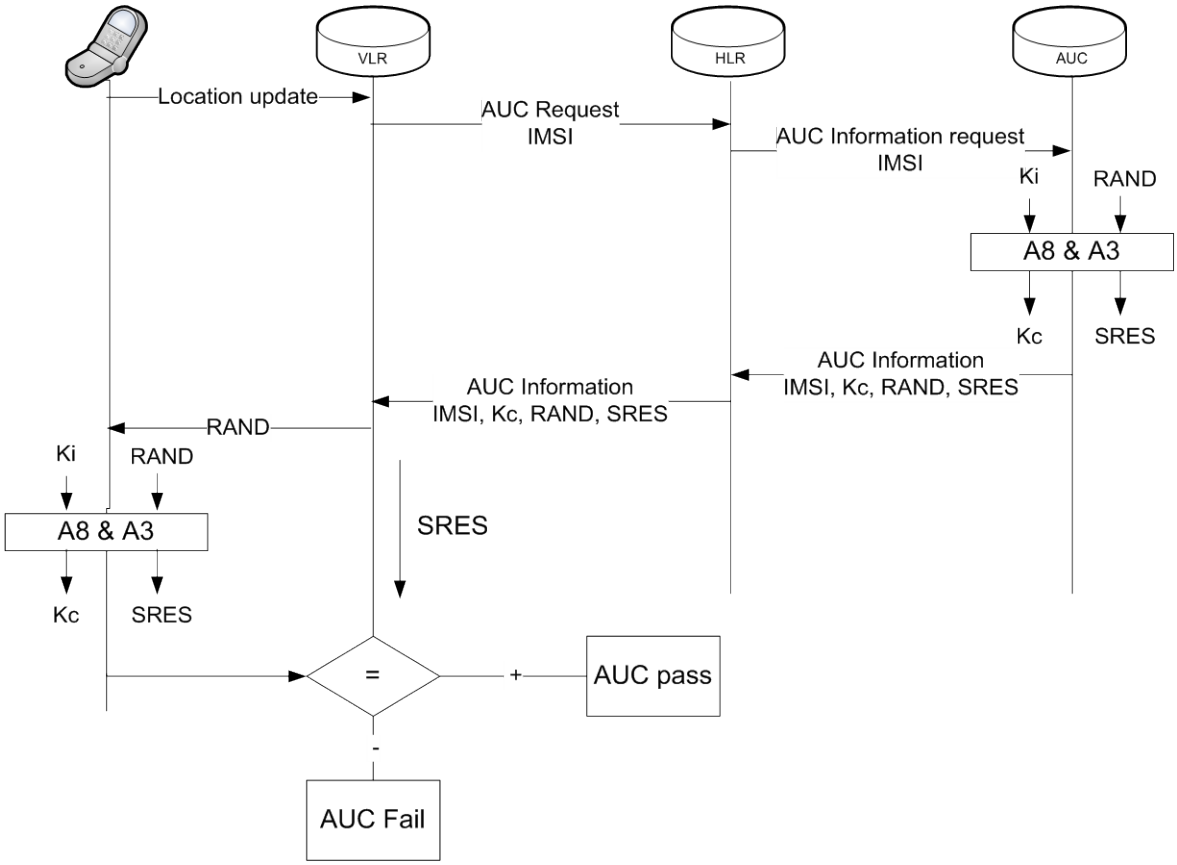

Рис.120. Процесс аутентификации SIM в сети GSM.

Именно поэтому, A5 переименовали в A5/1 и стали распространять в Европе и США. Для остальных стран (в том числе и России) алгоритм модифицировали, значительно понизив криптостойкость шифра. A5/2 был специально разработан как экспортный вариант для стран, не входивших в Евросоюз. Криптостойкость A5/2 была понижена добавлением еще одного регистра (17 бит), управляющего сдвигами остальных. В A5/0 шифрование отсутствует совсем. В настоящее время разработан также алгоритм A5/3, основанный на алгоритме Касуми и утвержденный для использования в сетях 3G. Эти модификации обозначают A5/x.

Сотовые станции (телефоны) оснащены смарт–картой, содержащей A3 и A8, а в самом телефоне есть ASIC–чип с алгоритмом A5. Базовые станции тоже оснащены ASIC– чипом с A5 и “центром аутенитификации”, использующим алгоритмы A3–A8 для идентификации сотового абонента и создании сеансового ключа.

Вся эта архитектура при надлежащем исполнении и качественных алгоритмах призвана гарантировать надежную аутентификацию пользователя, обеспечивая защиту сотовых станций от клонирования и остальных методов

мошенничества, и качественное шифрование конфиденциальных переговоров.

Обеспечение секретности абонента

Для исключения определения (идентификации) абонента путем перехвата сообщений, пере даваемых по радиоканалу, каждому абоненту системы связи присваивается «временное удостоверение личности» – временный международный идентификационный номер пользователя (TMSI), который действителен только в пределах LA. В другой LA ему присваивается новый TMSI. Если абоненту еще не присвоен временный номер (например, при первом включении MS), идентификация проводится через международный идентификационный номер (IMSI). После окончания процедуры аутентификации и начала режима шифрования временный идентификационный номер TMSI передается на MS только в зашифрованном виде. Этот TMSI будет использоваться при всех последующих доступах к системе. Если MS переходит в новую LA, то ее TMSI должен передаваться вместе с идентификационным номером зоны (LAC), в которой TMSI был присвоен абоненту.

При входе MS в новую LAC осуществляется процедура опознавания, которая проводится по старому, зашифрованному в радиоканале TMSI, передаваемому одновременно с LAC. LAC дает информацию центру коммутации и центру управления о направлении перемещения MS и позволяет запросить прежнюю зону расположения о статусе абонента и его данные, исключив обмен этими служебными сообщениями по радиоканалам управления.

8.3 Перехват информации в GSM

Клонирование SIM карты

Одной из распространенных проблем является клонирование SIM карты. В Интернете часто можно встретить объявления о легком способе клонировании карты, а также представлено множество утилит, например, SIM Card Seizure. В качестве целей клонирования обычно указывают возможность бесплатно звонить за чужой счет и возможность прослушивания разговоров владельца клонированной SIM–карты. В первом варианте использования у владельца клона будут проблемы с получением входящих звонков, а вот исходящие можно делать свободно. Основными потребителями являются люди, которые затем у метро предлагают прохожим дешево позвонить в любую страну мира. Что касается прослушивания абонента, то рассмотрению этого вопроса посвящен следующий раздел.

В предыдущем разделе была описан процесс проверки подлинности SIM–карты (рис. 120). Базовыми в этом процессе являются параметры IMSI и

K_I. Для того чтобы клон мог пройти аутентификацию в AUC, он должен знать эти параметры. Узнать IMSI просто, он может быть записан на самой карте или прилагаться к ней. Его легко можно прочитать с SIM-карты при помощи устройства чтения смарт–карт. А вот с K_I все несколько сложнее.

Как вы уже знаете, K_I хранится всего в двух местах – в памяти SIM–карты и в памяти AUC. K_I никогда не передается в открытом виде при аутентификации, т.е. его нельзя перехватить при аутентификации. У злоумышленников есть 4 варианта получения K_I. Первый вариант это инсайдер в компании–операторе. Этот вариант предпочтительнее, т.к. можно получить информацию сразу по нескольким картам. Недостатки этого варианта заключаются в том, что ввиду значимости K_I доступ к их значениям строго ограничен и при обнаружении массовой утечки инсайдер быстро будет вычислен. Кроме того, зачастую в AUC отсутствует функционал для считывания K_I из тех же соображений безопасности. Второй вариант основан на похищении K_I сразу после получения партии SIM–карт от производителя. Проблемы здесь те же что и в предыдущем варианте: количество людей, имеющих нужные доступы, исчисляется единицами.

Третий вариант: считать K_I из памяти SIM-карты. Начнем с того что необходимо получить физический доступ к карте (вынуть ее из телефона жертвы под каким-то предлогом, знать PIN код). Важный недостаток: у SIM–карты нет интерфейса, по которому можно непосредственно считать или изменить K_I.

И наконец, последний вариант: вычислить K_I. Злоумышленник должен обладать сведениями об используемом оператором алгоритме A3. В этом случае можно попытаться вычислить K_I, наблюдая за результатами преобразования RAND в SRES. Для этого вручную формируют RAND, вызывают алгоритм шифрования и передают ему RAND. Этот процесс автоматизируют такие программы как SimScan и WoronScan.

Именно таким образом были получены первые клоны SIM–карт. Это стало доступно из-за утечки сведений об алгоритме A3, называемой COMP128 в сеть. В алгоритме была обнаружена уязвимость, которая позволяла подбирать K_I за приемлемое количество попыток. После обнаружения уязвимости большинство операторов заменило его чем-то более устойчивым. На текущий момент существует три версии COMP128. Вторая и третья версия на данный момент считаются невскрываемыми. И хотя в сети присутствуют программы, декларирующие возможность взлома этих версий, на поверку всегда оказывается, что их цель – заставить пользователя скачать «трояна».

Если же злоумышленник не имеет сведений о реализации A3, то он может попытаться подобрать K_I путем перебора (brute force). Здесь возникает еще одно препятствие: количество попыток для подбора K_I ограничено. У

SIM–карты есть встроенный счетчик количества вызовов A3, и при превышении определенного порога (65535) карта блокируется и перестает отвечать на запросы регистрации (хотя остальные функции работают, например, телефонная книга). В обычных условиях эксплуатации, когда A3 вызывается при каждой регистрации SIM–карты в сети (при включении телефона), подобные ограничения не мешают абоненту. А вот для получения K_I может понадобиться большее количество попыток.

Если же злоумышленнику удалось подобрать K_I, то он получает возможность звонить за чужой счет. Но тут есть несколько ограничивающих факторов. Во-первых, т.к. деньги на счету начнут быстрее, чем обычно, весьма вероятно, что владелец SIM-карты может это заметить. В детальной распечатке сразу обнаружатся «лишние» звонки. Это касается и «безлимитных» тарифов, т.к. у них тоже есть ограничения, в частности при звонках за границу. Поэтому, злоумышленники стремятся как можно скорее выговорить весь доступный баланс и избавиться от клона. Во-вторых, если обе карты зарегистрированы в сети, то входящие звонки будут приходить на карту, которая последняя авторизовалась, либо с которой был совершен последний исходящий звонок. Соответственно, легитимный пользователь может заметить, что ему перестанут приходить ожидаемые звонки. Злоумышленникам в целях конспирации вообще противопоказано снимать трубку. Иначе корреспонденты пользователя сразу обнаружат мошенничество. В-третьих, оператор может вычислять SIM-карты, которые регистрируются в сети в географически разнесенных местах в течение ограниченного времени. При подозрениях в клонировании карты оператор заблокирует карту и выдаст абоненту новую.

Резюмируя, можно сказать, что клонировать SIM-карты возможно, но достаточно тяжело. Если оператор своевременно модернизировал реализацию A3, а его сотрудники лояльны и неподкупны, то абонентам не стоит бояться появления клонов своей SIM–карты. Кроме того, актуальность такого мошенничества спадает, т.к. спрос на дешевые звонки за границу компенсируется возможностью звонков в Skype, а также предложениями от легальных операторов.

Перехват разговоров в сети GSM

Переходим к рассмотрению взлома GSM. Статьи про уязвимости в A5/1 появились около 15 лет назад, но публичной демонстрации взлома A5/1 в условиях реального мира до сих пор не было. Более того, как видно из описания работы сети надо понимать, что помимо взлома самого алгоритма шифрования нужно решить еще ряд сугубо инженерных проблем, которые обычно всегда опускаются из рассмотрения (в том числе на публичных демонстрациях).

Большинство статей по взлому GSM опираются на статью Эли Баркана в 2006 году и исследование Карстена Нола (Karsten Noh).

В своей статье Баркан с соавторами показал, что т.к. в GSM коррекция ошибок идет до шифрования (а надо бы наоборот), возможно определенное уменьшение пространства поиска для подбора K_C и реализация known–ciphertext атаки (при полностью пассивном прослушивании эфира) за приемлемое время с помощью предварительно вычисленных данных.

Сами авторы статьи говорят, что при приеме без помех для взлома в течение 2 минут требуется 50 терабайт предвычисленных данных. В той же статье (в разделе про A5/2) указывается, что сигнал из эфира всегда идет с помехами, которые усложняют подбора ключа. Для A5/2 приведен измененный алгоритм, который способен учитывать помехи, но при этом требует вдвое большего объема предвычисленных данных и, соответственно, время взлома увеличивает в два раз. Для A5/1 указана возможность построения аналогичного алгоритма, но сам он не приведен. Можно предположить, что в этом случае также нужно увеличить объем предвычисленных данных вдвое.

Процесс подбора ключа A5/1 является вероятностным и зависит от времени, т.е. чем дольше идет прослушивание, тем больше вероятность подобрать K_C. Таким образом, заявленные в статье 2 минуты – это примерное, а не гарантированное время подбора K_C.

Карстен Нол разрабатывает самый известный проект по взлому GSM сетей. Его фирма, занимающаяся проблемами компьютерной безопасности, собиралась к концу 2009 года выложить в открытый доступ радужные таблицы сессионных ключей алгоритма A5/1, который используется для шифрования речи в сетях GSM.

Свой демарш против A5/1 Карстен Нол объясняет желанием привлечь внимание общественности к существующей проблеме и заставить операторов связи переходить на более совершенные технологии. Например, технология UMTS предполагает использование 128 битного алгоритма A5/3, стойкость которого такова, что никакими доступными средствами на сегодняшний день взломать его не удастся.

По расчетам Карстена, полная таблица ключей A5/1 в упакованном виде будет занимать 128 петабайт и распределенно храниться на множестве компьютеров в сети. Для ее расчета потребуется около 80 компьютеров и 2–3 месяца работы. Существенное уменьшение времени вычислений должно оказать использование современных CUDA графических карт и программируемых массивов Xilinx Virtex. В частности много шума наделало его выступление на 26C3 (Chaos Communication Congress) в декабре 2009 года. Кратко сформулировать суть выступления можно так: в скором времени можно ожидать появление бюджетных системы для онлайн декодирования A5/1.

Переходим к инженерным проблемам. Как получить данные из эфира? Для перехвата разговоров надо иметь полноценный сканер, который должен уметь разбираться, какие базовые вещают вокруг, на каких частотах, каким операторам они принадлежат, какие телефоны с какими TMSI в настоящий момент активны. Сканер должен уметь следить за разговором с указанного телефона, корректно обрабатывать переходы на другие частоты и базовые станции.

В интернете есть предложения по приобретению подобного сканера без дешифратора за 40–50 тыс. долларов. Это нельзя назвать бюджетным устройством.

Таким образом, для создания прибора, который после несложных манипуляций мог начинать прослушивать разговор по телефону, необходимо:

а) реализовать часть, которая работает с эфиром. В частности, позволяет указать, какой из TMSI соответствует искомому телефону или с помощью активных атак заставить телефоны «обнаружить» свои реальные IMSI и MSISDN;

б) реализовать алгоритм подбора K_C для A5/1, хорошо работающий на реальных данных (с помехами/ошибками, пропусками и т.п.);

в) рассчитать для него «радужные таблицы» (rainbow tables);

г) объединить все эти пункты в законченное работающее решение.

Карстен и остальные исследователи в основном решают пункт «в». В частности он его коллеги предлагают использовать OpenBTS, airdump и Wireshark для создания перехватчика IMSI (IMSI catcher). Подробнее об устройстве и перехвате с его помощью звонков написано ниже в разделе «Атака человек-по-середине в GSM». Пока можно сказать, что это устройство эмулирует базовую станцию и встраивается между MS и настоящей базовой станцией.

Докладчики утверждают, что SIM–карта легко может запретить телефону показывать, что он работает в режиме шифрования A5/0 (т.е. без шифрования вообще) и что большинство SIM–карт в обороте именно такие. Это действительно возможно. В GSM 02.07, написано (Normative Annex B.1.26), что SIM–карта содержит специальный бит OFM в поле Administrative , который при значении равном единице, приведет к запрету индикации шифрования соединения (в виде амбарного замочка). В GSM 11.11 указаны следующие права доступа к этому полю: чтение доступно всегда, а права на запись описаны как «ADM». Конкретный набор прав, регулирующих запись в это поле, задается оператор на этапе создания SIM–карт. Таким образом, докладчики надеются, что большая часть карт выпускается с установленным битом и телефоны у них действительно не показывают индикацию отсутствия шифрования. Это действительно существенно облегчает работу IMSI catcher–а т.к.

владелец телефона не может обнаружить отсутствие шифрования и что–то заподозрить.

Интересная деталь. Исследователи столкнулись с тем, что прошивки телефонов тестируются на соответствие спецификациям GSM и не тестируются на обработку нештатных ситуаций, поэтому, в случае некорректной работы базовой станции (например, «подставная» OpenBTS, которая использовалась для перехвата) телефоны зачастую зависают.

Наибольший резонанс вызвало заявление, что всего за $1500 можно из USRP, OpenBTS, Asterisk и airprobe собрать готовый комплект для прослушивания разговоров. Эта информация широко разошлась по Интернету, только авторы этих новостей и производных от них статей забыли упомянуть, что сами докладчики деталей не предоставили, а демонстрация не состоялась.

В декабре 2010 года Карстен и Мунот (Sylvain Munaut) снова выступил на конференции 27C3 с докладом про перехват разговоров в GSM сетях. На этот раз они представили более полный сценарий, но в нем присутствует множество «тепличных» условий.

Для обнаружения местоположения они используют интернет–сервисы, которые дают возможность вбрасывать в сеть SS7 запросы «send routing info». SS7 – это сеть/стек протоколов, которые используются для общения телефонных операторов (GSM и «наземных») друг с другом и для общения компонент сети GSM друг с другом.

Далее авторы делают ссылку на реализацию мобильной связи в Германии. Там полученное в результате запроса RAND хорошо коррелирует с кодом региона (area code/zip code). Поэтому такие запросы там дают возможность определить с точностью до города или даже части города, где в Германии находится этот абонент. Но так делать оператор не обязан.

Теперь исследователи знают город. После этого они берут сниффер, едут в найденный ранее город и начинают посещать все его LAC. Приехав на территорию, которая входит в какой–то LAC, они посылают жертве SMS и слушают, идет ли пейджинг(paging) телефона жертвы (это происходит по незашифрованному каналу, во всех базовых сразу). Если вызов есть, то они получают сведения о TMSI, который был выдан абоненту. Если нет – едут проверять следующий LAC.

Необходимо заметить, что т.к. IMSI при пейджинге не передается (и исследователи его не знают), а передается только TMSI (который они и хотят узнать), то производится «атака по времени» (timing attack). Они посылают несколько SMS с паузами между ними, и смотрят, для каких TMSI производится пейджинг, повторяя процедуру до тех пор, пока в списке «подозрительных» TMSI не останется только один (или ни одного).

Чтобы жертва не заметила такого «прощупывания», посылается такой SMS, который не будет показан абоненту. Это или специально созданный flash sms, или неверный (битый) SMS, который телефон обработает и удалит, при этом пользователю ничего показано не будет.

Выяснив LAC, они начинают посещать все соты этого LAC, посылать SMS–ки и слушать отклики на пейджинг. Если есть ответ, то жертва находится вот в этой соте, и можно начинать взламывать ее сессионный ключ (K_C) и слушать ее разговоры.

Перед этим необходимо записать эфир. Здесь исследователи предлагают следующее:

1) существуют производимые на заказ FPGA–платы, которые способны одновременно записывать все каналы либо uplink (канал связи от абонента (телефона или модема) к базовой станции сотового оператора), либо downlink (канал связи от базовой станции к абоненту) частот GSM (890–915 и 935–960 МГц соответственно). Как уже было отмечено, стоит такое оборудование 40–50 тыс. долларов, поэтому доступность такого оборудования для простого исследователя безопасности сомнительна;

2) можно брать менее мощное и более дешевое оборудование и слушать часть частот на каждом из них. Такой вариант стоит примерно 3,5 тыс. евро с решением на базе USRP2;

3) можно сначала сломать сессионный ключ, и потом декодировать траффик «на лету» и следовать за сменой частоты (frequency hopping) при помощи четырех телефонов, у которых вместо родной прошивки стоит альтернативная прошивка OsmocomBB. Роли телефонов: 1–й телефон используется для пейджинга и контроля ответов, 2–й телефон выделен абоненту для разговора. При этом каждый телефон должен писать и прием и передачу. Это очень важный пункт. До этого момента OsmocomBB фактически не работал и за год (с 26C3 до 27C3) OsmocomBB был доделан до пригодного к использованию состояния, т.е. до конца 2010 года не было практического работающего решения.

Взлом сессионного ключа. Находясь в одной соте с жертвой, они посылают ей SMS, записывают общение жертвы с базовой, и взламывают ключ, пользуясь тем, что во время установления сессии (session setup) происходит обмен множеством полупустых пакетов или с предсказуемым содержимым. Для ускорения взлома используются радужные таблицы. На момент проведения 26C3 эти таблицы были не так хорошо заполнены и взлом делался вовсе не за минуты и даже не за десятки минут (авторы упоминают час). То есть, до 27C3 даже у Карстена (основного исследователя в этой области) не было решения, которое позволяло взломать K_C за приемлемое время (в течении которого, скорее всего, не произойдет смена сессионого ключа (rekeying)).

Затем исследователи пользуются тем, что смена ключа редко делается после каждого звонка или SMS и сессионный ключ, который они узнали, не будет меняться в течение какого–то времени. Теперь, зная ключ, они могут декодировать зашифрованный траффик к/от жертвы в режиме реального времени, и делать смену частоты (frequency hopping) одновременно с жертвой. Для захвата эфира в этом случае реально достаточно четырех перепрошитых телефонов, так как не требуется писать все частоты и все таймслоты. Исследователи продемонстрировали эту технологию в работе. Правда «жертва» сидела на месте и обслуживалась одной сотой.

Подводя промежуточный итог можно утвердительно ответить на вопрос о возможности перехвата и расшифровке на лету GSM разговоров. При этом надо иметь помнить следующее:

1) Технология, описанная выше не существует в виде, доступном для любого желающего (в т.ч. script kiddies). Это даже не конструктор, а заготовка для деталей конструктора, которые надо доделывать до пригодного к использованию состоянию. Исследователи неоднократно замечают, что у них нет четких планов по выкладыванию в общий доступ конкретики реализации. Это означает, что на основании этих наработок производители Ближнего Востока не изготавливают массово устройства за 100 долларов, которые могут слушать все.

2) OsmocomBB поддерживает только одно семейство чипов (хотя и самое распространенное).

3) Способ определения местоположения по запросам к HLR и перебору LAC работает скорее в теории, чем на практике. На практике злоумышленник или знает, где находится жертва физически, или не может попасть в туже соту что и жертва. Если злоумышленник не можете послушать ту же соту, в которой находиться жертва, то способ не работает.

В отличие от демонстрации, в реальности в средней по нагрузке LA присутствуют тысячи пейджинговых сообщений. Более того, пейджинг работает не в момент отправки, а в определенные временные окна и пачками (по пейджинг–группам со своими очередями, номер которой есть остаток от деления IMSI на количество каналов, которое в каждой соте может быть свое), что опять усложняет реализацию.

4) Допустим, LA найден. Теперь надо “нащупать” ответ абонента. Передатчик телефона имеет мощность 1–2 ватта. Соответственно, просканировать его с расстояния нескольких десятков метров тоже является задачей (не простой). Получается парадокс: LA накрывает, например, целую область (город). В ней, например, 50 сот, у некоторых из которых радиус действия доходит до 30 км. Мы пытаемся поймать и расшифровать на ненаправленную антенну излучение. Для реализации этой задачи в таком варианте требуется

много оборудования. Если же исходить из предпосылки, при которой жертва находиться в прямой видимости, т.е. расстояния, на котором перехват выглядит более реалистичным, намного эффективнее и проще направленный микрофон. Надо отметить, что на демонстрации исследователи перехватывают свои телефоны на расстоянии 2–х метров.

5) Перемещение жертвы между сотами также вызывает проблемы, т.к. вам также надо перемещаться вместе с ней.

6) Телефоны, используемые в демонстрации, требуют аппаратной модификации, в них нужно убрать фильтр с антенны, в противном случае телефоны «чужой» uplink не «увидят». Фильтр в телефоне нужен для того что бы «слушать» не все частоты, а только «свою».

7) Если в сети регулярно происходит смена ключа (rekeying) или меняются TMSI (ни один из исследователей не учитывал это), то это способ не работает вообще или работает очень плохо (время расшифровки может оказаться больше чем время разговора).

8) Прослушивать всю сеть не получится, надо знать номер телефона.

Защита от перехватывания трафика

Как правильно замечают авторы, защититься от этого конкретного способа достаточно легко:

1) Вместо константного байта использовать для пейджинга пустых GSM–сообщений случайные значения.

2) Менять K_C после каждого звонка.

3) Менять TMSI как можно чаще.

Пункты 2 и 3 можно решить простой переконфигурацией элементов сети провайдера и не требуют обновления прошивок или оборудования.

Помимо этого, на рынке представлены разные модифицированные телефоны, например, крипто смарт телефон «Cancort», который обеспечивает работу на линиях связи стандарта GSM 900/1800 в двух режимах:

Открытый режим (обычный режим GSM);

Режим шифрования с гарантированным от взлома шифрованием информации.

Cancort выполняет следующие функции:

– шифрование/расшифровка голосовой информации.

– шифрование/расшифровка коротких сообщений (услуга SMS)

– шифрование/расшифровка данных (услуга BS26 и GPRS).

– шифрование/расшифровка электронной почты.

– шифрование/расшифровка информации всех телефонных директорий (SIM PB).

– шифрование/расшифровка информации MMS.

Также для защиты можно использовать скремблеры, которые хорошо зарекомендовали себя при защите обычных телефонных сетей. В качестве примера можно привести GUARD GSM. Данное устройство (как и аналоги) соединяется с сотовым телефоном по проводной гарнитуре и имеет небольшие размеры. Скремблер GUARD GSM имеет тридцать два режима скремблирования.

Принцип работы данного скремблера основан на первоначальном разрушении и временной перестановки звука на передающей стороне с его последующим восстановлением на принимающей стороне. Этот процесс двухсторонний. Временная перестановка отрезков речевого сигнала и восстановление их последовательности на приеме занимают некоторый интервал времени. Поэтому обязательным свойством такой аппаратуры является небольшая задержка сигнала на приемной стороне. Начало разговора, как правило, начинается в открытом режиме и далее по обоюдной команде устройства переключаются в режим скремблирования. При ведении переговоров прибор выполняет одновременно две функции скремблирование и дескремблирование. То есть произнесенная одним из абонентов речь шифруется с его стороны, а второй скремблер, находящийся у второго абонента расшифровывает данную речь. И тоже самое происходит в обратном направлении, когда начинает говорить второй абонент.

Технические характеристики:

1. Разборчивость речи не менее 95%.
2. Тип соединения полный дуплекс.
3. Задержка сигнала в линии не более 100 мс.
4. Уровень защищенности линейного сигнала временный.
5. Использование в сетях стандарта GSM 900/1800.
6. Тип подключения к сотовому телефону проводная гарнитура
7. Габаритные размеры 80x45x16 мм

Атака “человек-по-середине” в GSM

Рассмотренная ранее атака активно использовала устройство под названием IMSI–catcher. В этом разделе рассматривается принцип работы подобного устройства и его ограничения.

В Интернет можно встретить множество предложений по продаже специальных устройств, которые могут эмулировать базовые станции. В подобных объявлениях декларируется, что такие эмуляторы позволяют скрытно прослушивать любые разговоры, не ставя в известность оператора и даже не зная номера телефона прослушиваемого человека.

Устройства с подобным функционалом действительно существуют (например, производимый компанией Rohde & Schwarz комплекс RA 900), но они обладают далеко не столь впечатляющими возможностями:

1) скрытно можно только установить, находится ли в зоне покрытия телефон, в который вставлена SIM–карта с указанным IMSI, либо получить список IMSI/IMEI но не номеров телефонов в зоне покрытия «псевдобазовой». Это подразумевает, что злоумышленнику известен IMSI.
2) Можно прослушивать исходящие разговоры с конкретного телефона, но у абонента при этом будет отключено шифрование сигнала. Кроме того, номер звонящего абонента будет изменен или скрыт. При этом сам абонент может это обнаружить и установить факт прослушивания (или заподозрить).
3) При непосредственном прослушивании входящие звонки не могут быть доставлены абоненту и, соответственно, не могут быть прослушаны. Для остальных абонентов сети прослушиваемый абонент находится «вне зоны покрытия».

Как видно, функционал предполагает наличия определенных сведений о жертве.

Принципы работы IMSI–catcher

IMSI–catcher представляет собой устройство, которое, с одной стороны, ведет себя как базовая станция сети GSM, а с другой стороны содержит в себе SIM–карту или какие–то другие технические средства для соединения с коммуникационными сетями. Используется оно следующим образом:

1. Устройство размещается недалеко от мобильного телефона жертвы. Дальность определяется исходя из уровня мощности реальной базовой станции.
2. При работе устройство представляется обычной станцией. Естественно что она должна выдавать себя за станцию того оператора, к которому принадлежит жертва. В стандарте GSM не требуется, чтобы базовая станция подтверждала свою аутентичность телефону (в отличие от сетей UMTS, например), поэтому сделать это достаточно легко. Частота и мощность сигнала поддельной базы подбираются так, чтобы реальные базовые станции всех соседних сетей не создавали ей помех в работе.
3. Телефон жертвы заставляют выбрать поддельную базу в качестве наилучшей доступной базовой станции из–за ее хорошего и мощного сигнала. Принцип выбора был описан ранее. В результате, злоумышленник может определить IMEI жертвы.
4. Для прослушивания разговоров при регистрации поддельная база сообщает телефону о необходимости перехода в режим шифрования A5/0, то есть без шифрования вообще. Телефон по стандарту GSM не может отказаться.

5. После этого все исходящие звонки жертвы проходят через поддельную станцию в открытом виде и могут быть там записаны/прослушаны. Устройство при этом выступает в роли прокси, самостоятельно соединяясь с набранным номером и прозрачно транслируя сквозь себя голос в обе стороны.

Ограничения IMSI–catcher

1. При подключении к поддельной станции жертва становится недоступной для входящих звонков. Для обеспечения поддержки входящих звонков устройство должно обслуживаться сетью оператора так же как остальные базовые станции. Для этого надо подключиться к какому–то контроллеру базовых станций (BSC) и прописаться в его таблицах маршрутизации. Но если у злоумышленника есть доступ к сети оператора на уровне, позволяющем подключать и конфигурировать новые базовые станции, то в этом случае эффективнее использовать COPM. Если кроме жертвы в зону покрытия устройства попадут другие мобильные телефоны, расположенные рядом с жертвой, то они будут показывать наличие покрытия, но ни входящие, ни исходящие звонки обслуживаться не будут. Это может вызвать подозрения.

2. Большинство современных телефонов имеют индикацию шифрования (в виде замочка) и жертва может насторожиться, если увидит, что соединение не шифруется.

3. Для трансляции исходящих звонков, устройству нужен выход в телефонную сеть. Если для этого используется собственный GSM–модуль с SIM–картой, то исходящие звонки от поддельной станции будут совершаться с номером, отличным от номера жертвы. Для сокрытия этого можно использовать услугу «сокрытие номера звонящего» (calling line identification restriction, CLIR), что также может насторожить получателей звонка и они могут сообщить об этом жертве. Как вариант, при использовании WiFi+VoIP можно подменить номер поддельной станции на правильный, но это усложняет конструкцию.

Для более точной подмены необходимо чтобы устройство использовало SIM–карту того же оператора, которым пользуется жертва, в этом случае у злоумышленника будет возможность транслировать звонки жертвы на служебные и короткие номера.

4. Если жертва движется, то может легко выйти из зоны покрытия устройства, это приведет к тому, что процесс надо будет начинать сначала.

Перечисленные недостатки показывают, применение подобного устройства ограничивается краткосрочным перехватом разговоров и практически не подходит для длительного прослушивания.

Таким образом, основная польза от подобного устройства может быть в том, чтобы идентифицировать IMSI/IMEI жертвы, про которую точно известно только ее местоположение, а потом уже использовать сведения о IMSI для проведения обычного прослушивания средствами СОРМ.

Заключение

Перехват сообщений в GSM сетях возможен. Но, учитывая условия, необходимые для реализации перехвата, можно сказать, что GSM защищен намного лучше, чем это показано в фильмах и Интернете.

9. ПОЛУЧЕНИЕ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Применение компьютерной техники для решения разнообразных задач по хранению, обработке и передаче информации приводит к тому, что часть задач по перехвату данных лежит в плоскости обеспечения компьютерной безопасности. Целью злоумышленников становятся процессы, связанные в той или иной степени с использованием компьютерного оборудования для работы с информацией. При этом подвергаются воздействию все составляющие этого процесса:

- хранение информации;
- обработка информации;
- передача информации.

От злоумышленников исходят угрозы безопасности, которые могут быть связаны, как с особенностями функционирования компьютерных сетей (логическими и физическими), так с ошибками в реализации тех или иных функций по работе с информацией.

Далее в главе будет рассмотрены отдельно обозначенные группы способов получения информации злоумышленниками в компьютерных сетях.

9.1. Основные способы несанкционированного доступа

Под основными способами несанкционированного доступа к компьютерной информации обычно понимают следующие:

- несанкционированный доступ к информации на физическом носителе
- методы преодоления парольной защиты;
- перехват информации в каналах связи;
- использование недостатков программного кода для получения доступа к информации
- внедрение вредоносного программного кода
- навязывание небезопасной передачи информации;
- использование аппаратных закладок;
- перехват побочных электромагнитных излучений и наводок (ПЭМИН), и другие.

Такое деление является в значительной степени условным, так как практически каждый из приведенных способов может в определенных случаях выступать составной частью любого другого из перечисленных.

Аппаратные закладки – это специальные микросхемы, выполняющие те же функции по съему данных в компьютерной системе, либо радиозакладные устройства. Они могут перехватывать информацию, например, с клавиатуры или видеокарты, либо фиксировать аудиоинформацию (переговоры операто-

ров), а затем передавать ее по радиоканалу в пункт приема. Известны, в том числе, и радиозакладки, которые активизируют компьютерные вирусы по команде, передаваемой по радиоканалу с пульта дистанционного управления.

Кроме того, перехват аудио- и видеоинформации может осуществляться с помощью технических средств, размещенных в том же помещении, что и компьютер.

Проблеме перехвата побочных электромагнитных излучений и наводок (ПЭМИН) в современной литературе уделяется большое внимание ввиду важности этого технического канала утечки информации. Здесь же мы только отметим, что наиболее сильные электромагнитные излучения образуются от сигналов с выхода видеокарты системного блока, для которых случайной антенной служит кабель, идущий к монитору. Для перехвата этой информации достаточно иметь приемное устройство, работающее в диапазоне частот 50-500 МГц, специальный блок согласования и портативный компьютер типа Notebook. Дальность перехвата информации таким комплексом составляет 100-150 м.

9.2. Несанкционированный доступ к информации на физическом носителе

В случае доступа к физическому носителю информации выделяются следующие виды:

- доступ к среде передачи данных;
- доступ к компьютерной системе обработки данных.

Первый вид несанкционированного доступа к среде передачи подробно описан в разделе 9.3 «Перехват информации в каналах связи».

Доступ к компьютерной системе обработки данных подразумевает возможность непосредственного физического взаимодействия злоумышленника с компонентами компьютерной системы. При таком виде физического доступа у нарушителя открываются достаточно широкие возможности для несанкционированного съема информации.

Доступ к элементам, осуществляющим ввод и вывод информации из компьютерной системы, дает возможность без необходимости использования сложных методов взлома получить всю интересующую информацию. Ею будут являться данные, которые вводит легитимный пользователь в систему и выводит из нее посредством дисплея монитора, принтера либо иного устройства вывода информации. Для реализации такой угрозы безопасности нужно применять специальные технические средства, а именно средства съема данных с клавиатуры, дисплея, принтера и т.д. Такого вида устройства относят к аппаратным закладкам.

Отдельно можно выделить возможность доступа злоумышленника к данным на накопителях, либо информации, находящиеся в оперативной памяти компьютерной системы. В этом случаю нарушителю не придется преодолевать многоуровневые системы защиты информации в виде аутентификации, шифрования, систем обнаружения атак и прочих, а просто прочитать данные, находящиеся в обработке на компьютере. Для предотвращения такого рода атак нужно применять шифрование «на лету», либо жесткий физический контроль.

В крупных корпоративных сетях для хранения информации применяют системы хранения данных, обладающие определенными особенностями. Основная отличительная черта таких устройств заключается в применение специального оборудования, которое обладает некоторым количеством интерфейсов, предоставляющих доступ непосредственно к данным. Интерфейсы достаточно разнообразны: сетевое подключение по набору протоколов, оптическое подключение, использование технологии InfiniBand и др. В соответствии с выбранным способом подключения системы хранения данных к системе их обработки появляется возможность утечки информации на пути следования данных между ними. Конкретные угрозы безопасности зависят от используемого интерфейса, их рассмотрение выходит за рамки данной главы.

Особо выделяется вопрос обеспечения безопасности при помощи использования аутентификации на основе пароля. В настоящее время это наиболее распространенная практика для проверки подлинности субъекта доступа. В случае физического доступа к компьютерной системе и отчасти сетевого вопрос надежности реализации процесса аутентификации является одним из самых важных вопросов обеспечения безопасности. Методы взлома пароля можно разделить по схеме реализации на следующие типы:

- вскрытие путем прямого перебора;
- подмена пароля при работе с хранилищем паролей;
- использование уязвимостей процесса аутентификации;
- подмена программного кода, взаимодействующего с пользователем.

Нахождение пароля прямым перебором является одним из легко реализуемых способов подбора пароля. В случае использования короткого пароля время до его нахождения может исчисляться часами, поэтому применение этого способа может быть оправданным. Одной из разновидностей данного способа является подбор по «словарю». «Словарем» является перечень наиболее используемых паролей: список слов одного, либо нескольких языков и другие варианты паролей, которые часто применяются пользователями. При условии нахождения пароля в этом списке его подбор также не будет затруднителен для злоумышленника.

Так как при подборе основная проблема заключается в необходимости создания хеша введенного пароля и проверки его с хешем искомого пароля, существует еще один способ, который включает в себя наличие уже заранее подсчитанных хеше. Для нахождения пароля нужно сравнить хеш взламываемого пароля с базой уже подсчитанных хешей, что с точки зрения временных затрат гораздо быстрее чем формирование хеша в процессе взлома.

Учитывая, что система парольной защиты проверяет пароль с доверенным источником паролей, злоумышленник может направить свои атаки на это хранилище паролей. В случае автономного хранилища попытаться изменить содержащийся там пароль путем формирования нового хеша, либо вскрыть пароль, имея его хеш одним из способов указанным ранее.

В системах с централизованным хранением паролей наряду с озвученной атакой на хранилище злоумышленник может попытаться подменить сеанс связи между модулями аутентификации и хранилищем с целью замены корректного ответа на неверный пароль. Это даст возможность произвести успешную аутентификацию с неверным паролем на компьютере цели атаки.

Для реализации указанной выше атаки необходимо воспользоваться уязвимостями работы протоколов аутентификации в сети, а также недостатками алгоритмов шифрования, призванных надежно защищать передаваемые данные от раскрытия конфиденциальности и нарушения целостности. При наличии такого рода уязвимостей атаки могут иметь определенный успех.

Способ, основанный на подмене модуля системы аутентификации, позволяет получить пароль в незашифрованном виде до проведения проверки подлинности. Для этого при помощи вредоносного кода изменяется или подменяется модуль, отвечающий за аутентификацию пользователей так, чтобы он запускал форму для ввода пароля ничем не отличающуюся от настоящей. Тем самым пользователь будет введен в заблуждение и введет пароль в форму. Код злоумышленника сохранит пароль в открытом виде либо отправит его нарушителю безопасности, а затем либо сам аутентифицируется, либо запустит настоящий модуль аутентификации и пользователь повторно аутентифицируется в системе.

9.3. Перехват информации в каналах связи

Для взаимодействия между сетевыми узлами в компьютерных сетях используются различные среды передачи. Любая из них представляет интерес со стороны злоумышленника для несанкционированного съема информации.

Проводные сети передачи данных обладают очевидными особенностями, позволяющими нарушителю безопасности производить съем информации при помощи точных приборов, улавливающих побочные электромагнитные излучения, сопровождающие любую передачи по проводным сетям на основе

медного кабеля. Также злоумышленник может произвести распараллеливание проводного носителя сети связи и беспрепятственно производить получение циркулирующих потоков данных. В связи с большой протяженностью проводных сетей обеспечить должный физический контроль за каналом связи не всегда представляется возможным. Поэтому рассчитывать на какую-либо защиту от физического прослушивания нецелесообразно.

Беспроводная сеть передачи данных в силу своей спецификации распространяется без использования проводных элементов и может быть легко зарегистрирована злоумышленником на расстоянии, особенно учитывая тот факт, что зачастую зона приема беспроводной сети распространяется за пределы периметра безопасности организации. Поэтому предъявляются повышенные требования к беспроводной передаче, так как для доступа к среде не нужен ни физический доступ, ни специальные средства для съема побочного излучения.

До недавнего времени каналы передачи данных, основанные на использовании оптического сигнала как носителя информации, считались безопасными, так как считалось крайне затруднительным съем информации без нарушения целостности канала. В настоящее время есть ряд научно-практических работ по данной тематике, показывающих возможность с использованием соответствующих технических методов получения информации циркулирующей по оптическому кабелю.

Вопросы перехвата информации в каналах связи также рассмотрены в главах 6 и 7.

9.4. Использование недостатков программного кода для получения доступа к информации

Сложность программных продуктов, обеспечивающих работу компьютерных систем, постоянно растет. В этих условиях разработчики не всегда в состоянии обеспечить достаточный уровень тестирования для исправления всех ошибок программного обеспечения. В числе прочих ошибок встречаются проблемы приложения с безопасностью функционирования, которые ведут к появлению уязвимостей. Нарушители безопасности могут, воспользовавшись уязвимостью, получить несанкционированный доступ к данным. В зависимости от уязвимости способы получения доступа к информации различны. Это может быть просто недостаточно строгая проверка аутентичности пользователя при запросе определенных данных, неверная проверка подлинности и т.п.

Часть проблем с безопасностью функционирования сетевых приложений может быть связана с неверной их настройкой. Это вызвано, прежде всего тем, что сложность приложении день ото дня только растет и не всегда

квалификации обслуживающего персонала соответствует задачам, которые на него возлагаются. Выбор неверных параметров настройки специалистами отчасти ликвидируется поставщиками программного обеспечения путем установки изначальных настроек в наиболее безопасное состояние, но это не полностью решает проблемы снижении безопасности при последующем выборе неверной конфигурации.

Другим аспектом, связанным с сопровождением работы компьютерных систем, является использование программного кода не по назначению. Это неверный выбор техническим персоналом инструментов для выполнения поставленных перед ним задач, очевидно, это следствие недостаточной квалификации и малого опыта специалистов, ответственных за техническую поддержку. Для минимизации рисков неверного выбора программных продуктов полезно привлекать к решению задач как можно больше специалистов широкого профили. Также бывает полезно пользоваться услугами аудиторских организации, способных выдать экспертное заключение по используемому программному решению.

9.5. Внедрение вредоносного программного кода

Для получения несанкционированного доступа к информации злоумышленники могут задействовать вредоносный программный код. Основной метод включает в себя выполнение на атакуемой системе программного кода, спроектированного взломщиками таким образом, чтобы обеспечить доступ к информации на компьютерной системе. В соответствии со способом проникновения вредоносного кода на целевую систему можно выделить несколько вариантов распространения:

- использование уязвимостей в сетевых службах компьютерной системы;
- при помощи специальных сообщений электронной почты;
- выполнение скриптов на веб сайтах при их открытии веб браузером;
- использование флэш-накопителей из недоверенных источников с использованием функции автозапуска;
- другие способы внедрения вредоносного кода.

В службах, обеспечивающих взаимодействие по сети с другими компьютерными системами, зачастую обнаруживаются уязвимости, которые могут быть использованы злоумышленниками для проникновения в целевую систему и в дальнейшем позволяет им выполнять злонамеренных код.

При этом вредоносный код может приобретать различные виды. Детальная классификация производится антивирусными компаниями, цель которых написание программных продуктов, занимающихся активным противодействиям такого рода атакам на компьютерные системы.

Широкое распространение коммуникаций пользователей корпоративных сетей при помощи пересылки электронных сообщений обусловили привлекательность распространения вредоносного кода при помощи электронной почты. Психологический прием, основывающийся на использовании поля «От кого», где содержится имя известного пользователю человека, приводит к полному доверию к отправителю со стороны пользователя. Он, не задумываясь о последствиях, открывает письмо и вложение и тем самым неосознанно выполняет вредоносный код. Недостаток электронной почты в виде возможности подделки адреса отправителя широко используется злоумышленниками. При условии использования устаревшей версии почтового клиента иногда достаточно только открыть письмо, чтобы спровоцировать выполнения скрипта, встроенного в код письма, эксплуатирующего уязвимость почтового клиента.

Использование веб ресурсов для получения информации открыло широкие возможности распространения вредоносного кода злоумышленниками. Для этого нарушителю безопасности необходимо привлечь пользователя на инфицированную страницу, а дальше на ней выполнится на стороне компьютера-жертвы скрипт, реализующий возможность для злоумышленника манипулировать данными пользователя. Если раньше текст страницы представлял собой только ее представление на экране, то теперь это сложный механизм взаимодействия программного кода и визуального представления, причем программный код может выполняться как на стороне веб сервера, так и на стороне клиента - веб браузера. Этим и пользуются злоумышленники, изобретая все новые способы запуска вредоносного кода на компьютерной системе пользователя.

Применение флэш-накопителей все еще остается один из способов передачи информации между пользователями в компьютерных сетях. Встроенный механизм распространенных операционных систем для автоматического проигрывания содержимого и автозапуска предопределенного файла на сменных носителях вызывает запуск вредоносного кода сразу после подключения флэш-накопителя к компьютерной системе. При этом никакой интерактивности с пользователем не соблюдается - все происходит в автоматическом режиме. Таким образом, вредоносных код распространяется между компьютерными системами простым подключения съемных носителей.

К другим менее используемым видам распространения вредоносного кода можно отнести применение драйверов устройств для встраивания кода злоумышленника. После установки драйвера в операционной системе происходит запуск вредоносной программы.

Также можно отметить отдельно целый класс программ, маскирующихся под полезные программы. В реальности они являются только оболочкой,

снабженной компонентами, выполняющими вредоносные функции. Широкое распространение получили в данном направлении псевдо антивирусные программы, установка которых не несет никакой практической пользы, а за описанием скрывается программный код злоумышленника.

9.6. Принуждение к использованию небезопасных каналов передачи информации

Действия злоумышленника по получению доступа к информации, обрабатываемой средствами вычислительной техники, могут заключаться в применение методик, направленных на вынуждение передачи информации небезопасным способом. Суть метода заключается в изменение схемы взаимодействия сетевого приложения таким образом, чтобы вся передача данных производилась через сетевой узел злоумышленника. При этом всю информацию он в состоянии прочитать и при желании изменить. Для реализации такой атаки можно воспользоваться следующими недостатками работы в компьютерных сетях:

- недостатки сетевых протоколов;
- ошибки в архитектуре сетевого приложения;
- недостатки алгоритма шифрования передаваемых данных.

Многие из существующих протоколов сетевого взаимодействия не имеют функции по защите передаваемых данных от нарушения их конфиденциальности, целостности и доступности. Для проведения атак злоумышленник изучает принципы функционирования протокола, при помощи которого производится передача интересующей информации. Затем, воспользовавшись недостатками реализации протокола, производит действия злонамеренного характера. Можно выделить несколько способов использования недостатков. Первый представляет собой использование злоумышленниками ошибок в работе сетевых протоколов. Путем взаимодействия с сетевой службой можно вызвать переход сетевого протокола на работу по резервной схеме, которая, например, не обеспечивает шифрования данных, либо не производит проверку доверия к транзитным узлам и т.д. Другими словами воздействия на сетевую службу, которая ведет к использованию менее безопасного способа передачи данных. Также сюда можно отнести ошибки реализации обработки неверно сформированных пакетов данных стеком протоколов операционной системы. В этом случае возможно нарушения доступности работы службы путем вывода ее из строя.

Второй способ заключается в наличии ошибок в архитектуре приложения, к ним относится возможность изменения каких либо внешних факторов, которые находятся в ведении злоумышленника с целью перехода работы протокола в небезопасный режим. Под внешними факторами подразумевается

формирования побочного влияния путем пересылки специально сформированных пакетов. Примером может служить работа протоколов маршрутизации, которые на основе изучения ответов от соседних маршрутизаторов формируют записи о возможных путях следования трафика. Злоумышленник, подменяя ответы от маршрутизаторов, может создать такую конфигурацию сети в памяти маршрутизатора, когда весь поток данных будет передаваться через специальных узел нарушителя.

Другим примером является посылка специальных пакетов при работе протоколов, которые вынуждают либо пользоваться сервисами посредниками, которыми будут узлы злоумышленника, либо просто производить действия, приводящие к нарушению нормальной работы сетевых служб. Например, посылка сообщений о закрытие сеанса связи в протоколе TCP (пакет с установленным флагом FIN), если такой пакет будет обработан узлом-жертвой, то сеанс будет закрыт и передачу придется начинать сначала.

Еще один пример связан с работой сетевых устройств локальной сети, а именно обработка таблиц MAC адресов в коммутаторах локальной сети. Злоумышленник при помощи пересылки большего числа пакетов с различными MAC адресами переполнит таблицу соответствия сетевых интерфейсов и MAC адресов (MAC таблицу), что вызовет пересылки всех пакетов на все порты. При условии физического подключения злоумышленника к коммутатору он сможет получить все сетевые пакеты, циркулирующие через выведенный из строя коммутатор.

Ошибки в реализации алгоритмов шифрования передаваемых данных приводят к тому, что вся передаваемая информация становится доступна злоумышленнику. Время от времени появляется информация о том, что тот или иной сетевой протокол, использующий шифрование больше не является безопасным. Обычно это результат исследования специалистов по информационной безопасности на предмет корректности его использования в потенциально опасных средах передачи. Кроме того возможно появление уязвимости в сетевом протоколе при использовании его в среде передачи, для которой он изначально не проектировался.

Не так давно было продемонстрировано получение данных из шифрованного трафика беспроводной сети, использующий протокол WPA. Не исключено, что протоколы, в настоящий момент являющиеся стойкими к взлому, в скором времени будут переведены в разряд некриптостойких.

10. МЕТОДЫ И СРЕДСТВА ВЫЯВЛЕНИЯ ЗАКЛАДНЫХ УСТРОЙСТВ

10.1. Общие принципы выявления

Одним из элементов системы защиты информации является выявление возможно внедренных закладных устройств (ЗУ). Оно реализуется на основе двух групп методов (рис. 121).

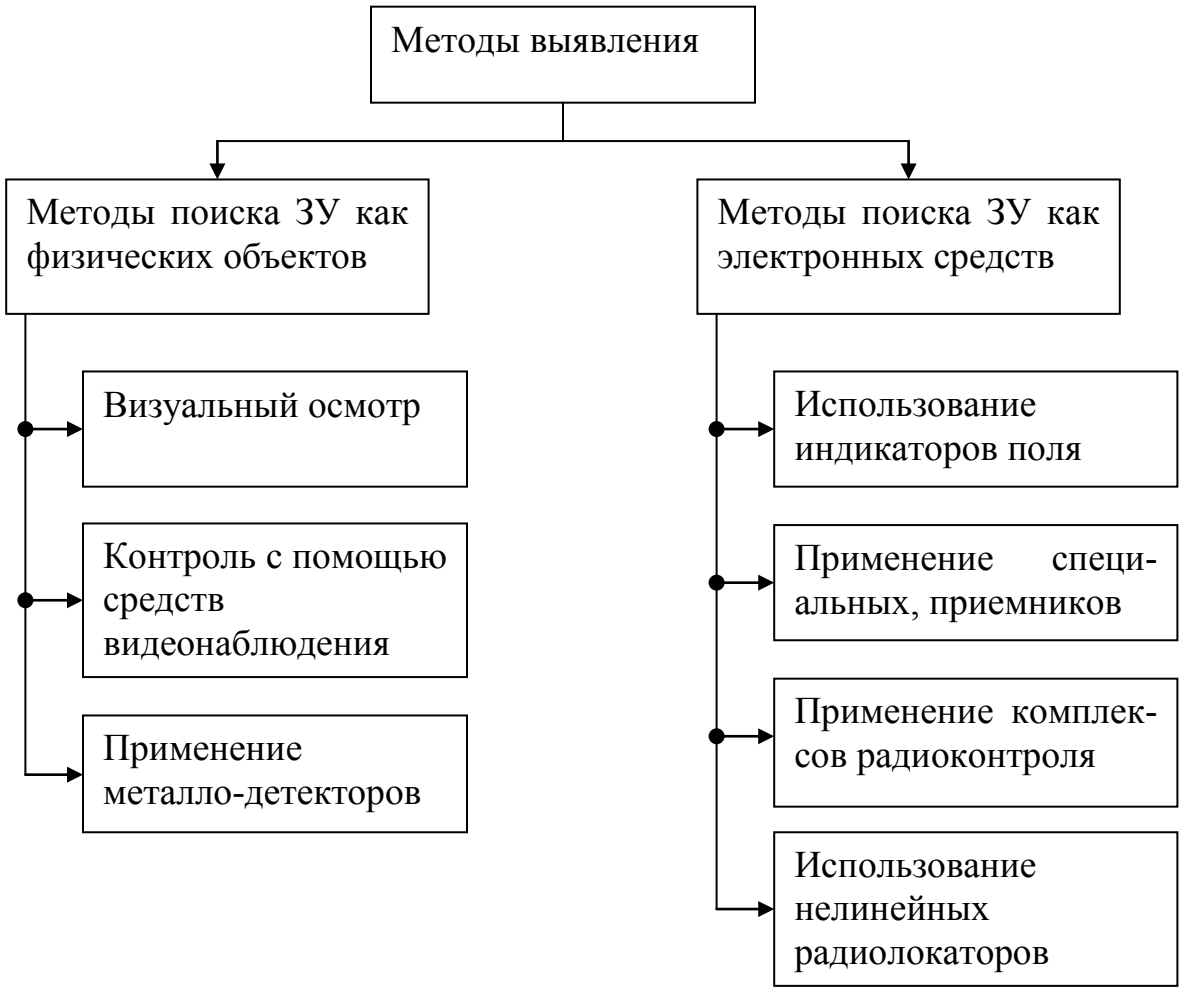

Рис. 121. Методы выявления закладных устройств

Первая группа – методы, основанные на поиске ЗУ как физических объектов с вполне определенными свойствами и массогабаритными характеристиками. К этой группе методов относятся:

- визуальный осмотр мест возможного размещения ЗУ, в том числе с применением увеличительных стекол, зеркал, средств специальной подсветки;
- контроль труднодоступных мест с помощью средств видеонаблюдения;
- применение металлодетекторов.

Вторая группа – методы, использующие свойства ЗУ как электронных систем. Она включает:

- использование индикаторов поля, реагирующих на наличие излучения радиозакладных устройств и позволяющих локализовать их месторасположение;
- применение специальных радиоприемных устройств, предназначенных для поиска сигналов по заданным характеристикам и анализа электромагнитной обстановки;
- применение комплексов радиоконтроля и выявления ЗУ;
- обследование помещений с помощью нелинейных радиолокаторов, позволяющих выявлять любые типы ЗУ.

Обнаружение ЗУ как физических объектов является наиболее общим случаем, попадающим под понятие осмотра или досмотра. Его основные методы и используемые технические средства будут рассмотрены ниже. Каждому из методов второй группы будет посвящен отдельный параграф.

10.2. Методы поиска закладных устройств как физических объектов

Визуальный осмотр

Это один из важнейших методов выявления, он не может быть заменен ни одним другим. Он предназначен для обнаружения ЗУ как в обычном исполнении, так и в закамуфлированном виде. Осуществляется периодически, а также перед проведением важных мероприятий в тех помещениях, где возможно размещение ЗУ.

При проведении визуального осмотра особое внимание обращается на изменения в интерьере, появление свежих царапин, следов подчистки или подкраски. Особенно тщательно осматриваются (с полной или частичной разборкой) сувениры, забытые посетителями личные вещи или другие «случайные» предметы. Проводится обязательный осмотр телефонных и других линий связи на участке от аппарата до распределительной коробки.

При проведении осмотра особое внимание уделяется скрытым и труднодоступным местам, так как именно они представляют наибольший интерес для лиц, устанавливающих ЗУ. Для облегчения процедуры поиска используют специальные фонари и зеркала (рис. 122, 123).

Однако такие простые приспособления не всегда удобны и эффективны, поэтому на практике, зачастую, применяют технические средства видеонаблюдения, специально приспособленные для осмотра труднодоступных мест.

Рис. 122. фонари Mag-Lite (оборудованы устройством, позволяющим изменять световой пучок от точечного до рассеянного)

Рис. 123. Зеркало, предназначенные для проведения осмотра в труднодоступных местах

Контроль с помощью средств видеонаблюдения

К современным средствам видеонаблюдения относят оптико-электронные системы, которые условно можно разбить на две группы:

- эндоскопическое оборудование;
- досмотровые портативные телевизионные или видеоустановки.

Ассортимент **эндоскопической продукции** включает в себя целую гамму волоконно-оптических фиброскопов, жестких бароскопов, а также видеоскопов, позволяющих осуществлять осмотр труднодоступных мест. Отличительной особенностью этих устройств является миниатюрный объектив, помещенный на конце тонкого гибкого рукава или жесткой трубки, которые служат и направляющим элементом, и защитной оболочкой для оптоволоконного жгута (реже многокомпонентной линзовой системы), предназначенного для передачи изображения с выхода объектива на окуляр либо ПЗС-матрицу. В некоторых типах видеоскопов ПЗС-матрица расположена непосредственно на зондирующем конце рукава или трубки. С выхода матрицы сигнал по кабелю или радиоканалу передается в блок преобразования и далее на монитор.

Гибкие *фиброскопы* предназначены для проникновения сквозь сложные изгибы различных каналов (см. рис. 124).

Рис. 124. Фиброскоп РК 1760

Бароскопы используются для осмотра узлов, к которым может быть осуществлен доступ через узкие прямолинейные каналы. В отличие от фиброскопов, вместо гибкого рукава они оборудованы жесткой штангой (рис. 125). Особенностью *видеоскопов* является то, что они позволяют в реальном масштабе времени осуществлять вывод изображения на телевизионный монитор, с одновременным фото- и (или) видеодокументированием, как, например, устройство РК 1700 (автомобильная антенна см. рис. 80). Кроме того,

видеоскопы позволяют вести наблюдение за объектами, находящимися на удалении до 22 м.

Общим недостатком эндоскопических устройств является то обстоятельство, что они скорее рассчитаны на статическое скрупулезное обследование, чем на быстрый оперативный осмотр. Кроме того, зачастую эти системы имеют многомодульную конфигурацию с кабельными соединениями, их функциональные блоки не минимизированы по весу и габаритам (PK 1765, PK 1700). Очевидны и проблемы с быстрой подготовкой к работе, переносом системы и сохранением ее целостности. Еще одна существенная особенность заключается в не всегда приемлемом качестве наблюдаемого через окуляр изображения.

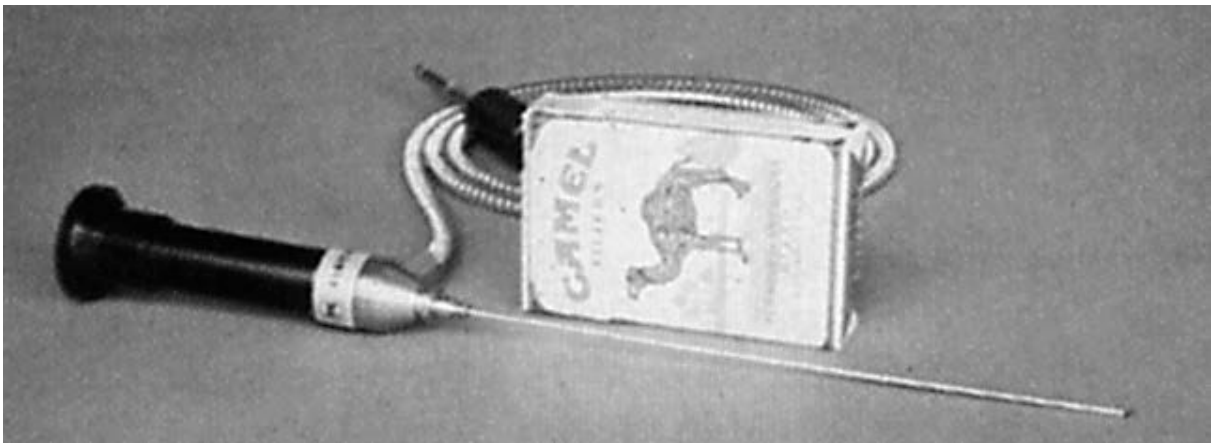

Рис. 125. Бароскоп PK 1700-S

Сравнительная оценка эндоскопических устройств различного типа показывает, что наилучшее качество изображения позволяют получать видеоскопы, кроме того, по телевизионному монитору следить за осмотром может практически неограниченное число наблюдателей. В то же время, подобное оборудование не может использоваться одним оператором, и не приспособлено для быстрой смены места осмотра и обхода объектов. Для этих целей больше подходят портативные эндоскопические устройства типа фиброскопов MP-660B, MM-013C или PK 1760.

Досмотровые портативные телевизионные системы

Досмотровые портативные телевизионные системы позволяют соединить достоинства высокого качества изображения с максимальным удобством пользования оборудованием при осмотре. Это достигается путем конструктивного объединения в едином устройстве миниатюрной телевизионной камеры, регулируемой штанги и телевизионного монитора.

Такое оборудование специально разрабатывается для нужд таможенных служб, но достаточно эффективно может быть использовано и для поиска ЗУ.

В качестве примера можно привести носимое досмотровое видеоустройство Альфа-4 (рис. 126), в комплект которого входят следующие основные компоненты:

- телескопическая штанга с черно-белой видеокамерой и источником инфракрасной подсветки, позволяющие досматривать объекты на удалении до 2,5 м;
- миниатюрный жидкокристаллический видеомонитор, размещаемый в руке оператора;
- специальный жилет, носимый поверх одежды.

Рис. 126. Поиск бамперных жучков с использованием переносимого оборудования

В жилете размещены пульт управления и индикации, миниатюрный микрофон, аккумуляторный блок питания и передатчик телевизионного сигнала с антенной. Последний используется в том случае, если необходима трансляция изображения на стационарную телевизионную станцию для более тщательного контроля и документирования.

Другим примером реализации портативной телевизионной аппаратуры досмотра может служить система S-1000 («Кальмар»), имеющая аналогичную комплектацию. Ее характерными особенностями являются следующие:

- изделие оборудовано пылевлагозащитным и ударопрочным корпусом, предохраняющим устройство от влияния окружающей среды, а герметизация камеры позволяет осуществлять осмотр даже в жидких средах;
- цилиндрический корпус камеры со встроенной инфракрасной подсветкой обеспечивает максимально возможную для этого оборудования способность проникновения в труднодоступные места;
- угловое положение камеры изменяется с помощью гибкой концевой штанги или фиксируемого шарнира;
- телевизионный сигнал и питание передаются по кабелю, пропущенному внутри телескопической штанги. Здесь же обеспечивается автоматическая подмотка избыточного кабеля на встроенный подпружиненный барабан;
- компактный монитор с электронно-лучевой трубкой крепится на штанге с помощью регулируемого кронштейна.

Применение металлодетекторов

Недостатком визуального осмотра является необходимость длительной повышенной концентрации внимания оператора, что не всегда дает надежный результат. Поэтому следующий шаг в повышении эффективности выявления ЗУ связан с объединением возможностей визуального и детекторного исследований.

Под детекторным исследованием понимается применение аппаратуры, которая контактным или бесконтактным способом воспринимает определенные физические свойства, свидетельствующие о наличии в обследуемом месте некоторых аномалий в виде неоднородностей, характерных излучений или конкретных веществ. С точки зрения эффективности обследования с применением детекторов существенно то, что они вырабатывают звуковой или световой сигнал в случае превышения заданного порога параметром, по которому осуществляется детектирование. Тем самым происходит не только выявление, но и локализация искомого устройства или предмета. *Все в дальнейшем рассматриваемые методы являются детекторными.*

Металлоискатели являются наиболее простым типом детекторов ЗУ, действующим по принципу выявления металлических предметов (элементов ЗУ) в непроводящих и слабопроводящих средах (дерево, одежда, пластмасса и т. п.). Детекторы бывают как ручного, так и арочного типа. Естественно, что для вышеопределенных целей подходят только ручные приборы. В настоящее время известны сотни модификаций металлодетекторов. Однако по принципу работы они почти не отличаются друг от друга, а их основные особенности составляют только потребительские и эксплуатационные характеристики.

Практически все современные металлоискатели предназначены для поиска предметов как из черных, так и из цветных металлов. При этом обнаружительная способность по дальности лежит в пределах от 10 до 500 мм и зависит от массы предмета. Все приборы имеют звуковую, а иногда и световую сигнализацию. Приведем следующие типы металлодетекторов:

АКА 7202М – селективный металлодетектор (см. рис. 127), предназначенный для поиска металлических предметов в диэлектрических и слабопроводящих средах. Подает различные звуковые сигналы при приближении к предметам из черных и цветных металлов. Максимальная дальность обнаружения: 80 мм – винт М3×7; 100 мм – диск 15×1 мм. Питание – «Крона» 9 В.

Рис. 127. Металлодетектор АКА 7202М

МАРС – металлодетектор (см. рис. 128), предназначенный для оперативного поиска предметов из черных и цветных металлов. Питание – «Крона» 9 В.

Рис. 128. Металлодетектор МАРС

СТЕРХ-92АР – металлодетектор (см. рис. 129), предназначенный для поиска металлических предметов в диэлектрических и слабопроводящих средах. Максимальная дальность обнаружения металлических предметов: 250 мм – диск 20×1 мм; 600 мм – пластина 100×100×1 мм. Питание – «Крона» 9 В.

Рис. 129. Металлодетектор СТЕРХ-92АР

МИНИСКАН – малогабаритный селективный металлодетектор (см. рис. 130), предназначенный для оперативного обнаружения металлических предметов. Подает различные звуковые сигналы при приближении к предметам из черных и цветных металлов. Не нуждается в предватительных настройках. Питание – «Крона» 9 В.

Рис. 130. Металлодетектор МИНИСКАН

10.3. Методы поиска ЗУ как электронных средств

В соответствии с классификацией, приведенной на рис. 109, основными способами выявления радиозакладных устройств являются: использование индикаторов поля; применение специальных приемников; применение комплексов радиоконтроля.

Все эти методы основаны на наличии у данного типа ЗУ радиоизлучений, которые кроме того, что сами по себе являются демаскирующим признаком, обладают еще и рядом характерных особенностей, позволяющих идентифицировать их именно как сигналы радиозакладок. Поэтому с точки зрения

поиска, радиозакладное устройство – очень удобный объект. Отметим эти особенности.

Основные признаки излучения радиозакладок

Первый признак – относительно высокий уровень излучения, обусловленный необходимостью передачи сигнала за пределы контролируемого помещения. Этот уровень тем выше, чем ближе к ЗУ находится аппаратура поиска.

Второй – наличие гармоник в излучении радиозакладок. Это обстоятельство является следствием необходимости минимизации размеров ЗУ, а следовательно невозможности обеспечить хорошую фильтрацию выходного излучения. В современных радиозакладках ослабление излучений на гармониках составляет всего 40–50 дБ, поэтому обнаружение этих нежелательных излучений без особых проблем возможно на удалении до 10 м, естественно, если позволяет частотный диапазон применяемого приемника контроля.

Третий – появление нового источника в обычно свободном частотном диапазоне. При этом оператор, осуществляющий радиоконтроль, должен очень хорошо ориентироваться в общей радиоэлектронной обстановке и знать, что и в каких диапазонах может работать.

Четвертый связан с использованием в ряде радиозакладок направленных антенн. Это приводит к сильной локализации излучения, то есть существенной неравномерности его уровня в пределах контролируемого объекта. На расстояниях в несколько метров этот эффект лучше всего проявляется для гармоник основного излучения.

Пятый признак связан с особенностями поляризации излучения радиозакладок. Дело в том, что при изменении пространственного положения или ориентации приемной антенны наблюдается изменение уровня всех источников. Однако однотипные удаленные источники одного диапазона ведут себя примерно одинаково, тогда как сигнал закладки изменяется отлично от остальных. На практике этот эффект наверняка замечали те, кто осуществлял поиск ЗУ с использованием анализаторов спектра.

Шестой признак заключается в изменении («размывании») спектра излучений радиомикрофонов при возникновении каких-либо шумов в контролируемом помещении. Он проявляется только в том случае, если ЗУ работает без кодирования передаваемой информации.

Седьмой признак связан со способностью человека различать акустические сигналы. Так, если закладка работает без маскирования, то оператор, осуществляющий поиск ЗУ, слышит шум помещения или тот тестовый сигнал, который сам создал. В аппаратном варианте этот эффект обыгрывается разного рода корреляторами и, так называемой, акустической завязкой. При

выявлении закладок с маскированием передаваемой информации сигнал напоминает неразборчивую речь или какофонию, если в качестве тестовых используются, соответственно, речевой сигнал или музыка. В последнем случае для аппаратного выявления необходимы специальные алгоритмы корреляции, но обычно можно обойтись и просто зондированием импульсными акустическими сигналами. Наконец, при применении кодирования, скорее всего, оператор будет слышать белый шум, и скорее всего никакая корреляция со звуком в данном случае не поможет.

Восьмой признак связан со временем работы радиозакладок. Так, самые простые из них, то есть не оборудованные схемами дистанционного включения и VOX, будут функционировать непрерывно в течение некоторого времени. Для закладок с VOX характерен прерывистый режим работы днем и практически полное молчание ночью. Устройства с дистанционным включением обязательно имеют несколько коротких сеансов в течение дня и почти наверняка будут работать во время переговоров, важных с точки зрения установившего их лица. Применительно к телефонным закладкам наличие восьмого признака проверяется очень просто: если какое-либо излучение возникает одновременно с поднятием трубки и исчезает, когда трубка положена, то это излучение прямо или косвенно связано с утечкой информации.

Вышеприведенный список признаков не является исчерпывающим и может быть существенно расширен.

Применение индикаторов (детекторов) поля

Простейшими средствами обнаружения факта использования радиозакладок являются индикаторы, или детекторы поля. Внешний вид наиболее распространенных детекторов поля приведен на рис. 131. По сути, это приемники с очень низкой чувствительностью, поэтому они обнаруживают излучения радиозакладных устройств на предельно малых расстояниях (10 – 40 см), чем и обеспечивается селекция «нелегальных» излучений на фоне мощных «разрешенных» сигналов. Важное достоинство детекторов – способность находить передающие устройства вне зависимости от применяемой в них модуляции. Основной принцип поиска состоит в выявлении абсолютного максимума уровня излучения в помещении. Хорошие индикаторы поля снабжены частотомерами, акустическими динамиками, имеют режим прослушивания и двойную индикацию уровня сигнала.

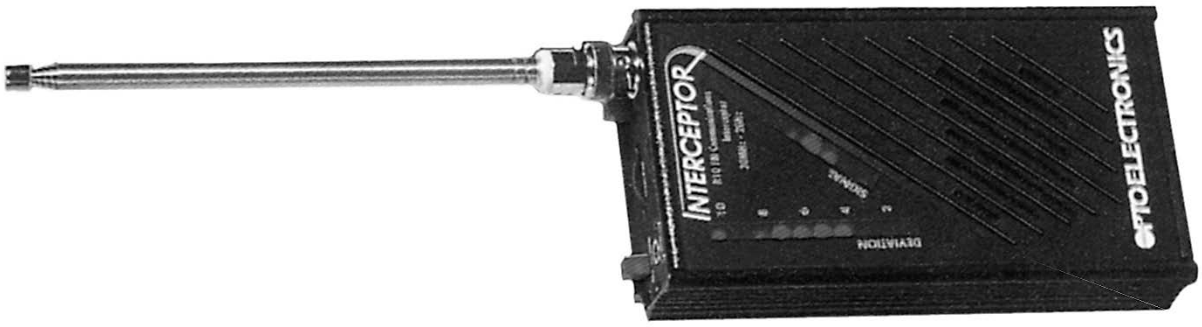

Рис. 131. Индикатор поля Interceptor R10

Иногда детекторы используют и в так называемом сторожевом режиме. В этом случае после полной проверки помещения на отсутствие ЗУ фиксируется уровень поля в некоторой точке пространства (обычно это стол руководителя или место ведения переговоров), и прибор переводится в дежурный режим. В случае включения закладки (примерно на удалении до двух метров от детектора), индикатор выдает сигнал о повышении уровня электромагнитного поля. Однако необходимо учитывать тот факт, что если будет использоваться радиозакладка с очень низким уровнем излучения, то детектор скорее всего не зафиксирует ее активизацию.

В некоторых случаях (при наличии достаточного времени) можно даже составить карту помещения, зафиксировав характерные уровни излучения в каждой точке пространства. Для достижения данной цели особенно удобны детекторы, снабженные цифровой индикацией уровня, например такие, как новая разработка фирмы Optoelectronics RF Detector или отечественный «Энтомолог-5».

Так как индикаторы поля должны реагировать на уровень электромагнитного излучения, то в них применяют амплитудные детекторы, которые дают дополнительный эффект, позволяющий прослушивать сигналы от радиозакладок с амплитудной модуляцией. Однако в ряде случаев наблюдается и детектирование излучений радиомикрофонов с частотной модуляцией. Это происходит как за счет неравномерности амплитудно-частотной характеристики индикатора, так и за счет неизбежной паразитной амплитудной модуляции, характерной для большинства закладок. Поскольку для индикатора частотная демодуляция – побочный эффект, то уровень демодулированного сигнала обычно невелик. Наличие же закладки обращает на себя внимание общим понижением уровня фона, создаваемого телевидением и вещательными станциями. Хорошие результаты по обнаружению дает также шум, возникающий при трении куска мягкого пенопласта по обследуемой поверхности.

Если индикатор снабжен частотомером, то это позволяет реализовать еще одну возможность. Дело в том, что в некоторых приборах частотомер

имеет фиксированный порог и в этом случае его срабатывание и отсчет одной и той же частоты в последовательных измерениях серьезный признак высокого уровня сигнала и, следовательно, наличия закладки. В других индикаторах частотомер работает при любом уровне сигнала и на него следует обращать внимание только тогда, когда он показывает одну и ту же частоту.

Технические характеристики индикаторов поля

Примерами индикаторов, в том числе и индикаторов-частотомеров, применяемых для обнаружения радиозакладок, могут служить следующие устройства.

Cub – прибор, предназначенный для измерения частоты радиосигналов и поиска подслушивающих устройств. Он имеет цифровой фильтр, функцию автозахвата, девятизначный дисплей. Его рабочий диапазон 1-2,8 МГц, чувствительность в зависимости от поддиапазона колеблется от 300 мкВ до 25 мВ. Период проведения измерений регулируется от 0,0001 до 0,64 с.

Optoelectronics M1 – предназначен для измерения частот радиосигналов, а также для обнаружения и локализации радиопередатчиков, работающих в двух поддиапазонах:10 Гц-50 МГц и 200 МГц - 2,8 ГГц. Чувствительность 3–50 мВ. Имеется встроенный микроконтроллер, который обеспечивает цифровую фильтрацию, цифровой автозахват, сохранение и последовательный вывод данных. Подключение к приемнику конвертора модели CX 12RS-232 позволяет протоколировать данные на персональном компьютере. Прибор имеет десятиразрядный жидкокристаллический дисплей, его габариты – 125×70×35 мм. Питание осуществляется от встроенного ni-cd аккумулятора с напряжением 9 В, которого хватает на 4–5 ч непрерывной работы.

Scout-40 – устройство, предназначенное для измерения частот радиосигналов с интервалом 10 мс, а также обнаружения и локализации радиопередатчиков в диапазоне частот 10 МГц - 1,4 ГГц. Для уменьшения ложных отсчетов изделие осуществляет цифровую фильтрацию и проверку приходящих сигналов на стабильность и когерентность. Scout позволяет запоминать до 400 различных частот, а также отмечать до 255 периодов активности на каждой из них. Встроенный интерфейс Optoscan 456 позволяет использовать частотомер для управления приемниками (ICOM R7000, R7100, R9000, AOR AR2700, AR8000 и др.). Чувствительность приемника около 1 мВ. Десятиразрядный жидкокристаллический дисплей; питание от встроенного ni-cd аккумулятора (6 В), обеспечивающего 10 ч непрерывной работы. Габариты – 94×70×30 мм.

MRA-3 – автоматический приемник ближней зоны. Предназначен для повседневного контроля радиообстановки и выявления вновь появляющихся

радиосигналов, в том числе от устройств несанкционированного съема информации с дистанционным управлением. В автоматическом режиме обеспечивает запоминание спектра сигналов с возможностью дополнения его новыми известными частотами, регистрацию и запоминание новых сигналов с выдачей сигнала тревоги. Его основные технические характеристики: диапазон рабочих частот 42-2700 МГц; виды модуляции принимаемых сигналов WFM, NFM, AM; время сканирования диапазона – 6 с; количество запоминаемых в фоновом режиме частот – 512; число новых запоминаемых новых сигналов – 16; индикация – звуковая, жидкокристаллический дисплей, светодиодная; питание от аккумулятора 9 В или сетевого адаптера. Габариты 136×49×137 мм.

ПИТОН – приемник-детектор, предназначенный для обнаружения и демодуляции частотно-модулированных сигналов, используемых в вещательных радиопередатчиках, а также поиска несанкционированных радиопередатчиков с использованием акустозавязки и индикатора уровня принимаемого сигнала. Технические характеристики прибора: диапазон частот – от 30 до 1000 МГц; чувствительность не хуже – 48 дБ относительно 1 В; время сканирования диапазона не более 2 с; задержка поиска после пропадания сигнала – не более 3 с; питание от 6 элементов по 1,5 В. Габариты – 146×70×45 мм.

R11 – тестовый приемник для работы в ближней зоне, анализирующий гармоники основных частот радиоизлучений для поиска радиозакладок. Диапазон его рабочих частот лежит в интервале от 30 МГц до 2 ГГц. Время поиска по диапазону не превышает 1 с. Чувствительность около 100 мВ.

Использование индикатора поля в качестве единственного поискового прибора весьма неудобно, так как связано с необходимостью обследования всех возможных мест размещения закладки на расстояниях не менее 10 см (при дальностях порядка 40 см вероятность пропуска закладки может составить уже десятки процентов).

Не следует особенно полагаться и на широко рекламируемую функцию акустической завязки (например, приемник **ПИТОН**). Дело в том, что этот эффект связан с необходимостью возникновения положительной обратной связи в цепи «собственный динамик с тестовым сигналом – радиомикрофон – приемник индикатора поля». А для формирования такой связи требуется выполнение определенных фазовых соотношений для звуковой волны, достаточно высокий уровень звукового сигнала и время установления не менее 1–2 с. Поэтому для гарантированного возникновения эффекта завязки на расстоянии от полуметра необходимо максимально повысить уровень звука на индикаторе и перемещать детектор в пространстве максимально медленно.

10.4. Панорамные приемники и их основные характеристики

Радиоприемные устройства, безусловно, являются более сложным и более надежным средством выявления радиозакладок, чем индикаторы поля и частотомеры. Однако для того, чтобы быть пригодными к решению задач поиска, они должны удовлетворять трем основным условиям:

- иметь возможность настройки на частоту работы устройств, скрытно передающих перехваченную информацию;
- обладать функциями выделения нужного сигнала по характерным признакам на фоне мешающих сигналов и помех;
- обладать способностью к демодуляции различных видов сигналов.

С решением *первой задачи* практически каждый многократно сталкивался, настраиваясь на свою любимую радиостанцию, правда, при этом зная ее рабочую частоту. О подслушивающем устройстве, по вполне понятным причинам, известно только то, что оно, скорее всего, работает в диапазоне 20-1500 МГц. То есть используемый приемник должен, как минимум, перекрывать весь этот частотный интервал. Однако, если посмотреть на шкалу своего домашнего тюнера и сравнить его рабочие частоты с требуемыми, то легко увидеть, что даже самые дорогие первоклассные «бытовые» системы не перекрывают и сотой доли необходимого диапазона. Следовательно, для надежного обнаружения радиозакладок нужен специальный приемник, позволяющий контролировать чрезвычайно большой набор частот, причем делать это он должен либо одновременно во всем диапазоне, либо перестраиваясь от значения к значению за предельно малый промежуток времени. Такие системы получили название *панорамных*.

Для решения *второй задачи* приемник должен иметь полосу пропускания $\Delta f_{П}$ (интервал частот в пределах которого ведется прием), приблизительно равную ширине спектра сигнала $\Delta f_{сп}$ ($\Delta f_{П} \approx \Delta f_{сп}$).

Спектр – это своеобразный частотный портрет электромагнитного излучения, который обычно представляют графически в декартовой системе координат в виде набора вертикальных составляющих. Их положение на оси ординат характеризует абсолютное значение частоты, а высота – амплитуду, значение которой определяется по оси абсцисс.

Задача приемника состоит в том, чтобы «вырезать» из всего многообразия частот интервал, соответствующий спектру принимаемого сигнала и «подавлять» все, что находится за его пределами. Качество выполнения этой операции характеризуется так называемой *избирательностью*.

Для понимания проблем, связанных с решением *третьей задачи,* следует иметь представление о том, что с физической точки зрения звук человеческой речи представляет собой акустические колебания воздуха, частота ко-

торых не превышает нескольких килогерц. Передавать их на большие расстояния невозможно, поэтому с помощью микрофонов эти колебания преобразуют в электрические, после чего применяют так называемую модуляцию. При осуществлении процесса модуляции сигнал звуковой частоты как бы совмещают с высокочастотным радиосигналом, и последний переносит полезную информацию в точку приема. Отсюда и название «несущая» для высокочастотного излучения. «Слияние» двух типов колебаний осуществляется за счет того, что по закону, диктуемому низкочастотным сигналом, меняется какой-нибудь параметр высокочастотного. Когда изменяется амплитуда, то модуляция называется амплитудной (AM), когда частота – частотной (FM) и т. д.

Указанное изменение (модуляция) приводит к тому, что передатчик излучает не одну частоту f_0 своего генератора, а целый набор, который включает в себя не только несущую, но и все частоты звукового сигнала, расположенные справа и слева от несущей в полосе $\Delta f_{сп}$. Радисты обычно называют их боковыми составляющими. Общий вид спектра амплитудно-модулированного сигнала представлен на рис. 132.

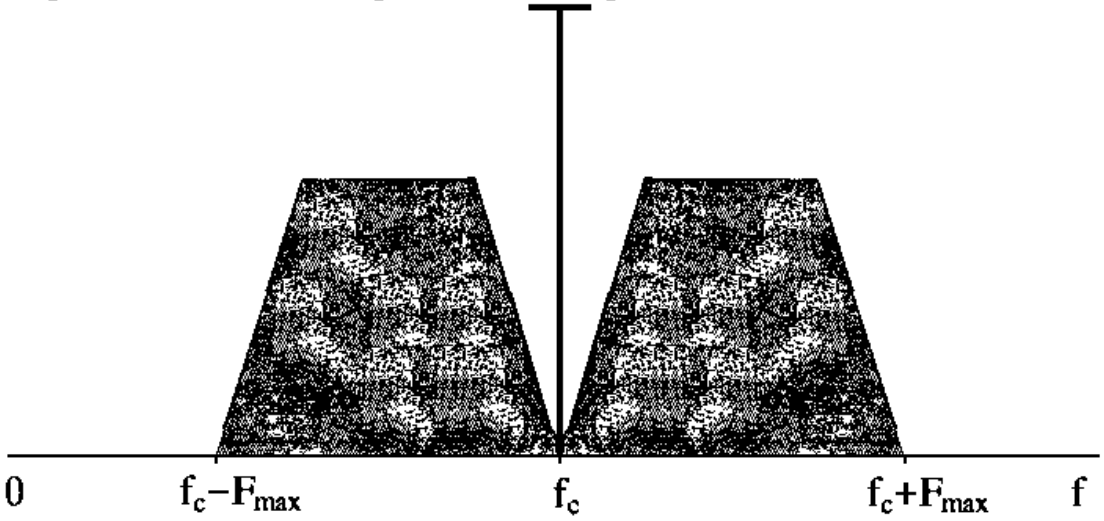

Рис. 132. Общий вид типового спектра AM-сигнала

Именно эти боковые составляющие и содержат полезную информацию. В радиоприемном устройстве избавляются от несущей, а полезный сигнал снова преобразуют в низкочастотный – его демодулируют с помощью детектора, соответствующего типу использованной модуляции. Для демодуляции AM-сигнала, в принципе, достаточно иметь только одну боковую полосу, поэтому с целью уменьшения ширины спектра $\Delta f_{сп}$ излучения передатчика иногда применяют однополосную модуляцию (SSB). В этом случае «отрезается» правая или левая боковая составляющая (см. рис. 133).

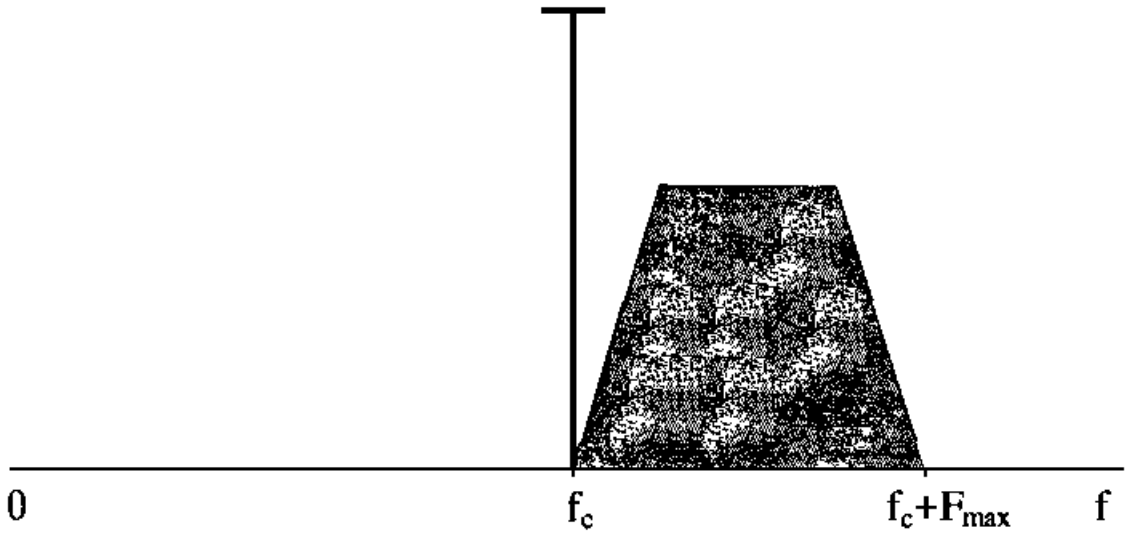

Рис. 133. Типовой спектр однополосного АМ-сигнала

В ряде случаев и несущая, не обладает никакой полезной информацией, поэтому она ослабляется или просто подавляется (см. рис. 134).

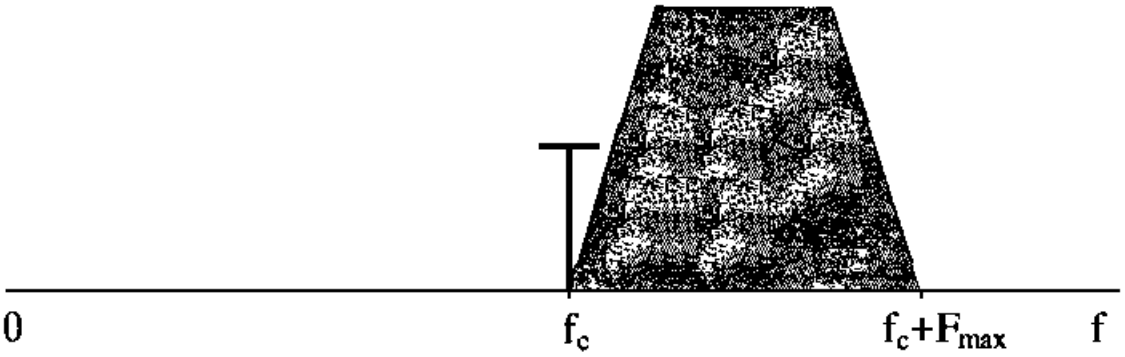

Рис. 134. Типовой спектр однополосного сигнала
с ослабленной несущей АМ-сигнала

При частотной модуляции процесс формирования спектра немного сложнее, а его вид зависит от индекса модуляции m_f – соотношения между величиной изменения частоты несущего колебания Δf_0 и максимальным значением модулирующей частоты F_{max} ($m_f = \Delta f_0 / F_{max}$). Если индекс m_f меньше единицы ($m_f < 1$), то спектр практически не отличается от спектра АМ-сигнала (см. рис. 132). При больших индексах модуляции ($m_f >> 1$) отличия становятся более существенными, но общая структура (наличие двух боковых полос) остается неизменной (рис. 135).

Рис. 135. Спектр частотно-модулированного сигнала
при большом индексе модуляции ($m_f >> 1$)

Весьма характерным является и вид спектра радиозакладных устройств, в которых применено цифровое кодирование передаваемой информации. Огибающая спектра такого высокочастотного излучения описывается функциональной зависимостью, известной как $\sin(x)/x$. Вид такого спектра на экране анализатора спектра показан на рис. 136.

Как было отмечено выше, полоса пропускания приемника должна соответствовать ширине спектра сигнала, однако она, в свою очередь, зависит от добротности системы и значения несущей частоты. На высоких частотах (100 МГц и выше) требуемую полосу сформировать практически невозможно и, поэтому применяют так называемое преобразование (уменьшение) частоты принятого сигнала с помощью специального генератора (гетеродина). Эта операция выполняется в специальном каскаде-смесителе, а уменьшенная частота называется промежуточной, ее значение, как правило, лежит в диапазоне 200-500 кГц.

Перестройка приемника в пределах заданной области частот осуществляется путем одновременного изменения параметров гетеродина и входных высокочастотных (ВЧ) фильтров. Такое техническое решение обеспечивает постоянную разность между частотами гетеродина и принимаемого сигнала, равную значению промежуточной частоты. Если диапазон перестройки невелик, то сделать такую систему не представляет особой трудности, но в панорамных приемниках – это очень сложная проблема.

Рис. 136. Спектр сигнала с цифровым кодированием передаваемой информации

Изменение частоты настройки производится путем изменения параметров элементов, входящих в состав фильтра или контура гетеродина. Эти детали так и называют «переменные», обычно это конденсаторы или их аналоги. Однако в природе нет таких радиоэлементов, которые могли бы плавно менять свою величину в очень больших пределах: теоретически можно получить отличие максимального значения от минимального в 3 или 3,5 раза, а на практике и того меньше. Поэтому наибольшая частота, на которую настроена избирательная система, тоже отличается от наименьшей не так сильно, как нам бы хотелось. Это отношение называется *коэффициентом перекрытия* и не превышает 2–2,5. Благодаря последнему обстоятельству весь диапазон рабочих частот приемника приходится разбивать на *поддиапазоны*, то есть участки, в пределах которых можно плавно изменять частоту настройки. Переход с одного поддиапазона на другой осуществляется заменой ВЧ-фильтра. В принципе, эту операцию вы многократно проделывали, переключая свой бытовой приемник, например, с СВ на УКВ, но в панорамных системах таких поддиапазонов приходиться делать более десятка и, конечно, нужны специальные алгоритмы, по которым должен вестись поиск сигнала.

Вывод – гарантированное обнаружение радиозакладок можно осуществить только при использовании специальной техники.

10.5. Принципы построения и виды панорамных приемников

Возможности панорамных приемников в значительной степени определяются методом анализа частотного диапазона. От него полностью зависит и вид структурной схемы. Различают методы параллельного и последовательного анализа.

Методы анализа частотного диапазона

При *параллельном анализе* все сигналы, находящиеся в определенной полосе частот, называемой полосой обзора, обнаруживаются одновременно. Структурная схема такого приемника приведена на рис. 137.

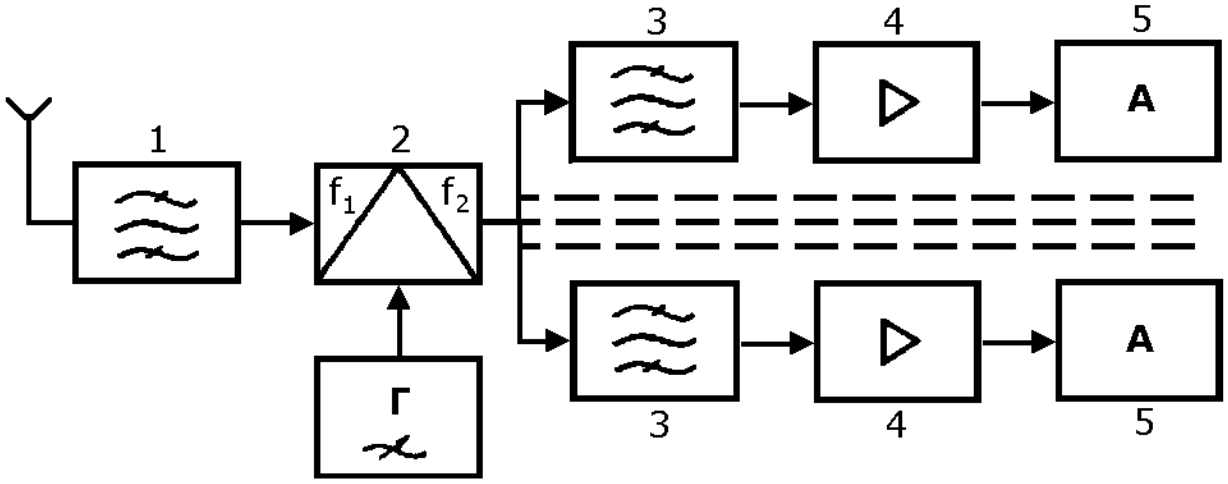

Рис. 137. Структурная схема панорамного приемного устройства с параллельным анализом сигналов

Здесь ВЧ-фильтр 1 формирует требуемую полосу обзора, в которой ведется обнаружение сигналов; смеситель 2 выполняет линейный перенос спектра принятого излучения в низкочастотную область радиодиапазона; полосовые фильтры 3 – осуществляют частотное разделение сигналов. Выходной усилитель 4 обеспечивает требуемый уровень сигнала, достаточный для нормальной работы анализирующего устройства 5.

Такая структура делает возможным практически мгновенное обнаружение сигналов в полосе обзора при условии, что их уровень превышает пороговую чувствительность приемника. Однако не сложно посчитать, что если контролируемый диапазон частот простирается хотя бы от 20 до 1500 МГц, то при ширине спектра модулированного речью сигнала 5-10 кГц потребуется от 2000 до 300 000 каналов. Ясно, что сделать такую систему, способной «брать»

любую радиозакладку, практически нереально из-за ее колоссальной сложности, а значит и стоимости.

В радиоприемнике *последовательного анализа*, соответственно, осуществляется последовательная перестройка в полосе обзора и обнаружение сигнала. Упрощенная структурная схема устройства подобного типа показана на рис. 116.

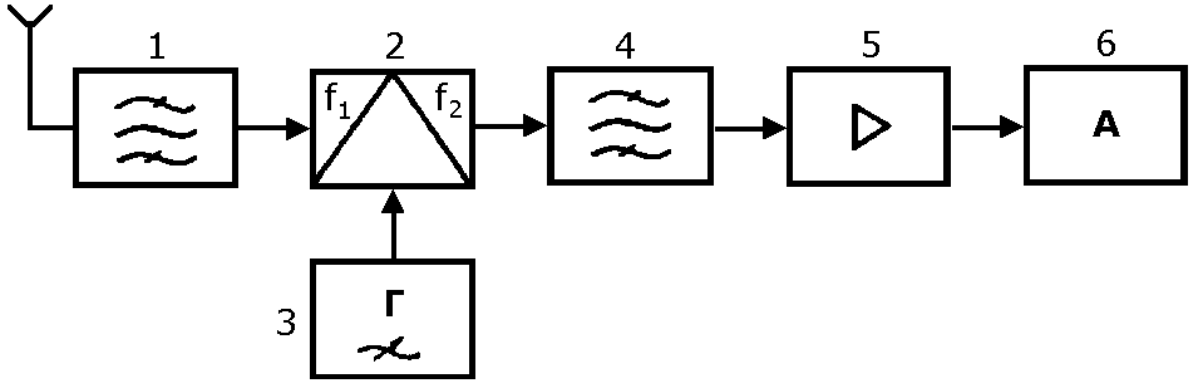

Рис. 138. Структурная схема панорамного радиоприемного устройства с последовательным анализом

Здесь ВЧ-фильтр 1 имеет полосу пропускания, равную полосе обзора, а гетеродин 3 обеспечивает перестройку приемника в заданной полосе. Промежуточная частота – фиксированная. После селекции фильтром 4 и усиления усилителем 5 обнаруженный сигнал поступает в анализирующее устройство 6. При автоматической перестройке приемник как бы «прощупывает» (сканирует) частотный диапазон, отсюда и его название – сканер. Термин не совсем точный, но широко используемый.

Этапы развития панорамных приемников

Панорамные приемники последовательного анализа в своем развитии прошли несколько этапов.

У нас в стране аппаратура *первого поколения* представляла собой *ламповые устройства* типа **Р-113, Р-250** или **Р-375**, обеспечивающие прием сигнала в определенных частотных диапазонах. В свою очередь, каждый из них имел 8-12 поддиапазонов. Проверка на наличие несанкционированных излучений сводилась к тому, что последовательно прослушивались все проверяемые частотные интервалы. Переключение с поддиапазона на поддиапазон и перестройка гетеродина осуществлялись оператором вручную. В качестве индикатора обнаружения сигнала использовались обычные наушники. Эта аппаратура имела прекрасные технические параметры (например, чувствительность не хуже 0,2-0,3 мкВ, возможность регулировки полосы пропускания и др.), но требовала высочайшей квалификации персонала и очень боль-

шого времени, необходимого для проведения полноценной проверки. Некоторые типы подобных устройств из-за их высокой надежности, а часто просто по инерции все еще используют профессионалы, но для любителей данная аппаратура не может быть рекомендована, ибо, она имеет неудовлетворительные массогабаритные характеристики.

Ко *второму поколению* приборов следует отнести популярные в 80-е годы в СССР *селективные микровольтметры* типа **SMV-6.5, SMV-8.5, STV-301, STV-401**, поставляемые ранее из ГДР. По сути они представляют собой полноценные супергетеродинные приемники с собственным генератором развертки, обеспечивающим визуальное представление зависимости уровня принимаемого сигнала от частоты в широком динамическом диапазоне. Значительное количество подобной аппаратуры на рынке и приемлемая цена ($100 - $1000) делает подобные приемники весьма привлекательными. Особенно если учесть, что высокая чувствительность (не хуже 2 мкВ) обеспечивается в широком частотном диапазоне (26-1000 МГц для **SMV-8,5**). Небольшие габариты **STV-301** и **STV-401** (360×320×130 мм), а также наличие калиброванных антенн, пробников, эквивалентов сети и встроенного никель-кадмиевого аккумулятора делает их очень удобными для мобильной эксплуатации. Однако недостаточно широкий диапазон контролируемых частот уже не отвечает современным требованиям. Поэтому для серьезной проверки данную аппаратуру применять не следует, поскольку целый ряд весьма распространенных типов «подслушек» находится за пределами возможностей этих приемников.

В конце 1992 года на отечественном рынке появилась аппаратура *третьего поколения* – сканирующие приемники, в основном японского или немецкого (ФРГ) производства. Сначала потенциальных покупателей отталкивала их достаточно высокая цена (до $2500), однако несомненные достоинства подобной аппаратуры быстро сделали ее популярной как у опытных специалистов, так и у «юниоров».

Сканирующие приемники

Сканирующие приемники можно разделить на две большие группы: носимые и возимые.

К первой группе (носимых) относятся малогабаритные приемники весом 150-300 г, выполненные в корпусе, удобном для скрытого ношения (типа сотового телефона первых моделей) и пригодные для работы в любых условиях. Они имеют автономные источники питания и свободно умещаются во внутреннем кармане пиджака. Однако, несмотря на малые размеры и вес, подобные приемники позволяют вести контроль в диапазоне частот от 100 кГц до 1300 МГц, а некоторые и до 2000 МГц (**AR-8000, HSC-050**). Они обеспе-

чивают прием сигналов с амплитудной (AM), узкополосной (NFM) и широкополосной (WFM) частотной модуляцией. Приемник **AR-8000**, кроме того, позволяет принимать сигналы с амплитудной однополосной модуляцией (SSB) как в режиме приема верхней (USB), так и нижней боковой полосы (LSB), а также телеграфных сигналов (CW). При этом чувствительность составляет, в зависимости от вида сигнала, от 0,35 до 6 мкВ. Портативные сканирующие приемники имеют от 100 до 1000 каналов памяти и обеспечивают скорость сканирования от 20 до 30 каналов за секунду при шаге перестройки от 50 Гц до 1000 кГц. Практически все они могут управляться компьютером. Характеристики некоторых переносных сканирующих приемников приведены в [88].

Возимые приемники отличаются от переносных несколько большим весом – от 1,2 до 6,8 кг, габаритами и, в некоторых случаях, имеют дополнительные возможности. Они предназначены для работы в помещениях или автомобиле. Почти все приборы этого типа имеют возможность управления с ПЭВМ. Характеристики некоторых, наиболее популярных у специалистов, перевозимых сканирующих приемников приведены в [88].

В несколько обособленный подкласс возимых приемников можно выделить сканеры, выпускаемые либо в виде специальных блоков, которые подключают к ПЭВМ, или в виде печатных плат, вставляемых непосредственно в системный блок компьютера. В качестве примера реализации подобной аппаратуры могут служить устройства **IC-PCR1000** и **Winradio**.

Приемник **IC-PCR1000** выполнен в виде отдельного блока и работает под управлением ПЭВМ через встроенный компьютерный интерфейс RS-232C. Сканер имеет шумоподавитель, функции автоматической подстройки частоты и остановки сканирования при обнаружении модулированного сигнала. В комплект входит специальное программное обеспечение для операционной системы Windows. Панель управления выводится на экран монитора (рис. 139).

Его основные технические характеристики:

- рабочий диапазон частот – 0,01 - 1300 МГц;
- виды модуляции принимаемых сигналов – USB, LSB, CW, AM, FM и WFM;
- количество каналов памяти – практически неограниченное;
- минимальное разрешение по частоте – 1 Гц;
- режим перестройки параметров приема при выборе частот – автоматический;
- размеры блока – 127×30×199 мм;
- вес – 1 кг.

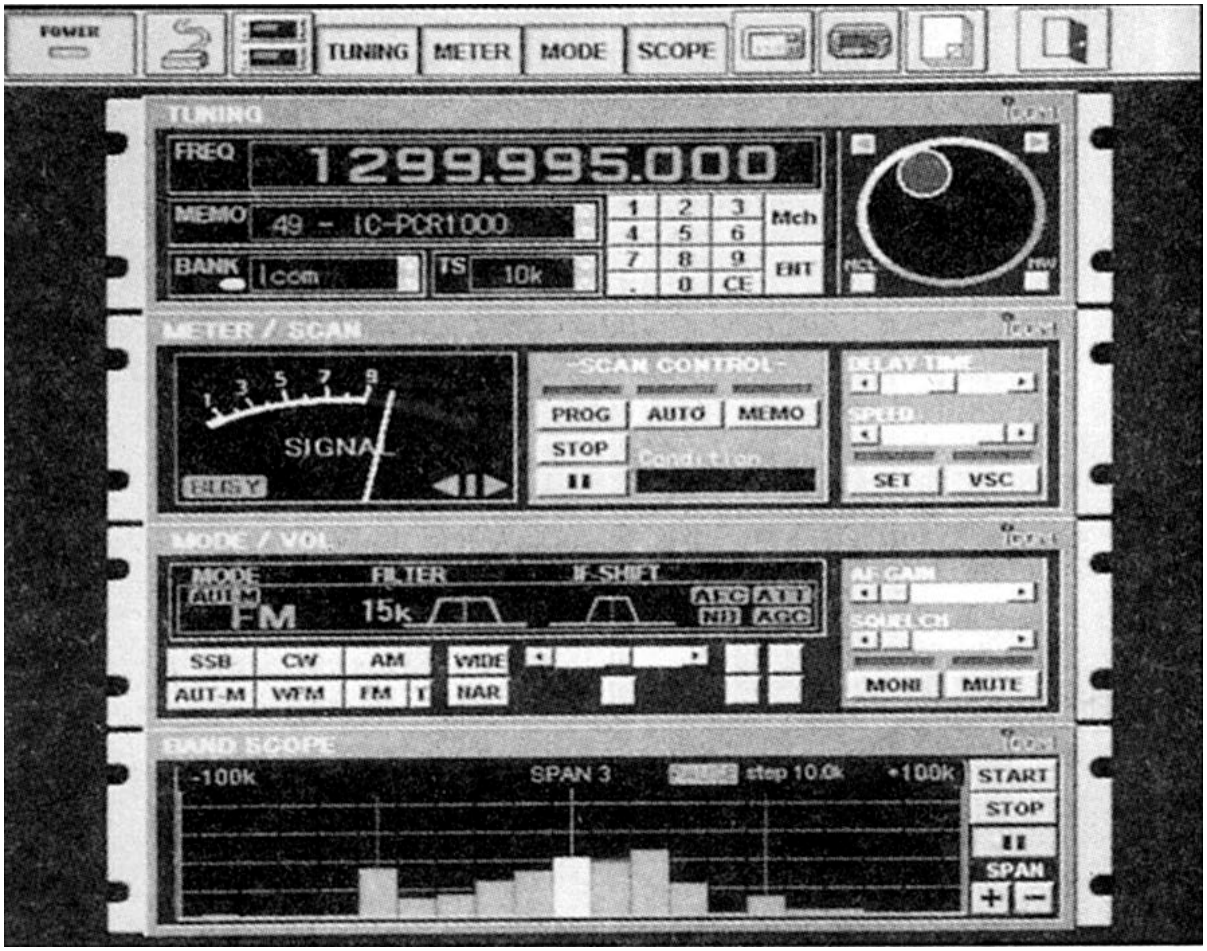

Рис. 139. Вид программной оболочки приёмника IC-PCR1000

Универсальный сканирующий приемник **Winradio** выполнен в виде печатной платы ISA IBM размером 294×121×20 мм. Он имеет режим автоматического сканирования в пределах диапазона 500 кГц-1300 МГц. Скорость сканирования 50 каналов/с. Чувствительность – 0,5 мкВ. Позволяет отображать на экране дисплея ПЭВМ спектрограммы и осциллограммы принимаемых сигналов и давать сведения об их уровне. Шаг перестройки по частоте может быть установлен в пределах от 1 кГц до 1 МГц. Панель управления также отражена на экране монитора.

Аппаратура данного типа представляет собой нечто промежуточное между обычными приемниками и специализированными автоматизированными комплексами по поиску радиозакладок, о которых будет подробно рассказано в следующем подразделе.

Обычные сканирующие приемники (как носимые, так и возимые) могут работать в одном из следующих режимов:

- автоматическое сканирование в заданном диапазоне частот;
- автоматическое сканирование по фиксированным частотам;

- ручной режим.

Первый режим работы является основным при поиске излучений радиозакладок. В этом случае устанавливаются начальная и конечная частоты сканирования, шаг перестройки и вид модуляции. Существенным преимуществом данного режима является то, что сканирование можно осуществлять с пропуском частот постоянно работающих в этом районе радиостанций (например, всех программ телевидения, городской трансляционной сети и т. д.). Они хранятся в специально выделенных для этих целей ячейках памяти. Наличие данной функции существенно сокращает время просмотра выбранного диапазона частот при поиске радиозакладок.

В зависимости от квалификации оператора можно использовать несколько режимов автоматического сканирования:

- при обнаружении любого сигнала (превышении им уровня установленного порога) сканирование прекращается и возобновляется только после подачи оператором соответствующей команды;
- при обнаружении сигнала сканирование останавливается и возобновляется после его пропадания;
- при обнаружении сигнала сканирование останавливается для принятия решения и автоматически возобновляется по истечении нескольких секунд. В ряде моделей этот интервал регулируемый, например, для приемника **AR-3000A** время паузы может изменяться от 1 до 9 с.

Второй режим используется для ведения радиоразведки, когда известны и записаны в каналы памяти возможные частоты работы радиосредств. Думаем, не надо быть специалистом, чтобы догадаться, что именно этот режим применяют в случае, когда панорамный приемник используется для приема сигнала от своей радиозакладки.

Третий режим работы применяется для детального обследования всего или отдельных участков частотного диапазона и отличается от первого тем, что перестройка приемника осуществляется оператором с помощью ручки изменения частоты, при этом информация о частоте настройки, виде модуляции, уровне входного сигнала и т. д. выводится на встроенный дисплей. Основным недостатком данного режима является очень малая скорость просмотра диапазона и, как следствие, возможность пропуска сигнала.

Перестройка по частоте в любом из перечисленных режимов идет с постоянным, заранее выбранным шагом. При поиске закладки этот шаг должен быть соизмерим с шириной спектра искомого сигнала. Кроме того, поиск должен осуществляться отдельно для каждого вида возможной модуляции сигнала.

У ряда приемников на дисплее, кроме информации о частоте настройки и виде модуляции, отображается уровень принимаемого сигнала. В частно-

сти, у приемника **AR-3000A** уровень входного сигнала отображается в виде 9-сегментной диаграммы (как на аквалайзере музыкального центра). При этом первый сегмент примерно соответствует уровню 10 мкВ, седьмой – 30 мкВ, а девятый – 300 мкВ. Более детально проанализировать сигнал можно с помощью специальной панорамной приставки, например, **SDU-5000.**

Для придания большей практической направленности сведениям, полученным из этого краткого обзора, рассмотрим более подробно некоторые, на наш взгляд, наиболее распространенные модели панорамных приемников.

Модели панорамных приемников

Возимый приемник AR-3000A. Заслуженной популярностью на рынке спецтехники пользуется приемник **AR-3000A** японской фирмы A.O.R Ltd, который отлично зарекомендовал себя в условиях России. Стоимость его довольно высока – $1200-$1500, но на «вторичном рынке» она существенно ниже, поскольку прибор завезен к нам в большом количестве. Внешний вид прибора можно видеть на рис. 140.

Рис. 140. Панорамный приемник AR-3000A

Это удобный приемник, имеющий достаточно широкие возможности. Он может работать как от сети 220 В, так и от бортовой сети автомобиля, для чего в комплект входит разъем подключения к гнезду «прикуривателя» – AR-3000A специально создавался в расчете на установку в салоне машины. Имея такой мобильный пункт радиоконтроля, можно решать задачи самого широкого круга в том числе и за пределами своего офиса. Диапазон приемника ох-

ватывает широкий спектр радиоволн – от 100 кГц до 2036 МГц. На момент создания это был самый широкодиапазонный малогабаритный сканер в мире.

Весь диапазон разбит на 13 поддиапазонов с помощью набора активных фильтров. Первый фильтр «вырезает» полосу частот от 100 до 500 кГц, а последний, тринадцатый, – от 940 до 2036 МГц. Эти фильтры – подлинная изюминка всех видов радиоаппаратуры указанной фирмы. Благодаря их отменным характеристикам они не только обеспечивают надежное подавление зеркального канала, но и используются в роли усилителя высокой частоты, что позволяет достичь очень высокой чувствительности (0,1 мкВ в режиме АМ).

Фильтры объединены в 3 блока, с каждого из которых сигнал поступает на свой смеситель, а затем через переключатель на линейку преобразователей частоты. Встроенный синтезатор обеспечивает необходимый набор частот гетеродина и их перестройку в заданных пределах. Управление всеми операциями осуществляет микропроцессор типа UNIT.

Сигнал промежуточной частоты усиливается в усилителе, выполненном на транзисторах 2SC2759, и направляется в блок детекторов. Детекторы различных видов сигналов (AM, FM, USB и т. д.) включены параллельно, но к выходному устройству подключаются поочередно в зависимости от желания оператора. К приемнику можно присоединить головные телефоны и записывающее устройство.

Достоинством приемника является наличие жидкокристаллического дисплея с подсветкой, часов, внутренних аккумуляторов для питания памяти, стандартного разъема для подсоединения к компьютеру. На рис. 140 приемник изображен с простейшей штыревой телескопической антенной, однако имеется возможность работать с антеннами различного типа и назначения. Для поиска радиозакладок наиболее эффективна всеволновая и всенаправленная антенна типа АН-7000. Ее внешний вид приведен на рис. 140.

Имеется возможность подключения приемника к персональному компьютеру типа IBM PC, что раскрывает перед пользователем самые широкие перспективы применения **AR-3000A** в составе различных программно-аппаратных комплексов.

Приемник достаточно прост в обращении, а если купить его в солидной организации, то в качестве приложения обязательно будет подробная инструкция по эксплуатации на русском языке, которая позволит быстро освоить основные приемы работы. В общем, приобретение этого прибора – неплохое начало в техническом оснащении любой службы безопасности.

Носимый сканирующий приемник IC-R10. На рынке спецтехники известна модель **IC-R1 (**фирма ICOM**)**, которую специалисты высоко ценят за качество и малые габариты. Модель – **IC-R10**, существенно расширяет ос-

новные функции прототипа. Внешний вид приемника представлен на рис. 142.

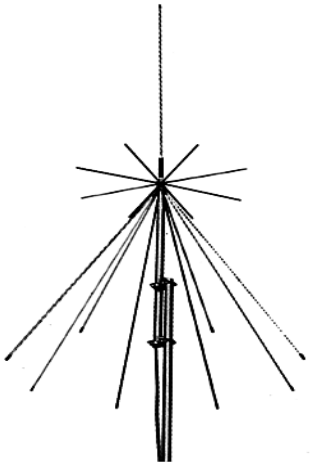

Рис. 141. Антенна АН-7000

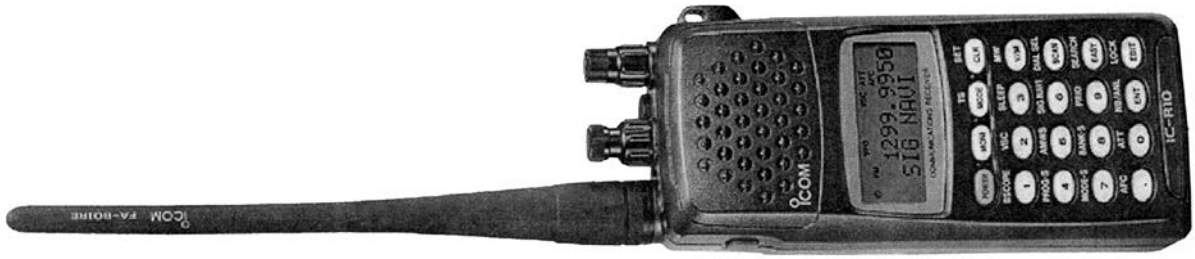

Рис. 142. Носимый сканирующий приемник IC-R10

Рабочий диапазон частот у этого приёмника несколько меньше, чем у **AR-3000A** – от 0,5 до 1300 МГц, но вполне достаточен для обнаружения всех видов радиозакладок. Он разбит на 8 поддиапазонов. На верхней границе диапазона предусмотрено трехкратное преобразование частоты (промежуточные частоты составляют: 1-я – 266 МГц, 2-я – 10,7 МГц, 3-я – 0,455 МГц). Блок детекторов обеспечивает прием сигналов практически со всеми видами модуляции. Высококачественный усилитель позволяет получать очень хорошую для такого класса портативных приемников чувствительность – 1-2 мкВ при модуляции АМ. Для удобства в работе расширен набор вариантов ведения сканирования, каждый из двух основных видов (программируемое и по ячейкам памяти) разбит на типы: сплошное, диапазонное, с автоматической записью обнаруженных частот, по ячейкам памяти и видам модуляции.

Впервые в портативных сканерах реализована система VSC (Voice Scan Control) – интеллектуальное устройство «поиска голоса», наличие которой позволяет игнорировать все немодулированные и шумоподобные сигналы. Этот режим чрезвычайно удобен при ведении оперативного радиоконтроля, например, по ходу совещания или переговоров. Если за несколько минут до начала мероприятия «пройти» весь диапазон и исключить из поиска частоты

постоянно работающих станций, то сканер подаст сигнал тревоги (притом довольно быстро) только при появлении нового сигнала того же вида, что излучает радиозакладка, но не среагирует на излучение от включившегося факса или вдруг «заискрившей» электророзетки. Большим преимуществом для осуществления такого рода деятельности являются малые размеры и вес.

Значительно сократит время, необходимое для просмотра всего частотного диапазона, наличие еще одной новой функции – «SIGNAVI» («навигатор сигналов»), которая позволяет в несколько раз увеличить реальную скорость сканирования. В этом случае используется дополнительный приемный контур, который продолжает просмотр диапазона в то время, пока вы остановились на сигнале, обнаруженном основным приемником, и пытаетесь выяснить его происхождение. Таким образом, приемник будет сканировать как бы скачками только по «занятым» каналам. Правда, величина скачка не сможет превысить 100 кГц.

Впервые на портативном приемнике имеется спектроскоп, работающий в реальном масштабе времени, что позволяет постоянно контролировать наличие сигналов в полосе частот шириной до 200 кГц (с шагом 20 кГц). Приемник может быть подключен к компьютеру и управляться им. Обмен данными происходит в формате CI-V через дополнительный блок-интерфейс CT-17. Для подсоединения последнего предусмотрено специальное гнездо. Питание осуществляется от четырех элементов типа AA или никель-кадмиевого аккумулятора. Размеры (без антенны) – 58,5×130×31 мм, вес – 310 г. Цена – до $600.

Внешний вид радиоприемных устройств фирмы ICOM приведен на рис. 143 и 144.

Эти приемники относятся к так называемым приемникам среднего класса – весьма эффективным, но относительно недорогим и не слишком «навороченным». Основные характеристики приёмников среднего класса приведены в табл. 24.

Рис. 143. Возимый сканирующий приемник IC-R100 фирмы ICOM

Рис. 144. Возимый сканирующий приемник IC-R9000 фирмы ICOM

Таблица 24.

Наименование характеристик	Приёмник			
	ICRIOO	AR3000A	1C R8500	AR5000
Фирма-изготовитель	ICOM	AOR	ICOM	AOR
Диапазон частот, МГц	0,1-1300	0,1-2036	0,1-2000	0,01-2600
Виды модуляции	AM, NFM, WFM	AM, NFM, WFM, LSB, USB, CW	AM, FM, NFM, WFM, LSB, USB, CW, AM-N	AM, FM, LSM, USB, CW
Чувствительность при отношении сигнал/шум 10дБ, мкВ	AM: 0,6-3,2 NFM 0,2-0,56 WFM 0,6-1,5	AM: 0,1-3,2, NFM: 0,35-1,5 WFM: 1,0-6,0 LSB: 0,25-1,0	AM: 2,5-6,3 NFM: 0,5 WFM: 1,4-2,0 USB: 0,25 1,0	AM: 0,36-0,56 FM: 0,2-1,25 SSB: 0,14-0,25
Избирательность на уровне 6 дБ, кГц	AM: 6, NFM: 15, WFM: 150	AM, NFM: 12 WFM: 180, LSB, USB: 2,4	AM: 5,5 FM: 12 WFM: 150	3, 6, 15, 40, 110, 220
Шаг перестройки, кГц	1, 5, 8, 9, 10, 12,5, 20, 25, 100, 1000	Кратный 50Гц	0,01, 0,05, 0,1, 1, 2,5, 5, 10, 12,5, 20, 25, 100, 1000	Or 1 Гц до 1 МГц
Число каналов памяти	21	По 100 (в 4 банках)	1000	1000
Питание, В	Внешнее	Внешнее	Внешнее	Внешнее
Размеры, мм	150×50×181	130×80×200	287×112×309	204×77×240
Масса, кг	1,4	1,2	7,0	3,5

Скорость сканирования, канал/с	20	30 (50)	40	50
Выходное устройство	Головные телефоны	Головные телефоны, ПЭВМ	Головные телефоны, магнитофон, ПЭВМ	Головные телефоны, ПЭВМ

Для богатых клиентов больший интерес может вызвать аппаратура немецкой фирмы «Роде и Шварц», которая стоит очень дорого, но позволяет не только фиксировать факт наличия в помещении подслушивающего устройства, но и приблизительно определять его местоположение. Ясно, что информация такого рода – неоценимое подспорье для поиска закладок с помощью, например, индикатора поля или нелинейного локатора. По своим возможностям лучшие приемники этой фирмы сопоставимы с автоматизированными комплексами.

В качестве примера приведем данные приемников типа **ESP**, которые перекрывают очень широкий частотный диапазон (**ESP-T1** – от 10 кГц до 1300 МГц, а **ESP-T2** – до 2300 МГц). Они имеют память на 1000 каналов, чувствительность – до 3 мкВ, шаг перестройки – 1, 7, 5, 25, 100 кГц или 2 МГц. Приемники способны разделить сигналы, отстоящие друг от друга всего на 100 Гц, и работать с любыми видами модуляции. Производится автоматическое распознавание принимаемого сигнала, а при наличии калиброванной антенны – и определение расстояния до его источника. В этом случае в помещении устанавливаются дополнительные эталонные генераторы – «скауты», которые входят в комплект. Внешний вид прибора представлен на рис. 145.

Рис. 145. Автоматический приемник ESP с генраторами

Фирма «Роде и Шварц» выпускает и относительно простую миниатюрную аппаратуру контроля, например приемник **EB100**. Устройство работает в диапазоне 20-1000 МГц, который, в свою очередь, разбит активными фильтрами на 5 поддиапазонов (первый от 20 до 108, последний – от 500 до 1000 МГц). Имеются все основные режимы сканирования с шагом от 1 кГц до 10 Мгц, принимаются сигналы с модуляцией AM, FM. Полоса пропускания – 7,5-150 кГц. Питание – комбинированное, от батареи 6 В или от сети 220 В.

Если вместе с приемником **EB100** использовать активную остронаправленную антенну HE 100, специально созданную для поиска в помещениях радиозакладок, то можно с неплохой точностью определять и местоположение источника излучения. Антенна представляет собой три сменных модуля (см. рис. 146) и работает в диапазоне 20-1000 Мгц. Первый модуль перекрывает диапазон от 20 до 200 МГц, третий – от 500 до 1000 МГц.

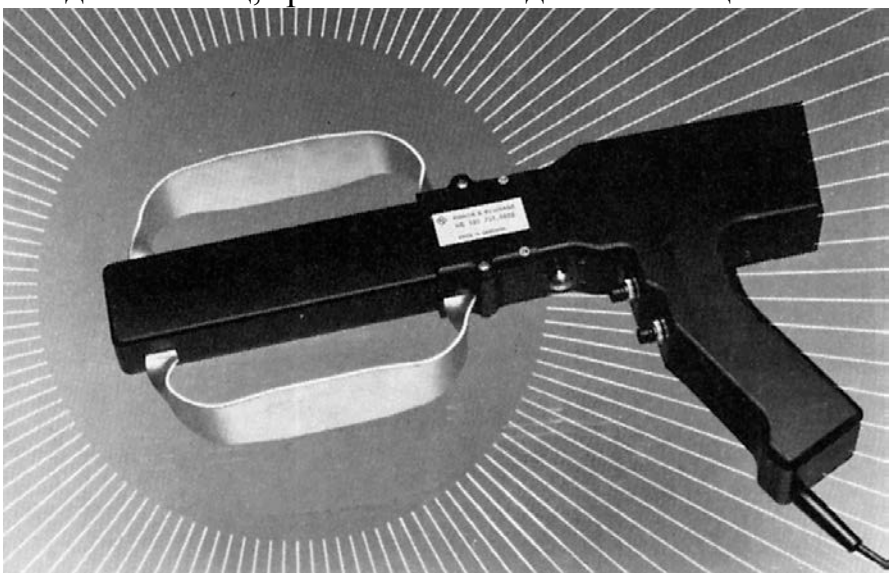

Рис. 146. Модуль антенны HE 100

Анализаторы спектра

Среди радиоприемных устройств следует выделить анализаторы спектра, которые позволяют получать частотный портрет сигнала за счет того, что принятый сигнал как бы последовательно просматривается специальным узкополосным фильтром, выводя данные на экран устройства. Развертка синхронизирована с перестройкой фильтра, поэтому на изображении с определенным шагом видны составляющие спектра сигнала, амплитуды которых определяются величиной сигнала на той или иной частоте. Ясность и полнота картинки зависят от шага перестройки фильтра и полосы обзора. На рис. 147 приведен спектр амплитудно-модулированного сигнала, полученный с помощью анализатора спектра **AX700E** при трех различных полосах обзора.

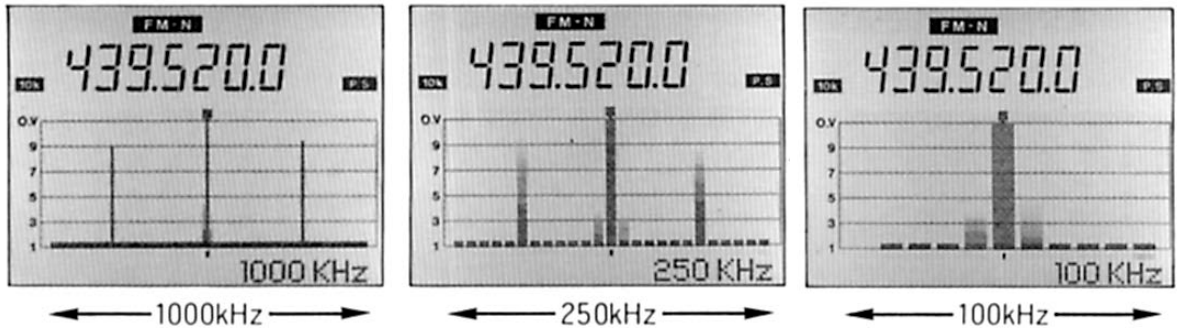

Рис. 147. Работа анализатора спектра AX700E

Анализаторы спектра незаменимы в качестве аппаратуры контроля, особенно если априорно не известны такие параметры сигнала, как частота, вид модуляции, способ кодирования и т. д. Например, прибор **EZM** («Роде и Шварц») позволяет анализировать сигналы в диапазоне от 9 кГц до 1300 МГц и устанавливать полосу обзора от 1 кГц до 2 МГц. Он совместим с **ЭВМ** и оснащен собственным 9-дюймовым монитором. У изделия **AX700E** данные несколько скромнее: диапазон частот 50-905 МГц, и цена почти на порядок меньше.

На базе анализаторов спектра фирма «Роде и Шварц» создала целые комплексы контроля, например FSAC (см. внешний вид на рис. 148).

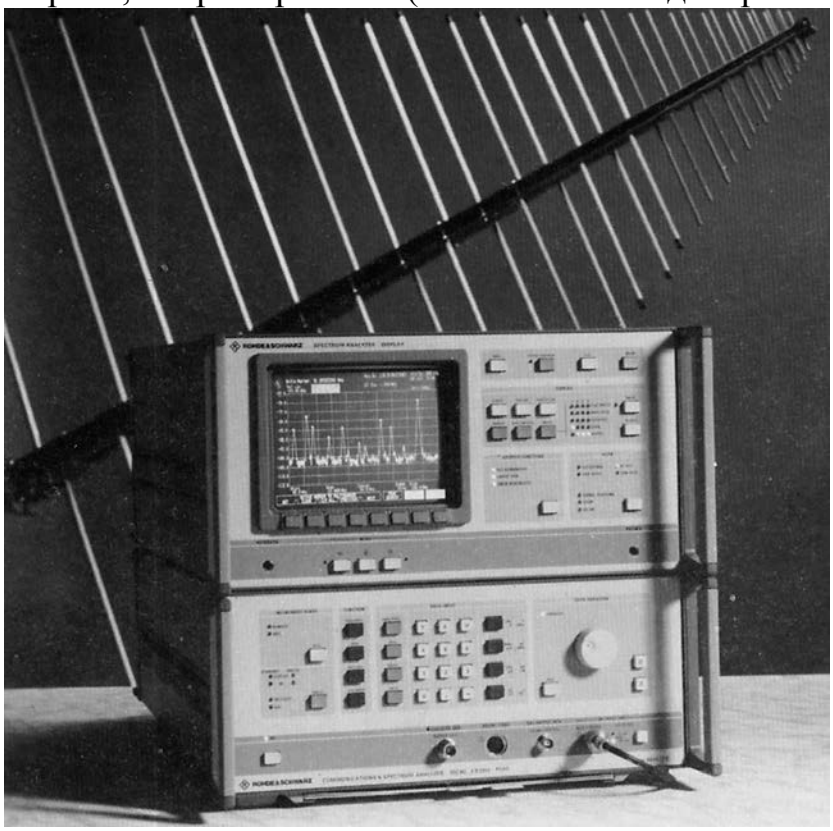

Рис. 148. Комплекс контроля FSAC

Эта аппаратура обладает высокой чувствительностью, позволяет контролировать диапазон частот 100 Гц-2000 МГц и анализировать сигналы как с амплитудной, так и фазовой модуляцией.

Наряду с вышеперечисленными в России в настоящее время широко используются и анализаторы спектра отечественного производства: СК-61, С4-42, СК4-59, С4-27, СК4-83, С4-9, СК4-84, С4-49, С4-60 и др.

Они значительно дешевле иностранных образцов и по своим техническим характеристикам вполне соответствуют решению задач ведения радиоконтроля. Основной их недостаток заключается в крайне низкой надежности, больших габаритах и весе.

10.6. Компьютерные программы для управления панорамными приемниками

Функциональное совмещение специальных приемников с персональными компьютерами существенно повышает надежность и оперативность поиска ЗУ, делает процедуру выявления более удобной (технологичной). На компьютер при этом возлагается решение следующих задач:

- хранение априорной информации о радиоэлектронных средствах, работающих в контролируемой области пространства и выбранных диапазонах частот;
- получение программными методами временных и частотных характеристик принимаемых сигналов (вместо использования достаточно громоздких осциллографов и анализаторов спектра);
- тестирование принимаемых сигналов по совокупности признаков на принадлежность к излучению ЗУ.

На российском рынке известно большое количество программ, специально разработанных для ведения поискового радиомониторинга. Наиболее известные среди них – это **«СканАР», Sedif**, **Filin**, **RSPlus**, **«Крот-mini», Arcon, Radio-Search**, а также некоторые другие.

Программа «СканАР»

Характерным представителем семейства программных продуктов, реализующих вышеуказанные свойства, является программа «СканАР», ее базовая версия имеет четыре основных режима работы:

- «Панорама» – для анализа загруженности контролируемого диапазона частот, сохранения полученной информации в архиве, сравнения результатов контроля, управления принтером для документирования полученных результатов;
- «Поиск» – для наблюдения за изменением уровней сигналов в нескольких частотных диапазонах;

- «Обзор» – для анализа наличия сигналов, превышающих заданный порог в широком диапазоне частот, а также просмотра наличия сигналов и их спектров на выбранных частотах;
- «Сканирование» – для слежения за состоянием каналов выбранного банка памяти (аналогичен режиму сканирования банков памяти в приемнике).

При переходе из режима в режим программа сохраняет все накопленные данные и предоставляет возможность продолжить работу с места остановки или сначала. При остановке работы любого режима программа осуществляет прием сигнала на фиксированной частоте с выбранными параметрами. При этом возможна ручная перестройка приемника, изменение вида модуляции принимаемого сигнала, включение – выключение звука, изменение значения аттенюатора и т. д. Рассмотрим подробно каждый из перечисленных режимов.

Режим «Панорама». Программа выполняет перестройку приемника в пределах заданной полосы обзора относительно выбранной центральной частоты и представляет результат в виде зависимости «уровень – частота». Горизонтальная полоса на изображении показывает выбранный порог. В рассматриваемом режиме программой предусмотрены три подрежима работы: «Сигнал»; «Спектр»; «Сравнение панорам».

Подрежим «Сигнал» предназначен для наблюдения за изменением уровня сигнала на фиксированной частоте.

Подрежим «Спектр» предназначен для подробного анализа спектральных характеристик выбранного сигнала. При этом предусмотрена возможность изменения ширины области просматриваемых частот и ее положения на оси частот.

Подрежим «Сравнение панорам» предназначен для сравнения двух панорам – эталонной и текущей. Эталонная хранится в памяти компьютера с запоминанием всех имеющихся установок (центральной частоты, полосы обзора, шага перестройки, полосы пропускания, вида детектора, значения аттенюатора, порогового уровня), текущая формируется при сканировании того же частотного диапазона.

Например, если в архиве была сохранена определенная панорама, то при загрузке ее из памяти и нажатии клавиши **«F5»** она определяется как эталонная. При этом панорама окрашивается в темно-серый цвет. Запустив «СканАР» на выполнение, получают вторую (результирующую) панораму, имеющую уже три цвета: светло-серый – для участков спектра, на которых значения частот и уровней обоих панорам совпадают; темно-серый – для участков, на которых сигнал пропал, белый – появился новый.

Чтобы извлечь панораму из архива, необходимо нажать клавишу **«F3»** и в появившемся списке выбрать требуемую клавишей **«Ok».** В противном случае нажать клавишу **«Отменить».**

Режим «Поиск» предназначен для наблюдения за изменением уровня сигнала в нескольких частотных диапазонах. Причем для каждого из них задаются свои параметры работы (шаг перестройки, вид модуляции принимаемого сигнала, значение аттенюатора и порогового уровня). Всего в программе предусмотрена возможность задания до 20 частотных диапазонов (в новой версии программы – до 120).

Для запуска «СканАРа» в режиме «Поиск» создается программа исполнения, которая может состоять из нескольких заданий. Создание задания подразумевает ввод значений левой и правой границ частотного диапазона и вышеперечисленных параметров – шага перестройки приемника, типа детектора, положения аттенюатора и величины порога.

Для создания программы служит таблица, появляющаяся после нажатия на кнопку **«Поиск»**. Каждая строка таблицы является элементом программы и может быть включена в программу по желанию пользователя.

Первый столбец таблицы показывает номер задания и предназначен для отметки тех из них, которые будут включены в программу. Перемещение по столбцу осуществляется стрелками, а включение задания в программу – нажатием клавиш **«Пробел»,** или **«Insert».** Для исключения из программы – повторным нажатием тех же «**Пробел»,** или **«Insert».** Во второй колонке указывается комментарий для каждого задания. Он не влияет на работу программы и служит лишь для облегчения работы пользователя. Третий столбец предназначен для выбора вида модуляции анализируемых сигналов в каждом задании. Для выбора детектора используются клавиши **«Пробел»,** или **«Insert»**, при этом появляется линейка с возможными вариантами. Нужный из них выбирается с помощью «горячей» клавиши и кнопки **«Enter».**

Колонки «$\mathbf{F_{мин}}$» и «$\mathbf{F_{макс}}$» предназначены для задания значений частот левой и правой границ диапазона. Для изменения значения используются те же «**Пробел»,** или **«Insert»**, ввод нового значения осуществляется клавишей **«Enter».**

Кроме того, в каждом задании устанавливаются значение порога и положение аттенюатора, а шаг перестройки вычисляется автоматически в зависимости от заданных значений граничных частот диапазона.

Переход к выполнению программы происходит после нажатия клавиши **«Enter»,** или кнопки **«Ok»**. Для выхода без сохранения изменений в программе и возврата в режим «Панорама» предназначена клавиша **«Отменить»**.

В режиме «Поиск» программа выводит окно, аналогичное окну режима «Панорама», но с выключенными кнопками изменения частоты, шага и порога.

После запуска программа сначала отработает первое задание, то есть пройдет первый заданный диапазон с определенным шагом и порогом, затем второе и т. д. После выполнения последнего задания программа снова перейдет к первому.

Режим «Обзор» предназначен для анализа широкого диапазона частот с отображением в виде зеленых точек сигналов, превышающих заданный порог.

В данном случае также предусмотрена возможность просмотра сигнала и спектра на интересующей частоте, сохранение полученной информации в архиве, вывод на принтер.

В случае остановки сканирования прием сигнала будет осуществляться на текущей, фиксированной частоте. При этом в окне «частота и уровень» отображаются значения, соответствующие положению курсора мыши или белого перекрестия, причем эти значения выводятся красным цветом, если уровень сигнала превышает установленный порог, зеленым – если нет.

При нажатии на кнопку «Продолжить» сканирование будет продолжаться с текущей частоты, а при нажатии кнопки «Сначала» сканирование начнется с начальной частоты диапазона.

При работе в режиме «Обзор» может возникнуть необходимость подробно просмотреть ряд сигналов, для этого используются подрежимы « Спектр», «Сигнал» или «Панорама Обзора». Полученные данные, как и в режиме «Панорама», могут быть сохранены в архиве на жестком диске. Для извлечения данных из архива используется клавиша **«F3».**

Режим «Сканирование» предназначен для слежения за состоянием каналов выбранного банка памяти (аналогичен режиму сканирования банков памяти в приемнике). Результат сканирования отображается в виде зависимости «время–уровень» для каждой из 20 частот текущего банка. Комплекс позволяет наблюдать за состоянием 20 каналов текущего банка памяти с точностью от 1 до 12 с в течение 10 ч. Предусмотрена возможность задания 20 банков памяти по 20 каналов в каждом банке.

При остановке сканирования комплекс осуществляет прием сигнала на фиксированной частоте с возможностью перестройки приемника по заданным частотам банков памяти.

Для выбора банка памяти и значения сканируемых (контролируемых) частот в каждом банке служит кнопка **«Канал»**, после нажатия на которую появляется окно для выбора банка, назначения частот и других параметров

сканирования. Для удобства пользователей все данные задаются в виде таблицы.

В первых двух колонках отображается номер банка памяти и комментарий для него, в качестве которого обычно используют условное обозначение, например, название радиостанции, работающей на контролируемой частоте. В третьей колонке задается вид модуляции принимаемого сигнала. В поле «Частота», соответственно,– значение частоты, подлежащей контролю. После запуска программа осуществляет сканирование по списку заранее заданных частот.

Программы семейства Sedif

В это семейство входят три программы: Sedif Plus, Sedif Pro и Sedif Scout, являющиеся, пожалуй, наиболее известными из всех подобных российских программ. Хотя в основном они реализуют примерно те же функции и возможности, что и другие рассматриваемые программы.

Sedif Plus – наиболее простой вариант, осуществляющий все основные необходимые функции программы.

Sedif Pro дополнительно позволяет работать со звуковыми картами типа Sound Blaster (однако необходима полная совместимость со стандартами фирмы Creative Labs). Эта возможность позволяет записывать принимаемые приемником сигналы на жесткий диск компьютера и в дальнейшем их анализировать и обрабатывать.

Sedif Scout имеет еще один дополнительный режим, названный «Поиск». В этом режиме возможно определение местоположения радиомикрофона, размещенного в том же помещении, что и приемник. Конечно, для удачной локализации необходимо соблюсти ряд условий, иначе вероятность может резко снизиться.

На сегодняшний день дальнейшее развитие продуктов серии Sedif остановлено. Его постепенно вытесняет новый программный продукт Filin.

Программа Filin

Программа Filin может быть отнесена к примерам удачной реализации концепции функционального совмещения специального приемника с персональной ЭВМ.

Программа предназначена для работы в операционных системах Windows и позволяет использовать для поиска ЗУ следующие типы сканирующих приемников: AR-3000A, AR-2700, AR-8000, IC-R10, IC-R8500, а при наличии приставки-анализатора спектра SDU-5000 и радиоприемники IC-R7000, IC-R7100 и IC-R9000. Она обладает информативным интерфейсом,

отображающим процесс работы аппаратуры поиска, характеристики сигналов и промежуточные результаты их анализа.

В программе предусмотрен набор корреляторов, позволяющих по тестовому акустическому сигналу или по естественному акустическому фону помещения опознавать принимаемый сигнал как излучение радиозакладки. Реализован ряд функций автоматического поиска неизвестных или подозрительных излучений. Кроме того, она дает возможность проводить анализ принимаемых сигналов по их спектрам, осциллограммам, корреляционным функциям и другим характеристикам.

Программа RSPlus

Программа RSPlus удачно сочетает возможности поиска средств негласного съема информации и радиоконтроля. Одновременное отображение эталонной и текущей панорам в расположенных друг под другом окнах при одновременной раскраске новых источников делает программу удобной для последовательного поиска в одном или нескольких помещениях.

Важная особенность программы – наличие банка частот, в котором могут храниться «портреты» источников: в число записываемых характеристик включаются не только спектральные портреты для первых трех гармоник, но и их звуковые образы.

Однако в специальной литературе встречаются ссылки на наличие в программе множества недоработок.

10.7. Программно-аппаратные комплексы

Дальнейшим шагом по пути совершенствования процедуры поиска ЗУ является применение программно-аппаратных комплексов радиоконтроля и выявления каналов утечки информации, так как их возможности значительно шире, нежели чем у просто совмещенных с ЭВМ сканирующих приемников. В наиболее общем виде эти возможности заключаются в следующем:

- выявление излучений радиозакладок;
- пеленгование радиозакладных устройств в реальном масштабе времени;
- определение дальности до источников излучения;
- аналого-цифровая обработка сигналов с целью определения их принадлежности к излучению радиозакладок;
- контроль силовых, телефонных, радиотрансляционных и других сетей;
- работа в многоканальном режиме, позволяющем контролировать несколько объектов одновременно;
- постановка прицельных помех на частотах излучения радиозакладок и др.

На рынке специальных технических средств защиты информации сегодня представлено достаточно изделий как отечественного, так и зарубежного производства, в той или иной степени реализующих эти функции. Однако поиск средств негласного съема информации и, в частности, локализация источников радиосигналов, находящихся в так называемой «ближней зоне» остается их основным предназначением. Решение задачи поиска обеспечивается наличием в составе комплексов следующих элементов:

- широкодиапазонного перестраиваемого по частоте приемника (сканера);
- блока распознавания радиозакладок, осуществляющего идентификацию излучений радиомикрофонов на основе сравнения принятых продетектированных сигналов с естественным акустическим фоном помещения (пассивный способ) или тестовым акустическим сигналом (активный способ);
- блока акустической локации, позволяющего по запаздыванию переизлученного зондирующего звукового импульса определять расстояние до активных радиомикрофонов;
- электронно-вычислительной машины (процессора), осуществляющей как обработку полученных данных, так и управление приемником.

По принципу построения все известные приборы данного класса делятся на две основные группы:

- специально разработанные комплексы, конструктивно выполненные в виде единого устройства;
- комплексы, сформированные на базе серийного сканера, персонального компьютера (обычно notebook) и специального программного обеспечения, аналогичного рассмотренному выше.

Специально разработанные комплексы

Среди приборов первой группы наибольшей популярностью пользуются следующие: **OSC-5000 (Oscor)**, **СРМ-700 («Акула»)** и **ST 031 («Пиранья»).**

OSC-5000 (Oskor). Его название происходит от Omni Spectral Correlator и характеризует основное назначение как спектрального коррелятора (рис. 149). Прибор разработан американской фирмой Research Electronics Intl., однако имеет сертификат Гостехкомиссии при Президенте РФ (сертификат № 81), что говорит о несомненных достоинствах прибора.

Программно-аппаратный комплекс Oscor достаточно хорошо известен и на российском, и на мировом рынке, ему более шести лет, и за эти годы он неоднократно модифицировался (с версии 1.6 до 2.2). Цена комплекса в зависимости от конфигурации колеблется от $12 000 до $16 000.

Рис. 149. Многофункциональный специальный коррелятор OSC-5000

OSC-5000 представляет собой функциональное сочетание нескольких приборов.

Во-первых, это панорамный приемник последовательно-параллельного типа (сканер), перекрывающий диапазон частот 10 кГц-3 ГГц с полосой пропускания 15 кГц. Столь широкий диапазон перестройки обеспечивается наличием нескольких входов (фактически нескольких приемников), к каждому из которых подключена своя антенна (рамочная, штыревая и дискоконусная). Анализ может производиться как во всем диапазоне, так и в заданных полосах (до 31 полосы), автоматически или в ручном режиме. Максимальная скорость перестройки по частоте составляет 93 МГц/с при полосе пропускания 250 кГц. Чувствительность приемника соответствует значению 0,8 мкВ, а динамический диапазон входных сигналов составляет 90 дБ. Прибор оснащен набором детекторов, что дает возможность принимать сигналы с различным видом модуляции.

Несомненным достоинством является наличие инфракрасного детектора с областью спектральной чувствительности 0,85–1,07 мкм и специального адаптера, позволяющего вести контроль наличия излучений от сетевых закладок в диапазоне частот 10 кГц -5МГц в проводных линиях с напряжением до 300 В.

Во-вторых, это осциллограф и анализатор спектра, позволяющий наблюдать амплитудно-временные развертки демодулированных сигналов и их спектры с разрешением по частоте не хуже 50 Гц.

Режим работы прибора, позволяющий осуществлять панорамный анализ выбранного диапазона частот с заданным разрешением носит название Sweep. В этом режиме можно масштабировать выбранный спектральный диапазон и выделять интересующие сигналы. Особо здесь следует подчеркнуть наличие специальной функции отображения меток пиков сигналов, так называемая функция Display Peak Signal, которая позволяет сохранять на экране метки пиков ограниченных во времени сигналов. Метки при этом остаются и при следующем сканировании, что бывает необходимо для поиска и распознавания излучений передатчиков (закладок), работающих с перестройкой по частоте.

Режим Analise дает возможность более детального излучения спектральных форм выбранных в Sweep-режиме сигналов и их временных характеристик.

В-третьих, это коррелятор, необходимый для идентификации сигналов ЗУ.

Принцип работы коррелятора заключается в том, что демодулированный низкочастотный сигнал сравнивается с акустическим фоном помещения. При этом на коррелятор одновременно подается для сравнения два низкочастотных сигнала: первый – демодулированный с выхода приемника, второй – аудиосигнал акустического фона помещения или сигнал телефонной линии. Роль источника аудиосигнала может выполнять либо обычный микрофон, либо линейный выход применяемого аудиовоспроизводящего устройства: CD-плейера или магнитолы.

На основании результатов этого сравнения рассчитывается коэффициент корреляции и в зависимости от полученного значения каждому обнаруженному сигналу присваивается один из пяти уровней тревоги. При превышении этим уровнем заданного пользователем порогового значения срабатывает система оповещения – это мигание сообщения на экране, звуковой сигнал, запись на диктофон или печать характеристик (по выбору). Прибор фиксирует частоту, тип демодулятора, дату и время обнаружения тревожного сигнала, сохраняет все эти данные в базе данных или выводит на встроенный термоплоттер. Прибор можно запрограммировать так, что при обнаружении

тревожного сигнала будет распечатан его спектр или произойдет запись передаваемой информации на диктофон. Переключение в режим Correlation осуществляется нажатием всего одной клавиши.

В программно-аппаратном комплексе OSC-5000 предусмотрен режим загрузки в память частот, излучения на которых прибор будет считать «дружественными» (Friendly Signals, например, сигналы теле- и радиовещательных станций) и не затрачивать время на анализ в автоматическом режиме. Всего Oscor может хранить информацию (дату и время обнаружения, частоту, тип демодулятора, полосу) о 7168 сигналах при штатной памяти 128 кБ или о 28 672 при расширенном до 512 кБ объеме памяти. Эта информация может редактироваться пользователем, протоколироваться самим прибором на термоплоттере или сбрасываться на ПЭВМ через COM-порт для дальнейшей обработки.

Дополнительными опциями для Oscor являются следующие:

- OVM-5000 (Video Monitoring Option), реализованная в комплекте **OSC-5000 Deluxe** и предназначенная для анализа видеосигналов систем PAL/SECAM/NTSC при поиске видеопередатчиков;
- OTL-5000 (Trangulate and Locate Option) – акустический локатор, предназначенный для определения местоположения активных радиомикрофонов;
- OPC-5000 – специальное программное обеспечение для работы с базами данных сигналов OSCOR через COM-порт персональной ЭВМ, а также организации дистанционного контроля работы комплекса через модем.

Зонд-монитор СРМ-700 «Акула» – это универсальный прибор, предназначенный для поиска и обнаружения устройств скрытого съема информации, известен у нас в стране как комплекс «Акула» (см. рис. 150). Он предназначен для решения следующих задач:

1) обнаружения радиосигналов специальных технических средств скрытого перехвата конфиденциальной информации (радиомикрофонов, импульсных передатчиков, устройств дистанционного управления), работающих в диапазоне частот 50 кГц...3 ГГц;

2) обнаружения ЗУ, использующих токопроводящие линии для передачи информации в диапазоне частот 15 кГц...1 МГц;

3) выявления скрытоустановленных микрофонов с передачей информации по специально проложенным проводам, а также определения степени опасности утечки информации за счет акусто-электрического преобразования в телефонных аппаратах, радиотрансляционных и других приборах;

4) обнаружения скрытых видеокамер и диктофонов;

5) выявления инфракрасных источников излучения (ЗУ с инфракрасным каналом передачи информации);

6) обнаружения каналов утечки акустической информации.

Рис. 150. Универсальный прибор СРМ-700 «Акула»

Первые три задачи являются основными, поэтому в любой комплект СРМ-700 обязательно входят три соответствующих зонда.

- *Высокочастотный (радиочастотный) РЧ-зонд* с областью спектральной чувствительности 50 кГц-3 ГГц. Это активный прибор с собственным коэффициентом усиления 20 дБ, обеспечивающий пороговую чувствительность приемного устройства на уровне – 85 дБ относительно 1 мВт и динамический диапазон входных сигналов 100 дБ. Он обеспечивает, например, обнаружение источника мощностью 1 мкВт и частотой излучения 150 МГц на дальности около 2 м.
- *Низкочастотный ОНЧ-зонд* для контроля токопроводящих линий. Его диапазон рабочих частот лежит в пределах от 15 кГц до 1 МГц, пороговая чувствительность – не хуже 60 дБ относительно 1 мВт. Максимальный уровень постоянного напряжения в тестируемых линиях не должен превышать 300 В, а переменного с частотой 60 Гц-1500 В.

- *Высокочувствительный усилитель* для прослушивания электромагнитных сигналов звукового диапазона (100 Гц - 15 кГц), возникающих вблизи токопроводящих линий. Он имеет систему автоматической регулировки усиления и обеспечивает прием сигналов, уровень которых может изменяться в пределах от 1,7 мкВ до 10 В (135 дБ). Один выход устройства предназначен для контроля принимаемых сигналов через наушники в реальном масштабе времени, другой – для записи на магнитофон. Уровни выходных сигналов, соответственно, имеют значения 5 В и 25 мВ.

Для решения задач 4–6 применяются дополнительные зонды.

- Электромагнитный зонд *MLP-700* – для обнаружения скрытых видеокамер и диктофонов.
- Инфракрасный зонд *IRP-700* – для обнаружения инфракрасных источников излучения.
- Акустический зонд *ALP-700* – для обнаружения каналов утечки акустической информации.

Кроме вышеперечисленных основных функций комплекс позволяет решать следующие задачи:

- *работа в дежурном режиме* («мониторинга опасности») – отслеживает электромагнитную обстановку в контролируемом помещении и подает соответствующий сигнал при обнаружении неизвестного устройства (звуковой с частотой 2,8 кГц или световой с частотой мигания 2 Гц);
- *обеспечение непрерывной записи* всех принимаемых сигналов на любой стандартный магнитофон.

Для контроля уровней принимаемых сигналов в приборе реализован 18-сегментный жидкокристаллический индикатор (в руководстве пользователя он может быть назван как дисплей или монитор).

Питание комплекса осуществляется от специального сетевого адаптера или никель-кадмиевого аккумулятора с напряжением 12 В.

Для предварительной проверки работоспособности аппаратуры в ее комплект дополнительно могут входить:

- *TTM-700* – тестовый радиопередатчик мощностью 0,7 мВт;
- *CCT-700* – тестовый передатчик с передачей сигнала по энергетической сети;
- *IRT-700* – тестовый инфракрасный передатчик.

Несомненно, комплекс CPM-700 («Акула») американской фирмы Research Electronics Intl. является достойным представителем рассматриваемого класса приборов.

Российский комплекс ST 031 («Пиранья») по своим характеристикам практически не уступает вышеперечисленным приборам, а порой и опережает их, имея при этом малые размеры и вес (180×97×47 мм; 0,8 кг).

Он предназначен для проведения оперативных мероприятий по обнаружению и локализации технических средств негласного получения конфиденциальной информации, а также контроля естественных и искусственно созданных технических каналов утечки информации (рис. 151).

Рис. 151. Комплекс выявления технических каналов утечки информации ST 031 («Пиранья»)

Фактически ST 031 – это комплекс, состоящий из следующих приборов: высокочастотного детектора-частотомера; сканирующего анализатора проводных линий; детектора инфракрасных излучений; детектора низкочастотных магнитных полей; виброакустического приемника; акустического приемника; проводного акустического приемника.

Важным достоинством «Пираньи» является то, что этот прибор позволяет анализировать принимаемые сигналы как в режиме осциллографа, так и в режиме анализатора спектра с индикацией численных параметров. При этом время вывода осциллограммы не превышает 0,2 с, а спектрограммы – 0,3 с. Разрешение собственного графического дисплея составляет 128×64 точки.

Чувствительность приемного устройства комплекса – 10 мВт, полоса пропускания – 22 кГц. Объем внутренней памяти позволяет удерживать от 15 до 60 отображений характеристик сигналов.

Комплексы, сформированные на базе серийного сканера

Среди программно-аппаратных средств второй группы, созданных путем функционального объединения нескольких серийно выпускаемых устройств, на российском рынке активно предлагаются комплексы радиоконтроля и пеленгации ЗАО «Иркос».

Комплексы АРК. Они представлены семейством стационарных, мобильных (автомобильных, вертолетных) и портативных приборов.

С точки зрения поиска ЗУ наибольший интерес представляют именно портативные комплексы **АРК-Д1** (**КРОНА-1**, см. рис. 152), **АРК-ПК** и многоканальный комплекс контроля помещений учреждения **АРК-Д3** (**КРОНА-2**).

Рис. 152. Портативный автоматизированный комплекс радиоконтроля АРК-Д1

Эти приборы построены на базе сканирующего приемника AR-3000A, функциональные возможности которого расширены за счет специально разработанного синтезатора частот, процессора быстрого преобразования Фурье

и 12-разрядного аналого-цифрового преобразователя. В результате этого обеспечена скорость перестройки 40–70 МГц/с в диапазоне частот 1-2000 МГц. Динамический диапазон входных сигналов лежит в пределах от 55 до 58 дБ.

Отличительными особенностями комплексов АРК являются следующие:

- Возможность обнаружения излучений радиомикрофонов, работающих под «прикрытием» мощных станций, различение внешних и внутренних источников излучений для контролируемых помещений. Данная функция обеспечивается за счет применения разнесенной антенной системы, состоящей из 3–4 широкополосных антенн типа АРК-А1, АРК-А2, а также внешней «опорной» антенны АРК-А4 или АРК-А5М.
- Контроль наличия ЗУ в сетях переменного тока с напряжением до 400 В (с помощью устройства АРК-КПС), радиотрансляционных, телефонных и других сетей в диапазоне до 30 МГц.
- Контроль излучений внедренных портативных телевизионных камер (устройство АРК-КТВ).
- Активное и пассивное выявление излучений специальных технических средств негласного съема аудиоинформации.

Активный способ реализован на основе применения специально подобранных акустических зондирующих сигналов; пассивный – на использовании естественного акустического фона помещения, анализе гармоник излучений ЗУ, а также анализе сигналов с выхода «опорной» вынесенной из контролируемого помещения антенны. При этом обеспечивается надежная идентификация сигналов с амплитудной и частотной модуляцией, инверсией спектра и частотными перестановками («частотной мозаикой»).

- Локализация мест размещения источников излучения в контролируемом помещении.
- Подавление радиозакладных устройств путем создания прицельных по частоте помех с помощью малогабаритных передатчиков АРК-СПМ, которые могут быть размещены в нескольких контролируемых помещениях и дистанционно управляться многоканальным комплексом АРК-Д3.

Специально разработанный пакет прикладных программ СМО-Д5, предназначенный для работы в среде Windows, обеспечивает следующие возможности:

- управление всеми устройствами комплекса в одном пакете (режимы «Панорама», «Обнаружение», «Поиск», «Контроль ВЧ», «Контроль НЧ», «ТВ»);
- изменение конфигурации используемых антенн;

- использование любого из алгоритмов тестирования радиоизлучений на принадлежность к классу радиомикрофонов;
- измерение уровней сигналов с выходов антенн (в децибеллах относительно 1 мкВ по входу радиоприемного устройства);
- записи спектральных характеристик принимаемых излучений на жесткий диск персональной ЭВМ и их дальнейшей обработки.

Благодаря размещению в кейсе с универсальным питанием от сети переменного тока, автомобильной бортовой сети и автономных аккумуляторов комплексы **АРК-Д1** и **АРК-ПК** могут быть использованы как для работы в помещениях, так и на выезде в сложных условиях эксплуатации.

Помимо рассмотренных, на рынке имеется достаточно широкий выбор и других приборов аналогичного назначения – это «Дельта-П», КРК-1, RS-1000, ECR-2, RANGER, Scanlock ECM+ и др.

Какому конкретно комплексу отдать предпочтение, зависит прежде всего от решаемых задач и возможностей потребителя.

Необходимо только помнить, что ни один прибор не сможет обеспечить для вас 100-процентную защиту от всех средств шпионажа. Кроме того, каждая система решает свои строго определенные задачи, а эффективность ее работы зависит главным образом от того, насколько профессионально она используется.

И последнее, хотя стоимость в гораздо большей степени отражает затраты и рыночную политику производителя или продавца, чем специальные характеристики приборов, все же надо иметь в виду, что работоспособная система, включающая в свой состав стандартный сканер или специальный приемник, не может стоить дешевле $800 – $1200, поэтому если вам предлагают панацею от всех бед за $200 – $300, то лучше воздержитесь от подобной покупки.

10.8. Нелинейные радиолокаторы

Одной из наиболее сложных задач в области защиты информации является поиск внедренных ЗУ, не использующих радиоканал для передачи информации, а также радиозакладок, находящихся в пассивном (неизлучающем) состоянии. Традиционные средства выявления такие, как панорамные радиоприемники, анализаторы спектра или детекторы поля, в этом случае оказываются неэффективны. Визуальный осмотр также не гарантирует обнаружение подобных ЗУ, так как современные технологии позволяют изготовлять их с любым видом камуфляжа, прятать в элементах строительных конструкций и интерьера.

Общие сведения о нелинейных локаторах

Именно эта проблема и привела к появлению совершенно нового вида поискового прибора, получившего название *нелинейного радиолокатора*. Своим названием он обязан заложенному физическому принципу выявления подслушивающих устройств.

Дело в том, что технические средства промышленного шпионажа являются радиоэлектронными устройствами. В их состав входят полупроводниковые элементы (диоды, транзисторы, микросхемы), для которых характерен *нелинейный* вид вольт-амперной характеристики, связывающей протекающий через *p–n*-переход электрический ток ***i*** с приложенным напряжением ***u*** (см. рис. 153).

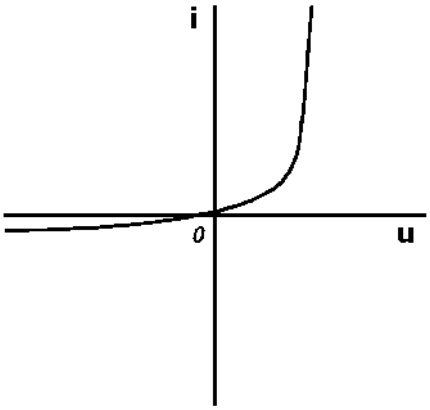

Рис. 153. Характеристика *p–n*-перехода

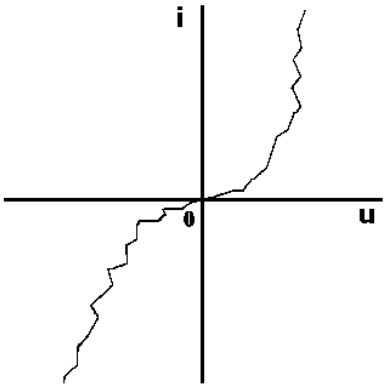

Рис. 154. Характеристика случайного МОМ-перехода

Наличие такой нелинейной связи приводит к возникновению на выходе полупроводникового прибора бесконечно большого количества переменных напряжений (гармоник) с частотами $f_n = n \times f_0$, где n = 1,2,3,.. (любое натуральное число), а f_0 – частота зондирующего сигнала, действующего на входе полупроводникового прибора. Сам факт возникновения сигнала с частотой f_0 на входе полупроводникового элемента обязан явлению наведения ЭДС и токов в случайных антеннах, которыми могут оказаться проводники печатных плат или другие компоненты ЗУ при облучении их высокочастотным сигналом.

Таким образом, нелинейный локатор – это прибор, который просто реализует следующий принцип: излучает электромагнитную волну с частотой f_0, а принимает переизлученные сигналы на частотах f_n. Если такие сигналы будут обнаружены, то в зоне действия локатора есть полупроводниковые элементы, и их необходимо проверить на возможную принадлежность к ЗУ.

В соответствии с вышесказанным нелинейный радиолокатор обнаруживает только радиоэлектронную аппаратуру и, в отличие от классического линейного радиолокатора, «не видит» отражений от окружающих предметов, то есть обладает высокой избирательностью.

Источниками помех для его работы могут служить контакты со слабым прижимом, для которых характерно наличие промежуточного окисного слоя (сваленные вместе металлические канцелярские скрепки, монеты; плетеные сетки) или просто подвергнутые коррозии металлы. В редких случаях (при большой мощности излучения) нежелательный эффект могут дать паяные и сварные соединения.

Причина возникновения указанных помех связана с тем, что слабые металлические контакты, как правило, представляют собой квазинелинейные элементы с неустойчивым *p*–*n*-переходом, вызванным наличием окислов на поверхности металлов. В физике полупроводников подобные структуры известны как «металл – окисел – металл», а нелинейные элементы такого типа называются МОМ-структурами. Вольт-амперная характеристика случайного соединения, в отличие от характеристики *p*–*n*-перехода, обычно симметрична. Примерный вид ее показан на рис. 154. Методы селекции сигнала в нелинейных радиолокаторах на фоне подобных помех подробно будут рассмотрены ниже.

Впервые принципы нелинейной радиолокации были применены еще в середине 70-х годов, когда на контрольно-пропускных пунктах заводов и складов были установлены устройства предупреждения о попытке скрытного выноса радиоаппаратуры или ее электронных компонентов. После этого идеей заинтересовались спецслужбы и стали разрабатываться приборы обнаружения скрытых электронных средств разведки и радиовзрывателей.

Несмотря на свою специфичность принципы нелинейной локации нашли себе и «мирное применение». Так, например, в настоящее время получили широкое распространение системы обнаружения несанкционированного выноса предметов из магазинов, поиск людей в снежных завалах и разрушенных зданиях, контроль багажа авиапассажиров и т. д.

Первым устройством, поступившим на вооружение спецслужб, в частности ЦРУ, был локатор Superscout, серийный выпуск которого начался с 1980 года. В 1981 году появился британский Broom (см. рис. 155), который несколько уступал американскому аналогу. Наш отечественный серийный локатор появился в 1982 году и назывался «Орхидея». Правда, раньше ему предшествовали несколько уникальных образцов, но они были сняты с появлением «Орхидеи».

Рис. 155. Нелинейный радиолокатор Broom ESM

В настоящее время на российском рынке представлено около двух десятков типов нелинейных радиолокаторов. Как правило, это портативные приборы отечественного и импортного производства стоимостью от $2000 до $30000. Имеющий место разброс цен обусловлен различными техническими характеристиками, важнейшими из которых являются возможность идентификации электронных и контактных источников помех, способы индикации принимаемых сигналов, габариты, вес, тип питания.

В России производится почти столько же моделей нелинейных локаторов, сколько в США и Англии вместе взятых. Однако западные производители предлагают многофункциональные приборы с широким набором сервисных функций, что естественно влияет на цену ($25 000–$30 000). Российские производители держат качество приборов на должном уровне при сохранении относительно доступных цен ($2 000–$10 000), за счет чего многофункциональность локаторов отходит на второй план.

Основные характеристики нелинейных радиолокаторов

К основным характеристикам нелинейных радиолокаторов относятся: значения рабочих частот зондирующих сигналов; режим излучения и мощность передатчика; форма, геометрические размеры и поляризация антенн; точность определения местоположения переизлучающего объекта; чувствительность приемника; максимальная дальность действия и глубина, на которой возможно обнаружение закладки внутри радиопрозрачного материала; количество анализируемых гармоник; размеры**,** вес и тип питания радиолокатора. Рассмотрим эти характеристики более подробно.

Значения *рабочих частот* передатчиков всех типов локаторов находятся в пределах от 400 до 1000 МГц (рабочие частоты приемников, соответственно, составляют удвоенную или утроенную частоту передатчиков). Большинство отечественных и зарубежных образцов работают в диапазоне, близком к 900 МГц. Такой выбор обусловлен компромиссом в решении следующего противоречия.

С одной стороны, чем ниже частота зондирующего излучения, тем лучше его проникающая способность внутрь предметов и сред, в которых могут быть спрятаны ЗУ, и больше относительный уровень высших гармоник в переизлученном сигнале;

С другой – чем выше частота излучения, тем уже диаграмма направленности антенны локатора при фиксированных геометрических размерах, следовательно выше плотность потока мощности зондирующего сигнала (кроме того, на высоких частотах лучшими свойствами обладают случайные антенны, в качестве которых выступают ножки навесных элементов, проводники печатных плат и т. п., а их размеры, как известно, невелики).

К сожалению, многие нелинейные радиолокаторы функционируют на фиксированных частотах без возможности перестройки. Причина такого подхода – упрощение схемотехнических решений, то есть существенное снижение цены. Расплачиваться за такое упрощение приходится худшими эксплуатационными характеристиками, так как на частотах приема могут присутствовать излучения посторонних радиоэлектронных средств. И если даже уровни мешающих сигналов невелики, их может быть достаточно для нарушения нормальной работы радиолокаторов, так как чувствительность приемных устройств очень велика.

Естественно, более удобны в эксплуатации локаторы, имеющие возможность перестройки в определенном диапазоне. Так, например, в нелинейном локаторе Orion (NJE-400) фирмы Research Electronics International (REI) предусмотрен автоматический режим выбора рабочей частоты в диапазоне

880-1000 Мгц. Ее оптимальное значение определяется по наилучшим условиям приема для 2-й гармоники частоты зондирующего сигнала.

От рабочей частоты зависит форма и геометрические размеры антенн, важной характеристикой которых является *поляризация*. Передающие антенны имеют, как правило, линейную, а приемные – круговую поляризацию.

Точность определения местонахождения радиоэлектронного устройства, которую позволяют достигать используемые размеры антенн, соответствует нескольким сантиметрам. Например, для локаторов «Родник» (см. рис. 156) и «Циклон» – это 2 см.

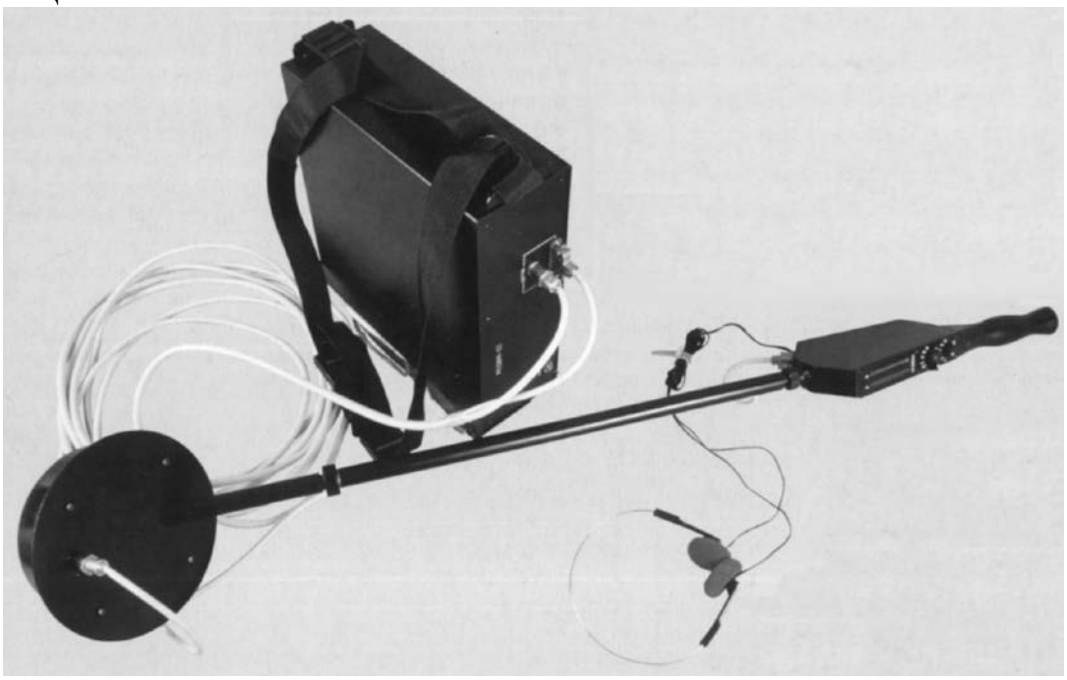

Рис. 156. Нелинейный радиолокатор Родник-2М

Следующей группой характеристик нелинейных локаторов являются режим работы передатчика, излучаемая мощность и чувствительность приемника.

В зависимости от *режима работы* нелинейные локаторы делятся на локаторы с непрерывным и импульсным излучением. Практически все зарубежные приборы и некоторые отечественные работают с непрерывными зондирующими сигналами малой мощности (10-850 мВт). Большинство отечественных локаторов работают в импульсном режиме излучения с пиковой мощностью 5-400 Вт. Из-за простоты используемых приемных устройств импульсные локаторы значительно дешевле непрерывных.

Следует отметить, что высокая *мощность* и характер излучения импульсных локаторов могут создать определенные проблемы в плане электромагнитной совместимости со средствами связи, навигации, телевещания, дат-

чиками пожарной и охранной сигнализации. Кроме того, зондирующее излучение оказывает негативное воздействие на операторов, эксплуатирующих аппаратуру. Поэтому, в соответствии с санитарными нормами, мощность современных локаторов ограничена максимальным значением 3-5 Вт для непрерывного режима и средним значением 0,1-1,5 Вт (до 400 Вт в импульсе) – для импульсного. Однако даже при таких ограничениях у оператора после часа работы часто начинают болеть глаза, так как именно они наиболее чувствительны к СВЧ-излучению.

Некоторые современные нелинейные локаторы имеют возможность изменения мощности зондирующего сигнала. Так, в локаторе NJE-400 уровень непрерывного излучения регулируется в пределах от 0,01 до1 Вт, а в радиолокаторе «Циклон-М» пиковое значение импульсной мощности – от 80 до 250 Вт. Более того, приемник локатора Superbroom Plus снабжен функцией автоматического установления мощности излучения в зависимости от величины принимаемого сигнала на 2-й гармонике.

Чувствительность приемников современных нелинейных локаторов лежит в пределах от 10^{-15} до 10^{-11} Вт. У импульсных она несколько хуже, что объясняется соответствующим превосходством пиковой мощности импульсных передатчиков (примерно на 35–40 дБ). В большинстве радиолокаторов используются приемники с регулируемой чувствительностью. Диапазон регулировки этого параметра составляет 30-50 дБ.

В соответствии с законом сохранения энергии (чем выше номер принимаемой гармоники *n*, тем меньше ее амплитуда) в современных локаторах анализируются только 2-я и 3-я гармоники зондирующего сигнала. И тем не менее, нелинейные радиолокаторы являются приборами ближнего действия, так как коэффициент преобразования энергии облучающего сигнала в энергию высших гармоник очень мал. Конкретная *дальность действия* зависит от множества факторов. В первую очередь, это тип обнаруживаемого устройства, наличие у него антенны и ее длина, условия размещения объекта поиска (в мебели, за преградами из дерева, кирпича, бетона и т. п.). Максимальное расстояние, на котором возможно выявление ЗУ ограничено величиной 0,5 м. Данное значение соответствует варианту работы на открытых площадях или в больших необорудованных помещениях, например таких, как готовящийся к сдаче строительный объект. Для офисных помещений возможности обнаружения еще скромнее. Это связано с высокой концентрацией различных «помеховых» объектов (канцелярские принадлежности, оргтехника и т. п.).

С понятием максимальной дальности действия тесно связана максимальная *глубина обнаружения объектов* в маскирующей среде. Для строительных конструкций она может достигать несколько десятков сантиметров. Например, локаторы серии «Циклон» обнаруживают радиоэлектронные изделия в

железобетонных стенах толщиной до 50 см, в кирпичных и деревянных – до 7 см.

Важной характеристикой является и *количество анализируемых гармоник* переизлученного сигнала. Так как одновременный прием на двух гармониках зондирующего сигнала дает неоспоримые преимущества по сравнению с однотональным приемом: он дает возможность осуществлять идентификацию обнаруженных объектов.

Современные нелинейные локаторы имеют небольшие *размеры, вес* и позволяют работать как от *электросети,* так *и от автономных источников питания (аккумуляторов).*

Например, у нелинейного локатора «Онега» (см. рис. 157) вес приемопередающего блока составляет 2 кг, а антенны со штангой – 0,8 кг.

Рис. 157. Нелинейный радиолокатор Онега-2М

Вес нелинейного локатора «Циклон-М» в упаковке (кейсе) – 5,5 кг (при этом вес приемопередающего блока составляет 1,2 кг). У нелинейного локатора «Orion» (NJE-400) приемопередающий блок и антенна закреплены на одной телескопической штанге, и общий вес конструкции не превышает 1,8 кг. Для удобства работы в этом локаторе используются беспроводные «инфракрасные» наушники.

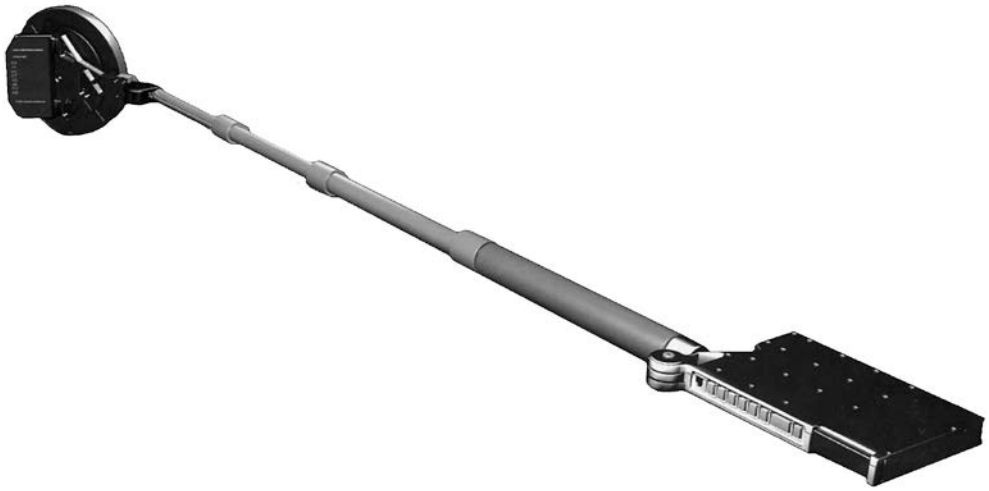

Рис. 158. Нелинейный радиолокатор Онега-2М

Конструктивное исполнение изделий «Переход», «Родник-ПМ» и «Энвис» дает оператору возможность работать без постоянного перемещения приемопередающего блока аппаратуры, который размещен в чемодане типа «атташе-кейс». Блок соединен с антенным датчиком кабелем длиной 5–7 м. Узел управления и индикации аппаратуры (регулировка мощности и чувствительности, световые индикаторы, гнездо головных телефонов) размещен на антенном датчике.

Иногда нелинейные локаторы выполняются в ранцевом варианте.

Способы селекции помех от случайных источников

Среди основных способов селекции сигнала на фоне помеховых воздействий, вызванных наличием в обследуемом пространстве случайных преобразователей частоты зондирующего излучения, выделяют следующие четыре способа:

- по относительному значению уровней принимаемого излучения на 2-й и 3-й гармониках частоты сигнала;
- по характеру изменения амплитуды шума на выходе приемника вблизи переизлучающего объекта;
- по реакции объекта на вибровоздействия;
- по наличию информационных признаков в принимаемом сигнале.

Первый способ применим для локаторов, снабженных функцией приема на двух гармониках частоты зондирующего сигнала (приборы Superbroom, Superscout, «Энвис» и др.). Он основан на различии преобразующих свойств полупроводниковых элементов и случайных МОМ-структур. Физическая сущность способа заключается в том, что для полупроводниковых элементов

характерен более высокий уровень переизлученного сигнала на 2-й гармонике по сравнению с 3-й (примерно на 20–40 дБ), и наоборот, контактные источники помех переизлучают сигнал на 3-й гармонике с большим уровнем, чем на 2-й.

Для удобства операторов такие нелинейные локаторы снабжены двумя индикаторами, относительная степень свечения которых и свидетельствует об амплитуде сигналов в соответствующих каналах (рис. 159). Индикаторные устройства могут располагаться непосредственно на приемо-передающем блоке (локаторы Superbroom, «Омега-3») или на антенной штанге (локаторы NJE-400, NR-900E, «Энвис»).

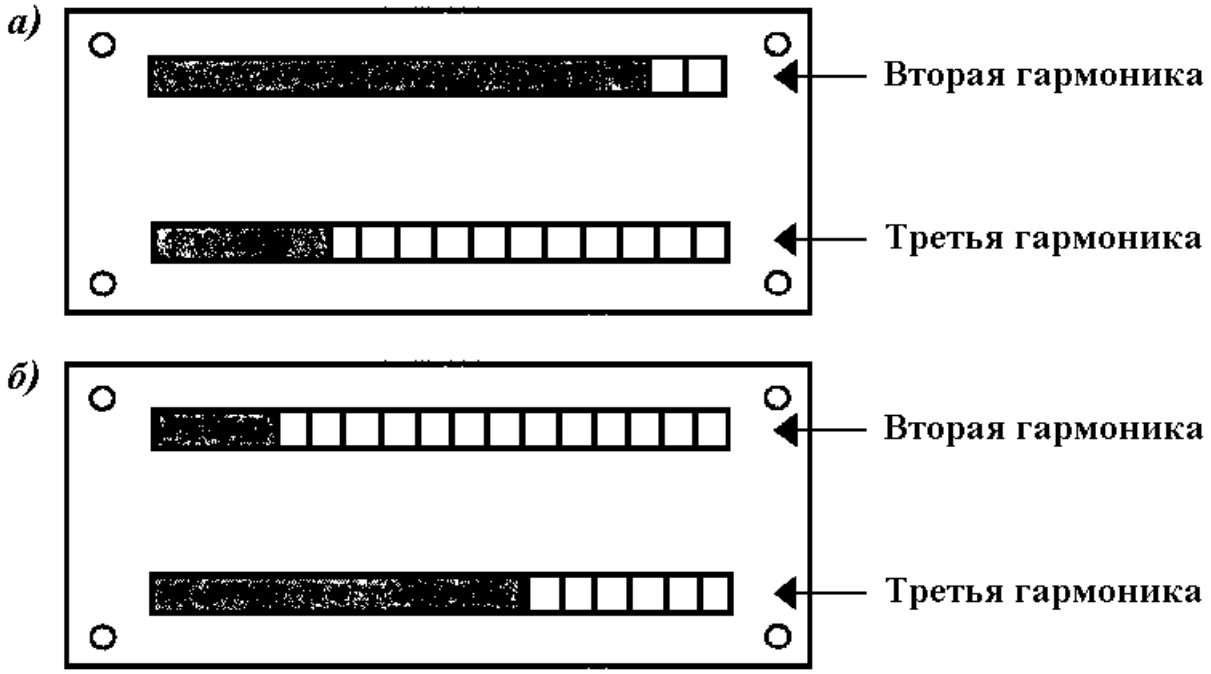

Рис. 159. Способ селекции помех по относительному уровню 2-й и 3-й гармоник переизлученного сигнала: а - обнаружен полупроводниковый элемент; б - в зоне облучения присутствует контактный источник помех

Второй способ. Характер изменения амплитуды шума на выходе приемника локатора также может служить признаком наличия объекта с нелинейной вольт-амперной характеристикой.

Так, при приближении антенны локатора к месту расположения полупроводникового элемента в головных телефонах, подключенных к выходу приемника, наблюдается значительное понижение уровня шума (примерно на 8–10 дБ). Минимальное значение $U_Ш$ имеет место на расстоянии ΔR от локируемого полупроводникового элемента, не превышающем 5 см (кривая 2, см. рис. 160). И наоборот, уменьшение расстояния между антенной и случайной

МОМ-структурой (помеховым объектом) сопровождается некоторым возрастанием уровня шума (кривая 1).

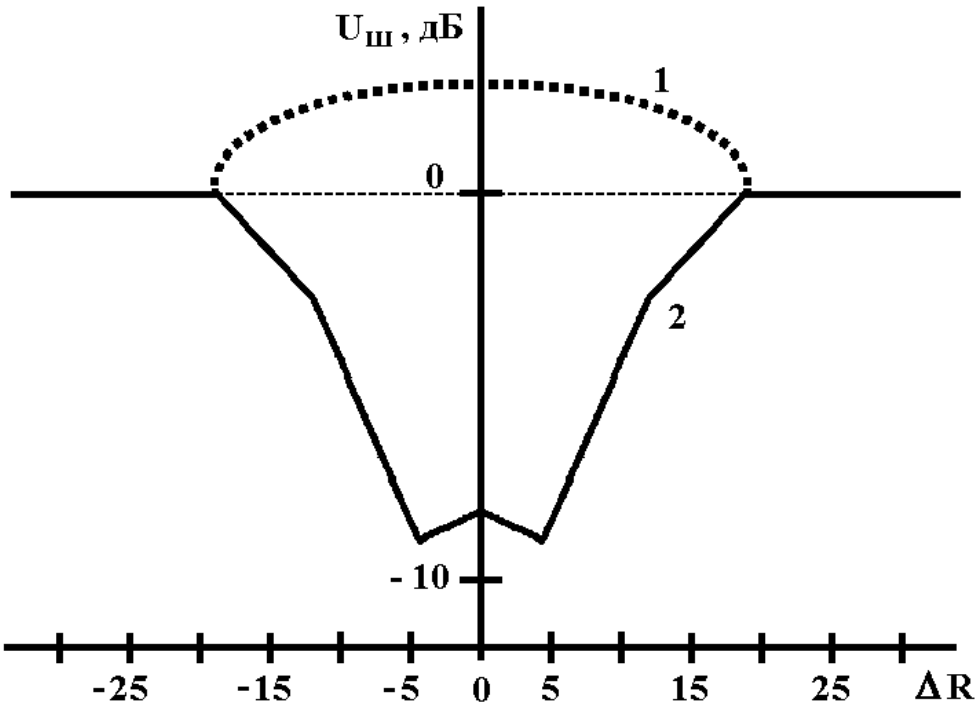

Рис. 160. Способ селекции помех по характеру изменения относительного уровня шума на выходе приемника нелинейного локатора.

К сожалению, применение данного способа может быть несколько ограничено следующими двумя факторами:

- данный способ может быть реализован только в локаторах, оснащенных амплитудным детектором;
- некоторые типы случайных электрических контактов вызывают не увеличение, а уменьшение амплитуды шума на выходе приемника радиолокатора.

Третий способ. Весьма эффективным способом селекции истинных полупроводниковых объектов на фоне ложных является физическое воздействие на исследуемый участок, например, методом простукивания. Характер звука в головных телефонах при этом позволяет судить о типе переизлучающего объекта: в случае ложного соединения в наушниках возникает типичное потрескивание на фоне тонального сигнала; в случае полупроводникового элемента сигнал остается чистым.

При использовании локаторов, работающих на двух гармониках, анализ объекта методом простукивания сопровождается наличием дополнительной информации о случайном объекте: хаотичным изменением уровня на световых индикаторах.

Часто в набор инструментов нелинейного локатора входит специальный резиновый молоток, предназначенный для простукивания поверхностей, под которыми могут быть спрятаны ЗУ.

Четвёртый способ. Ряд отечественных локаторов («Переход», «Родник-ПМ» и «Энвис») обеспечивают дополнительный способ анализа принятого от объекта сигнального отклика, а именно прослушивание процессов, происходящих в активно функционирующем объекте. Так, могут быть прослушаны речь, передаваемая подслушивающим устройством, тон таймера электронного взрывателя и т. п. Принцип получения этого эффекта аналогичен процессу модуляции при высокочастотном навязывании. Последний режим распознавания обеспечивает практически 100-процентную идентификацию объекта.

Сравнительная характеристика некоторых типов нелинейных локаторов

Для специалистов, эксплуатирующих радиоэлектронные средства, важное значение имеют не только паспортные сведения, но и их реальные параметры, характерные для различных условий эксплуатации. С этой точки зрения определенный интерес могут представлять данные компании «Гротек», опубликованные в журнале «Системы безопасности связи и телекоммуникаций» № 23, (1998), о результатах экспериментального исследования эффективности работы различных типов нелинейных радиолокаторов. Сравнительной оценке подверглись следующие типы локаторов отечественного производства: «Циклон-М1А»; «Онега-3»; NR-900M; NR-900E; «Родник-23».

Проведенные исследования показали, что при практическом использовании вышеперечисленных типов нелинейных локаторов для поиска электронных устройств скрытого съема информации наилучшие результаты показали мощные импульсные локаторы типа *NR-900M(E)* и *«Циклон-М1А»*, которые во многих случаях не требуют двустороннего обследования массивных элементов интерьера, обязательного вскрытия подвесных потолков, плинтусов и обеспечивают уверенный поиск в толще строительных конструкций. Тем не менее, при их использовании глубина односторонней «просветки» не должна превышать 20–25 см, в противном случае потребуется увеличение мощности передатчика или чувствительности приемника локатора, что приведет к росту количества ложных срабатываний, увеличению времени анализа или даже к пропуску объекта. Поэтому правильный подбор оператором чувствительности и мощности приборов нелинейной локации при обследовании различных мест проверяемого помещения имеет большое значение.

Следует отметить, что локаторы серии *NR* самые универсальные и удобные в эксплуатации приборы. Они имеют хорошую чувствительность и

избирательность, а также вполне современный внешний вид. При правильной настройке элементов управления позволяют легко отстраиваться от помеховых воздействий. Это самые «чувствительные» к экранированным «закладкам» локаторы. Узкая диаграмма направленности главного лепестка антенной системы и хорошее подавление задних ее лепестков позволяют эффективно работать рядом с бытовой оргтехникой без выноса их из помещений.

При умелом использовании нелинейный радиолокатор *«Родник-23»* также способен эффективно выявлять электронные устройства несанкционированного съема информации. Это удобный в эксплуатации и самый чувствительный прибор, поэтому работа в помещениях с большим количеством электронной техники затруднена из-за срабатываний локатора на помеховые объекты. При работе с этим устройством рекомендуется, по возможности, выносить или переставлять электронику от обследуемых мест. Глубина односторонней «просветки» не должна превышать 10–15 см. Это, естественно, увеличивает время проверки массивных элементов интерьера, но зато вероятность пропуска минимальна. «Родник-23» в режиме с выключенной модуляцией позволяет прослушивать сигнал отклика от электронных объектов, находящихся во включенном состоянии, при приеме излучения на 2-й гармонике зондирующего сигнала (например, при облучении работающего радиомикрофона отлично прослушивается акустика помещения). В ходе испытаний было отмечено, что локатор не оказывает вредного влияния на организм человека и не создает помех для работающей бытовой и другой техники, что также можно отнести к несомненным достоинствам прибора.

Основной недостаток «Родника-23» заключается в использовании антенны с линейной поляризацией, что приводит к необходимости обследования любой поверхности в двух взаимно перпендикулярных направлениях и, соответственно, к увеличению почти в 2 раза времени проверки помещения.

Самые скромные результаты продемонстрировал нелинейный радиолокатор «Онега-3», который по своим техническим и эксплуатационным характеристикам несколько уступил остальным исследованным приборам. Основной и существенный его недостаток – отключение звукового тона в головных телефонах при превышении 3-й гармоникой зондирующего сигнала уровня 2-й. Это существенно затрудняет обнаружение и даже приводит к возможному пропуску «закладки», находящейся рядом с помеховым объектом, например, рассыпанной мелочью, проволокой и т. п. Таким образом, сфера применения нелинейного локатора «Онега-3» ограничивается поиском в поверхностном слое строительных конструкций и элементах интерьера. Он способен обнаружить только простейшие объекты, серьезно неэкранированные и не имеющие специальных фильтров, снижающих эффективную нелинейную поверхность рассеивания искомого объекта.

Максимальная дальность (R_{max}, м) обнаружения различных типов ЗУ для некоторых видов нелинейных локаторов приведена в табл. 25.

Таблица 25.

Тип закладного устройства	Тип нелинейного локатора				
	«Циклон-М1А»	«Онега-3»	NR-900M	NR-900E	«Родник-2З»
Контрольное устройство аппарата NR-900E	0,5	0,8	0,8	0,7	1,1
Радиомикрофон, 50×28×10 мм, длина антенны L_a=17 мм, несущая частота f=418 МГц, корпус металлический	1,6	1,9	19	1,15	2,5
Радиомикрофон, 28х18х1 1 мм, L_a=77 мм, f=105,7 МГц, корпус металлический	1	1,9	1,9	1,05	1,9
Радиомикрофон, 31х9х8 мм, L_a=16 мм, f=410 МГц, корпус металлический	0,7	0,8	0,8	0,8	1,1
Телефонный радиомикрофон- конденсатор, f=101 МГц, корпус металлический	0,8	1	1	1,3	3,1
Телефонный радиомикрофон- конденсатор, 20х14х10 мм, f=93 МГц, пластмасса	1,5	1,6	8	1	3,8
Радиомикрофон, 58х35х18 мм, L_a=35 мм, f=179,19 МГц, пластмасса	2	2,5	2,5	1,8	3,4
Радиомикрофон-бочонок, d=18 мм, h=27 мм, L_a=57 мм, пластмасса	0,7	1,1	1,1	0,44	1,1
Радиостетоскоп, 60х40х20 мм, l_a=49 мм, f=108 МГц, пластмасса	1,6	2	2	1,25	3,1

Основные выводы

1. Нелинейные локаторы полностью не решают задачу выявления закладок в помещении. Так, например, если закладка с дистанционным управ-

лением установлена в какой-либо электронной аппаратуре (телевизоре, телефонном аппарате и т. п.) и включается только во время проведения совещания, то она не может быть обнаружена нелинейным локатором при обследовании помещения перед переговорами, так как сигнал отклика от нее будет замаскирован откликом от аппаратуры, в которой она вмонтирована. Поэтому в комплекте с локатором всегда должен использоваться панорамный приемник того или иного типа. При этом весьма желательно, чтобы контроль несанкционированных излучений в помещении осуществлялся и во время совещаний.

2. При выборе нелинейного радиолокатора следует исходить из задач, поставленных перед группой контроля.

При работе *на открытых пространствах* целесообразно использовать импульсные локаторы большой мощности и наилучшей чувствительности. Это же относится и к обследованию в необорудованных помещениях, имеющих толстые стены.

При работе *в офисах* предпочтительно применять локаторы непрерывного излучения, в особенности те, которые позволяют контролировать процессы, происходящие в обнаруживаемых устройствах. Они не создают проблем по части электромагнитной совместимости и экологически безвредны. Среди непрерывных локаторов целесообразно использовать те, которые осуществляют прием сигнала одновременно на 2-й и 3-й гармониках, так как они значительно снижают нагрузку на оператора, сокращают время, требуемое на обследование, и позволяют избежать демонтажа строительных конструкций (что иногда необходимо при использовании локаторов, работающих на 2-й гармонике). Однако их цена почти вдвое выше, чем у локаторов, принимающих только на 2-ю гармонику.

3. Ряд ЗУ выполняется по МОП-технологии в экранированных корпусах. Поэтому их обнаружение даже с использованием нелинейных локаторов затруднено, так как уровень переизлученных сигналов на 2-й и 3-й гармониках незначителен. Для поиска таких ЗУ могут использоваться металлоискатели (металлодетекторы).

10.9. Некоторые рекомендации по поиску устройств негласного съема информации

Всю процедуру поиска можно условно разбить на несколько этапов:

- Подготовительный этап;
- Физический поиск и визуальный осмотр;
- Обнаружение радиозакладных 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 отличается уровень выявляемых устройств, который может колебаться от примитивных радиомикрофонов 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 постороннего человека, «забытого» документа или другим доступным способом.

3. *Оценку возможности доступа посторонних 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:*

- 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);
- Время поиска должно приходиться на рабочие часы, когда ЗУ активны;
- Должна быть обеспечена скрытность проводимых мероприятий – если есть необходимость ведения своей «контрразведывательной» игры, то следует помнить, что разговоры с коллегами и заказчиком, 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 является базой для любой поисковой методики. Будьте предельно внимательны, смотрите тщательно! Физический поиск и визуальный осмотр является важным элементом выявления средств негласного съема информации, особенно таких, как проводные и волоконно-оптические микрофоны, пассивные и полуактивные радиозакладные устройства, дистанционно управляемые «ждущие» устройства и другие технические средства, которые невозможно обнаружить с помощью обычной аппаратуры.

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 радиомикрофонов;
- Активизировать устройства, оснащенные системой VOX.

Источник «известного звука» не должен настораживать противоположную сторону, следовательно это может быть любой кассетный или CD-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 радиостанция 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.

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 ультрафиолетовые маркеры.

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

Обнаружение радиозакладных устройств

Процедура поиска начинается с формирования опорной панорамы, которая представляет из себя совокупность частот и амплитуд легальных источников (их амплитудных спектров). Она может строиться как в ручную, так и автоматически, так как практически все современные программно-аппаратные комплексы оснащены этой функцией. Частотная область, в которой будет осуществляться поиск радиозакладок ограничивается практически только возможностями применяемых приемников, но должна как минимум перекрывать диапазон 50-1000 МГц. Раздвигать эти границы шире, чем от 300 кГц до 10 000 МГц вряд ли целесообразно.

Однако надо помнить, что применение опорной панорамы может послужить и причиной серьезных ошибок, приводящих в конечном итоге к пропуску излучения радиозакладок. Поэтому при использовании априорной информации о загрузке эфира необходимо учитывать следующие факторы:

- опорная панорама должна строится на расстоянии от проверяемого помещения, существенно превышающем оперативную дальность приема излучения закладки (то есть на удалении не менее 2–3 км от контролируемого объекта), что позволит избежать ситуации, когда мощное ЗУ будет принято за легальный источник;
- существует целая серия ЗУ, специально маскируемых под вещательные станции или устройства сотовой связи и работающих с небольшой отстройкой от них по частоте.

В качестве примерной последовательности производимых действий по выявлению радиозакладок можно порекомендовать следующий порядок.

1. Разместите прибор в центре контролируемого помещения, установите антенну, оденьте наушники.

2. Установите регулировки в такое положение, чтобы индикаторный прибор показывал среднее значение.

3. Выключите все приборы и свет в зоне контроля и близ нее и посмотрите, не изменились ли показания индикатора. Иногда обычная флуоресцентная лампа создает очень сильное радиоизлучение, в таком случае она должна быть выключена или удалена из комнаты. Если изменения в показаниях ин-

дикатора не могут быть вызваны такими явными причинами, то это означает реальное подозрение на «жучок».

4. Повращайте антенну в вертикальной и (или) горизонтальной плоскости (в зависимости от ее вида). Следите за показаниями индикатора, они будут меняться в зависимости от положения антенны.

5. Выделите направление с максимальным уровнем подозрительного излучения. Идентификацию подозрительного сигнала как излучения радиозакладки проводите в соответствии с возможностями вашей аппаратуры. Это может быть:

- Прием переизлученного «известного звука» (тестового сигнала);
- Изменение в опорной панораме;
- Наличие большого уровня гармоник;
- Резкое изменение уровня при перемещении антенны и т. п.

6. Обследуйте все объекты, в которых могут быть спрятаны радиозакладки, например, с помощью индикатора поля, сканирующего приемника, программно-аппаратного комплекса.

Примечание: иногда обнаруживается ложный источник сигнала, «висящий» где-то в воздухе, это значит, что реальный источник рядом. Продолжайте поиск.

7. После обнаружения сигнала радиозакладки следует локализовать зону с повышенным уровнем этого излучения, отслеживая его по индикатору. Для этой процедуры применяется «ходьба по кругу», которая позволяет очертить «горячую» зону.

Нельзя прерывать режим скрытности после обнаружения «жучка», так как ЗУ может быть несколько. Это делается для улучшения качества приема и резервирования. Если противоположная сторона знает о ваших подозрениях на прослушивание, то она может специально поставить одну или несколько легко обнаруживаемых «закладок», чтобы убедить вас в успехе проведенного поиска и прекратить дальнейшие усилия. Если «закладка» оснащена приемником сигналов дистанционного управления, то нарушение режима скрытности приведет к немедленному отключению устройства, а следовательно, к усложнению поиска и, возможно, снижению его эффективности.

В некоторых случаях увеличение уровня принимаемого подозрительного сигнала связано с приближением не к истинному, а к мнимому источнику, что может быть следствием, например, явления интерференции. Характерным признаком излучений скрытоустановленных *телевизионных камер* является изменение характеристик принимаемого сигнала при изменении уровня освещенности (включения/выключения света в помещении).

Проверка элементов *телефонных линий* на наличие излучений радиозакладок, как правило, осуществляется по изменению уровня сигнала на входе

приемника контроля в момент поднятия трубки. Если в линии установлена радиозакладное устройство, то процесс поднятия трубки сопровождается существенным изменением уровня принимаемого излучения, кроме того в наушниках прослушивается тональный сигнал номеронабирателя либо другой тестовый сигнал. В «чистой» линии имеет место только кратковременный скачок излучения в момент поднятия трубки (в наушниках слышен короткий щелчок), а тональный набор не прослушивается.

Для обеспечения благоприятных условий проверки целесообразно антенну приемника контроля держать как можно ближе к элементам телефонной сети – проводу, аппарату, трубке, распределительной коробке и т. д., последовательно перемещая ее от одной точки контроля к другой.

Однако не всегда наличие теста в радиосигнале свидетельствует о работе подслушивающих устройств. Вполне возможно, что причиной являются и паразитные электромагнитные излучения (ПЭМИ) самого телефонного аппарата, связанные с эффектом самовозбуждения его усилительных каскадов. Для выявления физической природы обнаруженных излучений целесообразно использовать приемные устройства с частотным диапазоном 10 кГц-30 МГц, так как именно в нем сосредоточена наибольшая мощность ПЭМИ. При этом необходимо контролировать не только электрическую, но и магнитную составляющую поля. Для этого могут быть использованы специальные электрические (например, HE 010, HE 013/015, HFH 2Z1), магнитные (HFH 2-Z3, HFH 2-Z2) или комбинированные (FMA-11) антенны.

Наличие радиозакладных устройств с непосредственным подключением к телефонной линии эффективно можно обнаруживать и с использованием стандартных анализаторов телефонных линий. Единственное неудобство – необходимость предварительного обесточивания проверяемой линии.

В *автомобиле* наряду с обычными радиомикрофонами могут быть установлены и так называемые «бамперные жучки» – специальные технические средства для слежения за перемещением автомобиля с выходной мощностью 100 мВт-5 Вт в импульсном режиме.

Поэтому выявление возможно внедренных устройств должно начинаться с их активизации. С этой целью необходимо:

- разместить в салоне источник «известного звука» (тестового сигнала), так как оба вида ЗУ могут быть снабжены системами VOX;
- воссоздать условия, соответствующие реальной эксплуатации – автомобиль нужно завести, разогнать, затормозить и т. д.

И тогда по изменению уровня фона на удалении нескольких метров от транспортного средства можно сделать вывод о наличии ЗУ.

Выявление технических средств с передачей информации по токоведущим линиям

Выявление технических средств с передачей информации по токоведущим линиям осуществляется с использованием специальных адаптеров, позволяющих подключаться к различным линиям, в том числе и находящихся под напряжением до 300–400 В.

Поиск необходимо производить в частотном диапазоне 50-300 кГц. Это обусловлено тем, что, с одной стороны, на частотах ниже 50 кГц в сетях электропитания относительно высок уровень помех от бытовой техники и промышленного оборудования, а с другой – на частотах выше 300 кГц существенно затухание сигнала в линии, и, кроме того, провода начинают работать как антенны, излучающие сигнал в окружающее пространство, поэтому устройства с частотами передачи 300 кГц и выше будут выявлены на этапе поиска радиозакладок.

К сожалению, некоторое оборудование, питаемое от сети, может производить характерный низкочастотный шум, который может быть принят за искомый сигнал «жучка», поэтому необходимо по очереди отключать все питаемые устройства, чтобы определить источник такого шума.

Примечание: регуляторы освещенности и дефектные флуоресцентные лампы также могут давать низкочастотный шум, который может быть устранен удалением такой лампы или выставлением регулятора на максимум. Применение полосового фильтра звукового диапазона также поможет уменьшить уровень шума. *Однако простое выключение шумящей цепи недопустимо, так как этим можно выключить и закладное устройство!*

Обнаружение ЗУ с передачей информации по ИК-каналу

Использование ИК-канала является хотя и редким, но все же достаточно реальным способом передачи информации от ЗУ, поэтому исключать его применения нельзя.

Источником излучения является ИК- или лазерный диоды с узким пучком. Размещаются они либо напротив оконных проемов внутри контролируемых помещений, либо на наружной стороне зданий.

Наиболее надежный способ их выявления – физический поиск. Если же последний ничего не дал, то нужно использовать поисковую технику со специальными ИК-датчиками. Поиск излучений от таких ЗУ лучше всего осуществлять с наружной стороны здания. Особое внимание при этом уделяется окнам.

Проверка наличия акустических каналов утечки информации

Иногда ответственные за безопасность так поглощены поиском хитроумных жучков, что упускают из вида такие каналы утечки, как элементарное подслушивание за стеной. Звук может распространяться наружу через окна, стены, водопроводные трубы, полости в здании и т. д. и улавливаться микрофонами за пределами охраняемого помещения. Поэтому при проведении физического поиска обязательно проверяются вентиляционные и кабельные каналы на возможность прослушивания, а также на наличие в них вынесенных микрофонов, соединенных проводами со звукозаписывающей аппаратурой. В случае необходимости проводится полная акустическая проверка контролируемого помещения.

11. ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

11.1. Защита информации в сетях связи

Известна цитата из американской книги «Шпионаж особого рода»: «Питер Карлоу был техническим экспертом ЦРУ, и ему были знакомы признаки того, что телефон прослушивается. Сигнал после набора номера поступал с задержкой, потому что подслушивающее устройство требовало дополнительного отвода из линии. С телефоном – было не все в порядке…» Если делать подобные выводы в России, то очень легко можно попасть впросак, ибо довольно часто это не соответствует действительности. Как правило, главная причина появления подобного феномена – низкое качество отечественных телефонных каналов связи. Вместе с тем, хотя и нельзя принимать категорическое решение, ориентируясь «на слух», но использование некоторых организационных мер защиты, предложенные в этой книге, в любом случае будет для вас очень полезно.

Дополнительные организационные меры для защиты информации в телефонных линиях связи

Необходимо, прежде всего, определить порядок ведения деловых бесед по телефону, узаконить круг лиц, допускаемых к тем или иным внутрифирменным секретам, запретить сотрудникам вести служебные переговоры с домашних телефонов. Для передачи особенно важных материалов, использовать только устойчивые сети связи (каналы ФАПСИ, МО, «Исток»), а также скремблеры. Если вы почувствовали, что за вами установлен контроль, то можно использовать во время беседы систему условностей и сознательную дезинформацию. Не рекомендуется называть фамилию и отчество собеседника, если это позволяет этикет. Назначая место и время встречи, лучше переходить на условности (например, пункт № 2 и т. д.), которые должны быть заранее оговорены и органически вписываться в контекст вашего разговора. Эзопов язык должен быть знаком всем сотрудникам фирмы. Правда, как показала практика, система подобного «кодирования» информации не сможет продержаться достаточно долго.

Рекомендуется приучить к определенному порядку ведения телефонных переговоров и членов семьи: они не должны сообщать кому бы то ни было информацию о том, где вы находитесь и когда вернетесь домой. При шантаже со стороны преступных групп не следует звонить со своего телефонного аппарата, чтобы сообщить об этом в милицию и т. д. Лучше это сделать с телефона-автомата, от соседей и друзей. Надо учитывать, что в маленьких городах телефонные аппараты милиции и органов безопасности могут прослушиваться преступными группировками. В этом случае необходимо, чтобы

позвонил ваш друг или коллега и, не называя истинной причины, организовал встречу или беседу с представителями данных организаций.

Для защиты телефонных каналов связи необходимо, чтобы распределительная коробка (РК) телефонов фирмы обязательно находилась в помещении офиса и контролировалась службой безопасности или охраной. В случае, если данное требование совершенно невыполнимо, то желательно установить ее в закрывающемся на замок металлическом ящике, оборудованном сигнализацией. Для ремонта телефонных аппаратов целесообразно приглашать только проверенных специалистов. Желательно заключить договор со специализированной организацией, которая могла бы периодически проводить проверки вашей аппаратуры и линий связи.

Если вы не знакомы с мастером узла связи, собирающимся ремонтировать телефоны в вашем офисе или просто проверить РК, не поленитесь, попросите у него служебное удостоверение, позвоните на узел связи и удостоверьтесь, что там действительно работает такой специалист и что именно он получал наряд на работу в вашей фирме. Если данные не подтвердились, срочно принимайте меры. В первую очередь вызовите бригаду для проверки линии и аппаратов. Усильте работу службы безопасности и охраны. Для передачи информации перейдите на запасные каналы связи, в том числе факс, телекс, телеграф.

Все перечисленные меры в значительной мере снижают риск потери информации, однако, не дают полной гарантии и даже могут привести к целому ряду дополнительных сложностей в текущей деятельности, если они в дальнейшем не подкреплены техническими мероприятиями.

В крупных организациях имеет смысл создавать собственные службы безопасности (СБ), на которые, в числе прочего, нужно возложить и проблемы защиты телефонной связи. Технический отдел СБ в первую очередь должен будет провести следующие основные мероприятия:

- Оценить состояние системы связи (состав, технические характеристики, наличие схем прокладки и т. д.);
- Оценить степень конфиденциальности информации, циркулирующей по каналам связи;
- Оценить уровень угрозы безопасности со стороны конкурентов, преступников, разведок и т. д.;
- Выявить и оценить степень опасности всех каналов утечки информации через технические средства;
- Организовать взаимодействие с соседними (по зданию) фирмами, правоохранительными органами, учреждениями связи, специализированными организациями по защите информации, имеющими соответствующие лицензии на данный вид деятельности;

- Изучить законодательные и иные документы по защите информации в сетях телефонной связи;
- Провести анализ доступных средств защиты этих сетей; приобрести и установить технические средства защиты информации;
- Провести обучение персонала по применению этой спецтехники;
- Осуществлять постоянный контроль за эффективностью принятых защитных мероприятий;
- Проводить распределение между пользователями необходимых реквизитов защиты (например, паролей или скремблеров) и т. д.

Из этого, далеко неполного, перечня видно, что организационные меры необходимо дополнить и проведением комплекса технических мероприятий по защите линий телефонной связи.

Технические средства и методы защиты

Обнаружение подслушивающих устройств всегда начинается с внешнего осмотра телефонных линий и телефонного аппарата (ТА) с применением способов и средств. Однако эта проверка, как правило, возможна только на участке от аппарата до РК. Контроль в остальных зонах практически невозможен без привлечения служащих АТС. Впрочем, в связи с тем, что подключения чаще всего и осуществляются в зоне ТА–РК, то обнаружение подслушивающих устройств или следов их применения при должном внимании к мелочам более чем вероятно.

При проведении осмотра обязательно производится разборка ТА и телефонных розеток. На рис. 161 показан внешний вид «жучка» английского производства, вмонтированного в ТА. Устройство такого рода может устанавливаться в считанные секунды и используется в тех случаях, когда нет времени для более основательного внедрения. Думаем, не надо быть специалистом по связи, чтобы сообразить, что в телефоне находится посторонний объект.

Дальнейшие действия по обеспечению защиты информации, циркулирующей в телефонных линиях связи, требуют наличия специальной аппаратуры, которую по принципу действия можно разделить на группы.

Аппаратура контроля линий связи:

- Индикаторные устройства;
- Анализаторы проводных линий и кабельные локаторы (последние, соответственно, делятся на два типа: рефлектометры и устройства, использующие принципы нелинейной локации);
- Детекторы поля, специальные радиоприемные устройства и универсальные комплексы контроля.

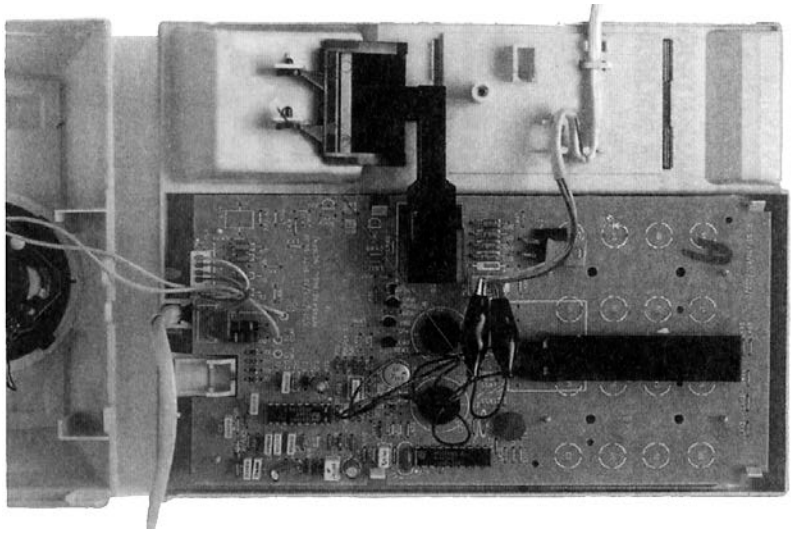

Рис. 161. Устройство негласного съёма информации, установленное в телефонном аппарате

Аппаратура защиты:

- Многофункциональные устройства защиты телефонных линий;
- Устройства уничтожения «закладок»;
- Устройства защиты от пиратского подключения;
- Аппаратура линейного и пространственного зашумления;
- Аппаратура кодирования информации;
- Аппаратура защиты от ВЧ-навязывания.

Детекторы поля, частотомеры, специальные радиоприемные устройства и универсальные комплексы контроля различной сложности применяются для обнаружения излучений радиозакладок, установленных в линиях связи. Принцип их действия и порядок работы были рассмотрены выше. Аппаратура линейного и пространственного зашумления, аппаратура кодирования информации и аппаратура защиты от ВЧ-навязывания и остальные виды перечисленных технических средств будут рассмотрены ниже.

11.2. Аппаратура контроля линий связи

Главный недостаток многих видов проверок – их периодичность, что не всегда соответствует требованиям гарантии безопасности. Одна из реальных возможностей обеспечения постоянного контроля за телефонной линией – применение специальных индикаторных устройств.

Индикаторные устройства

Простейшим *индикатором* наличия подслушивающих устройств, вполне доступным по цене $30 и работающим достаточно надежно, является уст-

ройство типа **ЛСТ-1007**, обычно называемое «*Телефонный страж*» (рис. 162).

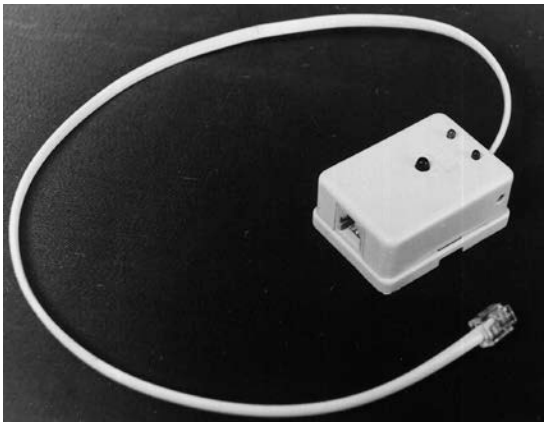

Рис. 162. Телефонный страж, ЛСТ-1007

Данное устройство устанавливается на предварительно проверенной телефонной линии и настраивается с учетом ее параметров. Питание осуществляется от самой линии. При подключении любых несанкционированных устройств, которые тоже питаются от телефонной сети (например, аппаратура с непосредственным включением), подается сигнал тревоги (загорается красная лампочка).

Зарубежным аналогом **ЛСТ-1007** является устройство типа **ST1**. Дополнительно к световому на нем установлен и стрелочный индикатор (вольтметр), по степени отклонения стрелки которого (в красный сектор) и принимается окончательное решение о наличии подслушивающих устройств на линии либо об очередном броске параметров сигнала АТС.

Схема простейшего индикатора, который легко сможет сделать радиолюбитель средней квалификации, приведена на рис. 163.

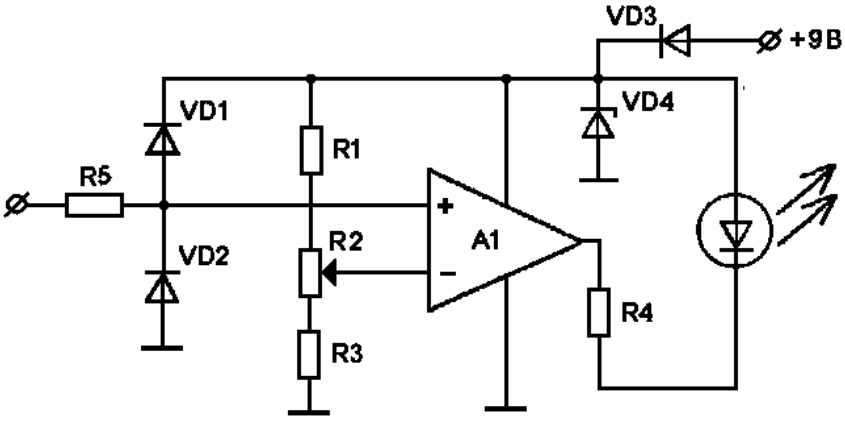

Рис. 163. Простейшее индикаторное устройство подключения к телефонной линии

Анализаторы проводных линий

Для проведения углубленных исследований телефонных линий на предмет обнаружения несанкционированных подключений подслушивающих устройств используется более серьезная аппаратура, эффективная работа с которой доступна только специалистам. Это анализаторы телефонных линий и кабельные локаторы.

Телефонный анализатор в простейшем виде представляет собой комбинацию мультимера и прибора, позволяющего обнаруживать переделки в телефонном аппарате. С помощью мультимера отмечаются отклонения от нормальных значений ряда параметров (например, напряжения) абонентской линии связи при снятой и положенной телефонной трубке. Повышенное или пониженное по сравнению со стандартным значением напряжение или сопротивление может означать, соответственно, параллельное или последовательное подключение подслушивающих устройств. Существуют анализаторы, способные инициировать работу и тем самым выявлять подслушивающие устройства, приводимые в действие от сигнала вызова.

Один из типичных представителей данного класса приборов – **CCTA-1000** – портативный анализатор фирмы CCS Communication Control (см. рис. 164).

Рис. 164. Анализатор телефонных линий CCTA-1000

Он позволяет проводить 6 типов контрольных проверок телефонных линий с целью выявления факта подключения подслушивающих устройств, магнитофонов или дополнительных телефонных аппаратов.

В ходе этой операции телефонный разъем подключается к гнезду анализатора, а инструкции (последовательность действий) по проведению самой проверки и ее результаты высвечиваются на двухстрочном 80-знаковом индикаторе, вмонтированном в верхнюю панель прибора. Анализатор осуществляет измерение напряжения, емкости, тока и сопротивления линии в автоматическом и ручном режимах.

В приборе предусмотрена также антенна для выявления подслушивающих устройств с радиопередатчиками (радиозакладок). Анализатор может быть использован для одновременной проверки 25 телефонных пар. Оформлен он в виде стандартного кейса. Вес – 6,8 кг. Питание – от сети 220 В. Цена – порядка $18 000.

Кабельные локаторы

Кабельные локаторы, как было отмечено выше, бывают двух основных типов: рефлектометры; устройства, использующие принципы нелинейной локации.

Рефлектометр (или «кабельный радар») позволяет определять расстояние до подозрительного места в телефонной линии. Принцип его действия основан на том, что в линию посылается импульс, который отражается от неоднородностей сети, возникающих в местах параллельного и последовательного подключения к ней различных дополнительных устройств. Расстояние до места подключения определяется по положению отраженного импульса на экране электронно-лучевой трубки, зависящему от времени задержки отраженного импульса.

В России существует целая серия подобной аппаратуры – это так называемые импульсные испытатели кабельных линий: **Р5-1А**, **Р5-5**, **Р5-8**, **Р5-9**, **Р5-10**, **Р5-11, Р5-13**, **Р5-13/1**, **ИКЛ-5**. Эти приборы были разработаны для определения расстояний до мест повреждения линий связи (обрыв, короткое замыкание, пробой между жилами и т. п.), но нашли применение и как средства поиска сетевых закладных устройств. Рассмотрим некоторые из них.

Р5-9 – измеритель неоднородности кабеля. В приборе имеется три диапазона измеряемых расстояний: до 100 м; до 1000 м; до 10000 м. Погрешность измерения составляет ±1 % от предельного значения диапазона. Длительность зондирующего импульса выбирается из следующей совокупности значений – 10, 30, 100, 500, 2000 нс. Амплитуда зондирующего сигнала изменяется в пределах от 10 до 30 В. Габариты прибора составляют 213×310×455 мм, масса – не более 12,5 кг. Питание возможно как от сети 220 В, так и от

встроенного автономного источника (аккумуляторной батареи). Р5-9 может работать на кабелях различных типов с волновым сопротивлением 10-1000 Ом длиной до 10 км при максимальном затухании отраженного сигнала – 50 дБ. Разрешающая способность позволяет проводить измерения расстояния до неоднородности на отрезках кабелей длиной всего в 1-1,5 м. По форме, полярности и относительной величине отражения импульсов можно оценить характер неоднородностей и прикинуть их величину (изменение размера сечения, параметров диэлектрического заполнения и т. д.).

Р5-13 – измеритель неоднородностей телефонных линий. Отличается улучшенными эксплуатационно-техническими характеристиками и большим удобством в работе. Его вес – всего 9 кг, а габариты – 120×304×350 мм.

В России используется и аналогичная зарубежная аппаратура.

«Дигифлекс Т12/3» – импульсный эхометр (Германия). По своим техническим возможностям он существенно не отличается от отечественных аналогов, однако сервисные функции значительно лучше (главное – возможность подключения персонального компьютера, что позволяет производить сравнительные замеры, а также осуществлять распечатку на принтере результатов контроля).

Основные технические характеристики «Дигифлекс Т12/3»

Диапазон измерений, км:.....0,5; 1; 2,5; 10, 20;
Динамический диапазон:.....более 90 дБ;
Память, рефлексограмм:.....10;
Длительность импульсов, нс: 50, 100, 200, 500, 1000, 2000;
Дисплей: Контрастный жидкокристаллический с разрешением 128×256;
Габариты, мм: 255×155×250.

Системы, производящие анализ телефонной линии на основе принципов нелинейной локации, не получили широкого распространения в связи со сложностью работы и неоднозначностью получаемых результатов. Кроме того, уровень зондирующих сигналов, используемых в этих устройствах, составляет 50-300 В, что недопустимо много для большинства элементов телефонных сетей.

Производители утверждают, что дальность обнаружения неоднородностей такими устройствами достигает 5000 м, но на самом деле измеряемое расстояние существенно меньше (реально – до 100 м). Приведем параметры некоторых подобных приборов.

LBD-50 – анализатор проводных линий. Предназначен для анализа параметров любых проводных линий с целью выявления несанкционированных подключений устройств негласного съема информации (рис. 165). В основу работы прибора положен метод нелинейной локации.

Рис. 165. Анализатор проводных линий LBD-50

Прибор позволяет исследовать переходные процессы в линиях и проводить «традиционные» измерения: величины тока, сопротивления утечки и т. п. Он может быть подключен к электросети без отключения напряжения. В комплект анализатора включено устройство для бесконтактного определения противоположного конца анализируемой линии и поиска ее в жгуте проводов.

Основные технические характеристики LBD-50

Диапазон измерения токов утечки: ..... 0,1-200 мА;
Диапазон измерения сопротивления изоляции: 100 кОм - 20 Мом;
Дальность фиксации тестового сигнала в линии: до 1см;
Питание от сети переменного тока: ..... 220 ± 20 В, 50 Гц.

ВИЗИР – низкочастотный нелинейный детектор проводных коммуникаций. Предназначен для обнаружения средств подслушивания, подключенных к проводным коммуникациям (как силовым, так и слаботочным) с целью съема и передачи информации, а также к цепям питания таких устройств. Принцип действия прибора заключается в подаче в линию зондирующего синусоидального сигнала и регистрации высших гармоник тока, возникающих в полупроводниковых элементах подключенного к линии средства прослушивания. Анализ наличия высших гармоник проводится оператором визуально путем наблюдения изображения на жидкокристаллическом экране прибора.

Основные технические характеристики ВИЗИР

Индикация обнаружения: ..... Визуальная;

Мощность постоянного тока в нагрузке
блока питания обнаруживаемого средства:. Не менее 1 мВт;
Сопротивление подключенной параллельно
к обследуемой линии согласующей цепи
обнаруживаемого устройства..... Не более 1 Мом;
Сопротивление подключенной последовательно
к обследуемой линии согласующей цепи
обнаруживаемого устройства: ..... Не менее 100 Ом;
Длина обследуемых линий:..... Не более 1000 м;
Напряжение зондирующего сигнала:..... 220 В, 50 В;
Частота зондирующего сигнала:..... 50 Гц;
Время задержки подачи зондирующего сигнала в линию: 20 мс;
Напряжение питания:..... 220 В, 50 Гц.

11.3. Аппаратура защиты линий связи

Многофункциональные устройства индивидуальной защиты телефонных линий

На практике разработаны и широко используются специальные схемы предотвращения прослушивания помещений через телефонные аппараты. Так, на рис. 166 показана простая, но очень эффективная схема подавления слабых информационных сигналов, возникающих в звонковой катушке, при воздействии на нее акустических волн (эффект акусто-электрического преобразования).

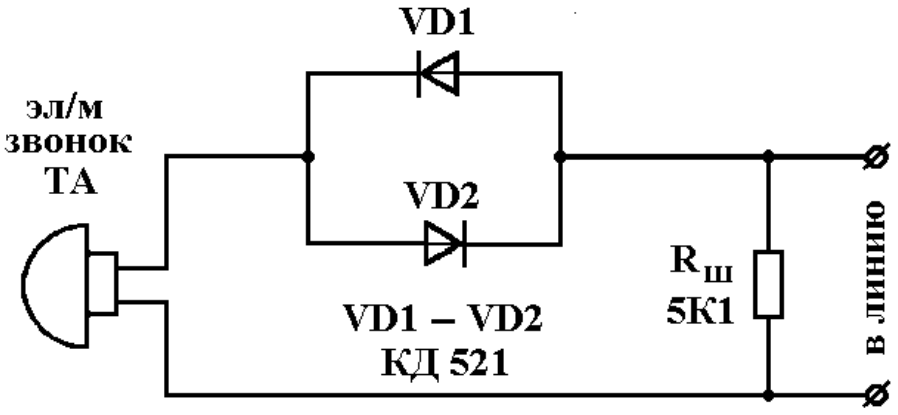

Рис. 166. Простейшая схема защиты телефонного аппарата

Здесь два кремниевых диода, включенных по схеме варистора, образуют зону нечувствительности для малых паразитных токов, возникающих в

обмотке катушки (упрощенная вольт-амперная характеристика диодов приведена на рис. 167).

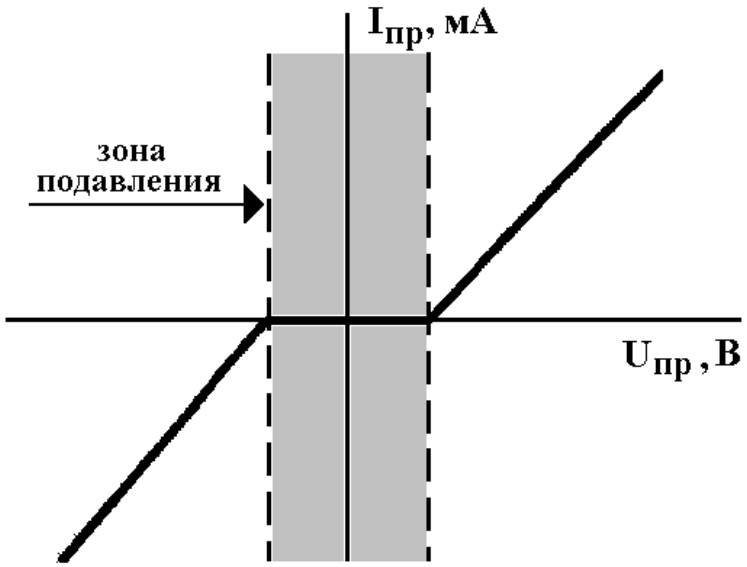

Рис. 167. Упрощенная вольт-амперная характеристика встречновключенных полупроводниковых диодов

В то же время речевой сигнал абонента и напряжение вызова телефонного аппарата свободно «проходят» через диоды, так как их амплитуда значительно превышает порог нечувствительности этих элементов (0,3–0,5 В). Резистор *Rш* является дополнительным шунтирующим элементом. Подобная схема, включенная последовательно, уменьшает ток в линии, который вызван наводимой в катушке ЭДС, на 40-50 дБ.

Наиболее распространенным серийным устройством защиты, работающим по этому принципу, является изделие типа «**Гранит-VIII**», которое обладает техническими характеристиками, приведенными в табл. 26.

Таблица 26.

Характеристики	Значения
Затухание в полосе частот 0,15-10 кГц при уровне входного сигнала 10 В, не более, дБ	3
Затухание при входном напряжении 10 В на частоте 50 кГц, не менее, дБ	6
Габариты, мм	95×60×25
Вес, кг	0,2

Значительное распространение получили аналоги **«Гранита-VIII»**, выпускаемые различными производителями: «**Утес-ТА**», «**Обрыв**», **ТА-1**, **ТА-2**, **ТФ** и др.

Небольшая доработка вышеприведенного устройства позволяет защитить ваш телефон и от прослушивания с использованием метода ВЧ-навязывания.

Так как объектом ВЧ-воздействия является микрофон ТА, то достаточно подключить параллельно микрофону конденсатор емкостью 0,01-0,05 мкФ. При этом данный конденсатор шунтирует по высокочастотной составляющей микрофонную капсулу, глубина модуляции навязываемого излучения уменьшается более чем в 10 тысяч раз, что практически делает невозможным извлечение из него информации.

На рис. 168 приведен еще один вариант схемы защиты. Ее основное отличие заключается в использовании двух пар кремниевых диодов, шунтирующих конденсаторов и дополнительных катушек индуктивности. Элементы *L* и *C* здесь являются дополнительным фильтром ВЧ-сигналов. Эта схема обеспечивает одновременно эффективную защиту от обоих вышеперечисленных способов прослушивания.

Существует целый ряд и достаточно сложных индивидуальных устройств защиты ТА, выполняющих следующие функции:

- изменения напряжения в линии, приводящего к отключению диктофонов с системой автоматического включения при снятии трубки и других устройств, которые используют для работы напряжение телефонной линии;
- генерации маскирующей речь помехи, которая не мешает разговору, поскольку автоматически фильтруется на всех АТС, зато те, кто подключился на линию до станции будут слышать только громкое шипение;
- защиты ТА от попыток модификации с целью использования его для прослушивания помещения.

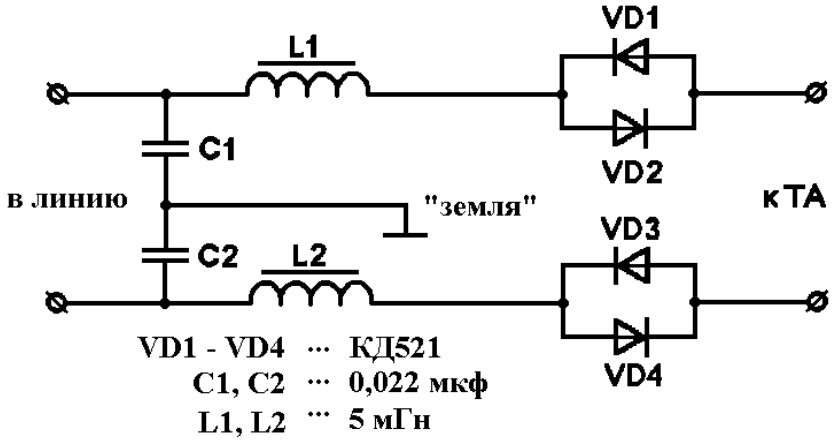

Рис. 168. Схема защиты телефонного аппарата от прослушивания за счет эффектов акусто-электрического преобразования и ВЧ-навязывания

Phone Guard 2 – устройство индивидуальной защиты. Имеет три основных режима работы.

- *Режим 1*. Самый простой режим, в котором «телефонный страж» обнаруживает только факт непосредственного подключения к линии подслушивающих устройств с низким сопротивлением, а также параллельное включение постороннего телефона. Как только вы снимете трубку, загорается красный индикатор «PRIV». Пока горит этот индикатор – разговор безопасен. Если произойдет параллельное подключение, индикатор гаснет, а разговор прерывается автоматически.
- *Режим 2*. В данном режиме производится регистрация излучений радиопередатчиков, находящихся в непосредственной близости от телефонного аппарата, если их работа совпадает по времени с вашим разговором.
- *Режим 3*. «Телефонный страж» может нейтрализовать некоторые виды подслушивающих устройств (например, телефонные диктофоны с автоматическим включением записи при снятии трубки).

NG-303 – устройство защиты от утечки информации. Выполняет функции по защите телефонных линий от прослушивания переговоров с использованием различных средств негласного съема информации, а также защите электросетей переменного тока 220 В 50 Гц от несанкционированного их использования для передачи речевой информации (аналогично изделию **NG-401**).

В отличие от предыдущих подобных моделей в этом устройстве реализована возможность сигнализации о пиратском подключении к телефонной линии и блокировки несанкционированно подключенного параллельного телефонного аппарата. Еще одним достоинством является простота настройки изделия.

Фактически это комплекс, состоящий из свипирующего генератора для защиты электросети, а также ряда независимых генераторов для зашумления телефонных линий. В нем используются следующие виды излучений:

- синфазная помеха в виде сложного шумоподобного сигнала с цифровым формированием (М-последовательность) в звуковом (100 Гц – 10 кГц) диапазоне частот;
- парафазная помеха с цифровым формированием (М-последовательность), обеспечивающая подавление радиозакладных устройств в диапазоне частот 30 кГц - 650 МГц.

Устройство обеспечивает эффективное противодействие следующим средствам негласного съема информации:

- микрофонам, использующим для передачи информации электросеть 220 В;

- радиопередатчикам, включаемым в телефонную линию как непосредственно (последовательно и параллельно), так и индукционным способом;
- аппаратуре магнитной записи, подключаемой к телефонной линии с помощью контактных или индукционных датчиков;
- телефонным аппаратам, факсам, модемам, негласно подключаемым к телефонной линии.

Основные технические характеристики NG-303

Гарантированная полоса защиты сигнала .	80–5000 кГц
Мощность сигнала защиты.....	5 Вт
Отношение сигнал/шум в устройстве прослушивания телефонного канала, не хуже	20 дБ
Отношение сигнал/шум в телефонном аппарате	Не менее 14 дБ
Габаритные размеры	205×60×155 мм
Питание	220 В

Shark – модуль защиты телефонной линии. Предназначен для противодействия несанкционированному съему информации как во время разговора, так и при положенной трубке.

Основные технические характеристики Shark

Регулировка тока в линии в режиме разговора	30–7 мА
Шумовая помеха в виде псевдослучайной последовательности с ограничением спектра в полосе	8–25 кГц
Напряжение шумовой помехи	до 25 В
Потребляемая мощность.....	10 Вт
Напряжение питания.....	220 В
Включение и регулировка защитных функций	Ручная

SI-2001 – 4-канальный прибор защиты телефонных линий. Предназначен для защиты переговоров по телефонным линиям (до четырех одновременно) от утечки информации. Принцип действия основан на маскировке спектра речи широкополосным специальным сигналом. Позволяет защищать переговоры в линии от точки подключения к прибору до АТС и предназначен для эксплуатации как на городских, так и местных (внутренних) линиях.

Прибор обеспечивает эффективное противодействие:

- радиопередатчикам, включенным в линию последовательно и параллельно (в том числе с индукционными датчиками и внешним питанием);
- аппаратуре магнитной записи, подключаемой к линии с помощью контактных или индукционных датчиков;
- параллельным ТА и аналогичной аппаратуре;
- аппаратуре ВЧ-навязывания;

- аппаратуре, использующей линию в качестве канала передачи или источника электропитания.

Прибор обеспечивает защиту линии как при поднятой, так и при положенной трубке вашего ТА.

Основные технические характеристики SI-2001

Количество каналов прибора (количество защищаемых линий) 4
Полоса пропускания каналов № 1–3 ..... 1,5 кГц
канала № 4 ..... 3 кГц
Максимальное значение спецсигнала,
генерируемого прибором по линии ..... 3 В
Отношение напряжения спецсигнала, генерируемого прибором
по линии, к напряжению спецсигнала на клеммах ТА:
в каналах № 1–3 ..... Не менее 50 дБ
в канале № 4 ..... Не менее 40 дБ
Переходное затухание между каналами прибора
в рабочем диапазоне частот ..... Не менее 100 дБ
Диапазон регулировки тока в линии ..... Не менее 5 мА
Электропитание ..... Сеть 220 В
Потребляемая мощность ..... Не более 30 Вт
Габаритные размеры ..... 170×280×60 мм
Масса ..... Не более 3 кг

SI-2020 – устройство защиты телефонных линий. Предназначено для защиты переговоров по телефонной линии от утечки информации и обеспечивает:

- модуляцию тока телефонной линии широкополосным спецсигналом;
- цифровую индикацию напряжения линии;
- возможность подключения аппаратуры магнитной записи для регистрации переговоров, проводимых по защищаемому ТА.

Прибор предназначен для эксплуатации на городских линиях (в том числе с электронными АТС и частотным уплотнением каналов); защищает переговоры по линии от ввода в прибор до АТС.

Обеспечивает эффективное противодействие следующим средствам несанкционированного съема информации:

- радиопередатчикам с питанием от линии, включенным в линию последовательно и параллельно;
- аппаратуре магнитной записи, подключаемой к линии с помощью контактных или индукционных датчиков;
- параллельным ТА и аналогичной аппаратуре;
- аппаратуре ВЧ-навязывания;

- аппаратуре, использующей линию в качестве канала передачи или источника электропитания.

Примеры противодействия:

- прибор активирует при положенной трубке ТА питающиеся от линии радиопередатчики, что облегчает их поиск (см. п. 2.3);
- прибор активирует при положенной трубке ТА диктофоны с целью холостого проматывания ленты;
- прибор обеспечивает защиту линии как при поднятой, так и при положенной трубке ТА.

Основные технические характеристики SI-2020

Максимальное значение спецсигнала,
генерируемого прибором по линии..... 40 В
Электропитание..... сеть 220 В
Потребляемая мощность от сети ..... Не более 2 Вт
Габаритные размеры ..... 95×135×45 мм
Масса ..... Не более 0,3 кг
Время непрерывной работы ..... Не ограничено

SPRUT – электронный модуль. Предназначен для защиты проводных телефонных линий от подключения различных устройств съема информации (параллельных телефонов, трубок, индукционных и емкостных съемников, диктофонов, телефонных активаторов, радиопередатчиков). Кроме того, делает неэффективной работу микрофонов, использующих для передачи информации телефонную линию при положенной трубке.

В модуле реализованы следующие защитные функции:

- постоянный контроль телефонной линии на разрыв со звуковой и визуальной индикацией;
- контроль за напряжением в телефонной линии как при положенной трубке, так и во время разговора;
- постановка заградительной шумовой помехи в случае подключения (в момент разговора) параллельного аппарата или аналогичной нагрузки;
- включение состояния «высокий уровень» в момент начала разговора (при этом формируется такой уровень сигнала, что нормальная работа возможна только для вашего аппарата);
- включение регулируемой помехи в телефонную линию во время разговора;
- постановка помехи в линию при положенной трубке.
- Модуль предназначен для работы на телефонных линиях, по своим параметрам соответствующих городским телефонным линиям. Полноцен-

ная работа возможна только по схеме: одна телефонная линия – один аппарат.

Основные технические характеристики SPRUT

Помеха	Модулированная по амплитуде псевдо-шумовой последовательностью
Несущая частота	45 кГц
Занимаемая полоса	100–3500 Гц
Повторение последовательности	через 24 ч
При положенной трубке несущая	12 кГц
Напряжение активной шумовой помехи	30 В
Порог срабатывания на параллельное подключение при положенной трубке	50 В
Порог срабатывания на аварийное падение напряжения в линии	5 В
Автоматической включение защитных функций после набора последней цифры номера	8 с
Точность измерения напряжения в линии	0,5 В
Соотношение сигнал/шум во время разговора	30 дБ
Потребляемая мощность	до 15 Вт
Габаритные размеры	60×155×198 мм

SPRUT-MINI – устройство защиты телефонных переговоров. Предназначено для защиты телефонных разговоров на участке «телефон – АТС» от следующих видов устройств несанкционированного съема информации:

- бесконтактных индуктивных и емкостных датчиков;
- радиопередающих устройств, подключаемых параллельно или последовательно;
- радиопередающих устройств акустического контроля помещения, работающих при опущенной трубке телефона;
- звукозаписывающих устройств (диктофоны и т. д.), подключаемых к телефонной линии;
- устройств акустического прослушивания помещения, передающих информацию по телефонной линии («телефонное ухо» и т. п.).

Препятствует нормальной работе параллельного ТА при попытке позвонить с него. Не требует установки такого же устройства у вашего абонента, то есть защищаются ваши телефонные переговоры с любым абонентом. Служит анализатором состояния телефонной линии и сигнализирует об активизации устройств типа «телефонное ухо», а также о непосредственном подключении подслушивающих устройств.

Основные технические характеристики SPRUT-MINI

Питание	Сеть 220 В

Напряжение телефонной линии..... 45–60 В
Потребляемая мощность..... 2 Вт
Габаритные размеры ..... 110×90×50 мм
Масса ..... Не более 500 г

TSU-3000 – устройство защиты телефонных линий. Предназначено для защиты телефонных линий от различных подслушивающих устройств, блокирует автопуски диктофонов, делает невозможным прослушивание с параллельного телефона, с телефонной трубки линейного монтера, подавляет работу телефонных радиозакладок, в том числе с индуктивным съемом информации. Действие прибора основано на размывании спектра речевого сигнала и уменьшении тока потребления в линии при разговоре, что снижает эффективность последовательно подключенных передатчиков.

Устройство позволяет подключить цифровой вольтметр для контроля изменений, происходящих в телефонной линии, отличается простотой эксплуатации. После включения требуемый режим устанавливается с помощью двух кнопок. Работа устройства контролируется автоматически с использованием светодиодных индикаторов. При разрыве телефонной линии или подключении к линии подслушивающего устройства подается звуковой и световой сигналы тревоги. Изделие позволяет прослушивать телефонную линию на наличие любых звуковых сигналов без снятия телефонной трубки. Не требует наличия аналогичного прибора у вашего абонента.

«БАРЬЕР-3» – устройство защиты телефонных переговоров. Предназначено для защиты телефонных переговоров на участке от ТА до АТС и обеспечивает:

- подавление подслушивающих устройств, подключенных к телефонной линии, вне зависимости от их типов и способов подключения (в том числе и с индуктивным съемом);
- подавление автоматических звукозаписывающих устройств, подключенных к телефонной линии и активируемых поднятием трубки;
- подавление звукозаписывающих устройств с ручным управлением записи;
- запуск диктофонов, активируемых голосом, при положенной трубке;
- защиту от ВЧ-навязывания и «микрофонного эффекта», позволяющих прослушивать акустику в помещении через ТА с положенной трубкой;
- блокирование работы микрофонов, работающих по телефонной линии;
- блокирование работы подключенного к телефонной линии параллельного ТА;
- цифровую индикацию напряжения телефонной линии и напряжения отсечки;

- возможность подключения к телефонной линии звукозаписывающей аппаратуры для архивации телефонных переговоров.

Основные технические характеристики «БАРЬЕР-3»

Защищаемый участок телефонной линии.. от ТА до АТС
Уровень маскирующего шума ..... до 40 В
Напряжение отсечки ..... до 50 В
Потребляемая мощность..... Не более 5 Вт
Напряжение питания..... 220 В, 50 Гц
Габаритные размеры ..... 220×110×50 мм

Комплект поставки: основной блок «БАРЬЕР-3»; сетевой шнур питания; телефонный шнур «евростандарт»; телефонный шнур с вилкой; телефонный шнур с розеткой; шнур соединительный к диктофону; пульт ДУ; кнопка ДУ.

«ПРОКРУСТ ПТЗ-003» – прибор защиты телефонной линии. Предназначен для защиты телефонных переговоров от прослушивания на участке от ТА до АТС. Защита осуществляется путем изменения параметров стандартных сигналов.

Изделие имеет цифровой дисплей – указатель напряжения на телефонной линии и световой индикатор снятия трубки. В нем предусмотрено три режима подавления («Уровень», «Шум», «ВЧ-помеха»), которые могут включаться независимо друг от друга, имеется возможность экстренного отключения всех режимов защиты, подключения диктофона для записи телефонных переговоров.

Режим «Уровень» позволяет поднимать напряжения в телефонной линии во время разговора. В режиме «Шум» в линию подается шумовой сигнал звукового диапазона частот при положенной на рычаг трубке. В режиме «ВЧ-помеха» в линию подается помеховый ВЧ-сигнал вне зависимости от положения трубки.

Основные технические характеристики«ПРОКРУСТ ПТЗ-003»

Максимальное поднятие постоянного напряжения
на линии в режиме «Уровень»..... до 35 В
Амплитуда «белого» шума в режиме «Шум» до 10 В
Диапазон шумового сигнала в режиме «Шум» 50 Гц-10 кГц
Максимальная амплитуда помехи в режиме «ВЧ-помеха» до 35 В
Напряжение на диктофонном выходе ..... 10 мВ
Питание ..... Сеть 220 В, 50 Гц
Потребляемая мощность..... Не более 10 Вт

«ПРОКРУСТ 2000» – телефонный модуль для комплексной защиты телефонной линии от прослушивания. Позволяет осуществлять обнаружение подключенных телефонных закладок и подавлять их путем постановки ак-

тивных помех. Предусмотрена защита помещений от прослушивания с использованием методов ВЧ-навязывания.

Прибор обеспечивает ложное срабатывание звукозаписывающей аппаратуры, снабженной системой VOX и подключенной в телефонную линию в любом месте от модуля до АТС (это приводит к непродуктивному расходу пленки и батарей питания звукозаписывающей аппаратуры).

Защитный модуль легко интегрируется в конфигурацию сети офисной мини-АТС. Предусмотрено временное отключение защиты для предотвращения сбоев при наборе номера.

Основные технические характеристики «ПРОКРУСТ 2000»

Габаритные размеры ..... 47×172×280 мм
Напряжение питания..... 220 В, 50 Гц
Максимальная потребляемая мощность.... до 10 Вт

«ПРОКРУСТ минипак» – прибор защиты телефонной линии. Предназначен для защиты городской телефонной линии от ТА до АТС. Он позволяет:

- подавлять работу различных типов телефонных радиозакладок, в том числе с автономным питанием и индуктивным способом подключения к линии (путем постановки активных помех);
- защищать ТА от ВЧ-навязывания;
- автоматически блокировать попытки прослушивания телефонного разговора с параллельного аппарата;
- подавлять нормальную работу звукозаписывающих устройств, подключенных к линии с помощью контактных или бесконтактных адаптеров;
- превентивно воздействовать на звукозаписывающую аппаратуру, оборудованную системой VOX с целью холостого сматывания пленки и вырабатывания заряда батарей питания.

Основные технические характеристики «ПРОКРУСТ минипак»

Габаритные размеры ..... 62×155×195 мм
Напряжение питания..... Сеть 220 В, 50 Гц
Максимальная потребляемая мощность . до 10 Вт

«ПРОТОН» – устройство комплексной защиты телефонной линии. Оно обладает следующими возможностями:

- визуальной и звуковой (отключаемой) индикацией о нарушении целостности телефонной линии (короткое замыкание, обрыв);
- цифровой индикацией постоянной составляющей напряжения в телефонной линии во всех режимах работы;
- развязкой ТА от телефонной линии при положенной трубке (питание осуществляется от отдельного стабилизированного внутреннего источ-

ника тока, что исключает использование резонирующих свойств электромагнитных вызывных устройств);

- постановкой шумовой помехи в звуковом диапазоне частот (отключаемой) в телефонную линию при положенной трубке (обеспечивает активацию диктофонов, препятствует прослушиванию помещения);
- автоматическим включением режима минимального тока в телефонной линии, без ухудшения качества связи, после набора номера абонента;
- обнаружения и противодействия попытке непосредственного прослушивания телефонной линии во время разговора (с параллельного аппарата, низкоомных наушников и др.).

Помимо перечисленных сложных универсальных устройств защиты существует целый ряд технических средств, предназначенных исключительно для линейного зашумления телефонных каналов передачи информации.

Устройства уничтожения закладок

Для практического решения задач защиты информации нашли применение устройства, получившие название «телефонные киллеры». Принцип их действия основан на подаче высоковольтного напряжения в телефонную линию. В результате уничтожаются все подключенные устройства. Средство действительно радикальное, но беда в том, что использование данной техники с отступлениями от инструкции по эксплуатации может привести к выводу из строя параллельно подключенных ТА, факсов, модемов, а также оборудования мини- и городской АТС. Приведем характеристики некоторых подобных устройств.

BUGROASTER – электронный модуль для уничтожения закладных устройств. Предназначен для физического уничтожения устройств несанкционированного съема информации, гальванически подключенных к телефонной линии. Генерирует серию коротких ВЧ-импульсов, приводящих к разрушению микросхем устройств, подключенных к телефонной линии. Прибор предназначен для зачистки линии в ближней зоне (на расстоянии не менее 200 м).

Применяется в двух основных режимах работы: линия отсоединена от АТС (в коммутационной коробке), провода разомкнуты; линия отсоединена от АТС, провода замкнуты накоротко.

Это позволяет уничтожать ЗУ, подключенные к линии как последовательно, так и параллельно.

Основные отличия от аналогов:

- возможность работы в ручном и автоматическом режимах;
- современный дизайн;
- наличие панели, отображающей информацию о работе прибора;

- специально сформированный электрический импульс, позволяющий более эффективно уничтожать устройства несанкционированного съема информации.

Основные технические характеристики BUGROASTER

Напряжение импульса	1500 В
Длительность импульса	400 мс
Время непрерывной работы в режиме «автомат»	10 мин
Напряжение питания	Сеть 220 В, 50 Гц
Габаритные размеры	60×155×198 мм

«КОБРА» – выжигатель телефонных закладных устройств. Предназначен для предотвращения прослушивания абонентских телефонных линий с помощью устройств несанкционированного доступа, установленных в телефонные линии с непосредственным параллельным или последовательным подключением. Принцип работы – электрическое уничтожение (прожигание).

Основные технические характеристики «КОБРА»

Напряжение на выходе	Не менее 1600 В
Время непрерывной работы в ручном режиме	10 мин
Время непрерывной работы в автоматическом режиме	20 с
Питание	Сеть 220 В, 50 Гц
Габаритные размеры	65×170×185 мм

КС-1300 – генератор импульсов. Предназначен для уничтожения подслушивающих устройств, установленных в телефонную линию.

Основные технические характеристики КС-1300

Количество подключаемых телефонных линий	2
Временные интервалы, устанавливаемые таймером	от 10 мин до 2 сут
Мощность «прожигающего» импульса.....	15 Вт
Время непрерывной работы в автоматическом режиме	24 ч
Электропитание	220 В, 50 Гц
Габаритные размеры	170×180×70 мм

Устройства защиты от пиратского подключения

Отдельная, но очень актуальная проблема – борьба с лицами, использующими незаконное подключение к телефонным сетям в корыстных целях, например, для междугородных звонков и звонков в дальнее зарубежье. С широким распространением радиотелефонов различного типа (от сотовых до элементарных домашних «радиоудлинителей») эта проблема еще больше обострилась.

Традиционно все способы противодействия пиратскому подключению можно разбить на две основные группы: организационные и технические (см. классификацию в табл. 27).

Таблица 27.

Организационные	Технические	
	Пассивные	Активные
1. Установка телефонов в месте, недоступном посторонним лицам. 2. Отключение выхода на межгород по заявке на АТС. 3. Регламентирование и контроль за использованием телефона на производстве 4. Контроль линии с опломбированием шкафов с распределительных щитков, ограничение доступа к шкафам и колодцам	1. Сигнализаторы подключения и обрыва линии 2. Счетчики времени разговора 3. Устройства контроля увеличения количества междугородных разговоров	1. Устройства защиты от параллельного подключения. 2. Устройства кодирования доступа к телефонной линии. 3. Программирование цифровых АТС на работу с номерным телефонным аппаратом. 4. Настройка «в резонанс» системы АТС-ТА по различным параметрам. 5. Блокираторы выхода на межгород. 6. Устройства, ограничения продолжительности разговоров

Под *организационными способами* понимается комплекс мер по регламентированию и контролю за использованием телефонной линии. Они проводятся как работниками линейных узлов связи, так и индивидуальными абонентами АТС. Особенно большой эффект от организационных мер получают предприятия и организации, на балансе которых имеется достаточно много городских телефонных линий.

Под *техническими способами* противодействия понимается применение специальных устройств защиты, ограничивающих возможности нелегальных абонентов по доступу к линиям связи.

По воздействию на телефонные линии технические способы подразделяются на пассивные и активные.

Пассивные устройства защиты предназначены для регистрации факта подключения и самовольного использования линии. Они не вмешиваются в процесс связи, а только помогают владельцу линии оперативно реагировать на начальный процесс возникновения факта самовольного использования.

Активные устройства защиты предусматривают вмешательство в процесс установления и проведения несанкционированной связи с целью предотвратить реальные финансовые затраты в случаях самовольного подключения.

Так, для защиты проводных линий разработан совмещенный индикатор подключения и обрыва линии, схема которого приведена на рис. 169.

Принцип работы схемы заключается в следующем. В исходном состоянии блок индикатора подключается параллельно используемому телефонному аппарату ТА. При наличии в линии напряжения свыше 40 В на входе элемента DD1.1 присутствует уровень логической единицы, и, в соответствии с этим, генератор частоты, равной 2,5 кГц, заперт.

При поступлении вызова с АТС амплитудой 100 В и частотой 25 Гц специально рассчитанная цепочка фильтра R3, C2 не позволяет переключить элемент DD1.2 и включить звуковой сигнал ЗП-3. Если же на каком-то участке линии была снята трубка (либо произошел обрыв) более чем на 1 с, на выходе DD1.1 появится нулевой уровень, и с указанной задержкой переключится DD1.2. Далее включится генератор 2,5 кГц, который подаст непрерывный звуковой сигнал о пиратском использовании или обрыве линии. При возвращении линии в исходное состояние (напряжение более 40 В) индикатор вновь переходит в ждущее состояние. Возможна доработка индикатора схемой на основе триггера для индикации попытки использования (обрыва) линии и после установления в линии номинального напряжения. Питание индикатора от встроенной батареи 9 В («Крона» или «Корунд»).

Благодаря высоким номиналам R1, R2, индикатор абсолютно не влияет на параметры линии (в соответствии с ГОСТом). Правда, к недостатку устройства можно отнести тот факт, что индикатор будет срабатывать при подъеме трубки (ведение разговора) и самим хозяином телефона, поэтому целесообразно установить дополнительный выключатель или выполнить индикатор в виде заглушки, подключаемой к розетке вместо ТА.

Кроме всех видов пиратских подключений на участке проводной связи, для *радиотелефонов* характерно подключение в зоне радиоканала. Количество жалоб на это постоянно возрастает. Службы АТС практически не готовы решать проблему противодействия пиратству на радиочастоте.

Однако «черный» рынок отреагировал появлением так называемых «трубок-сканеров», сводящих на нет такие способы защиты. Они позволяли отслеживать как скачкообразное изменение частоты, тем более, что количество фиксированных частот работы очень ограничено, так и подбирать индивидуальный номер трубки методом перебора.

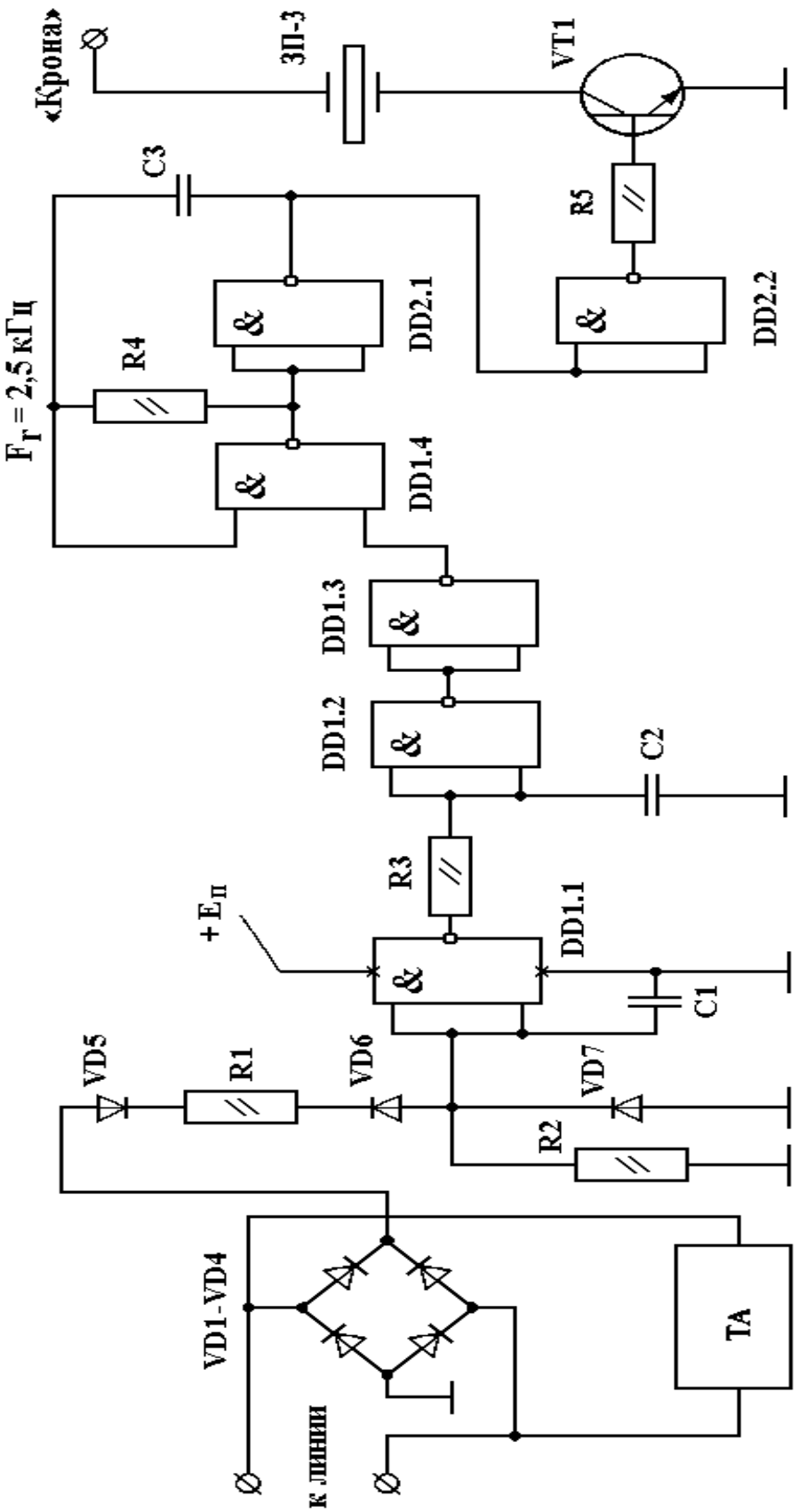

Рис. 169. Совмещенный индикатор подключения и обрыва линии

Надежным способом борьбы (без изменения принципиальной схемы радиотелефона) оставалась только установка блокиратора межгорода и блока дополнительного кодирования линии. На рис. 170 приведена такая схема защиты радиотелефона.

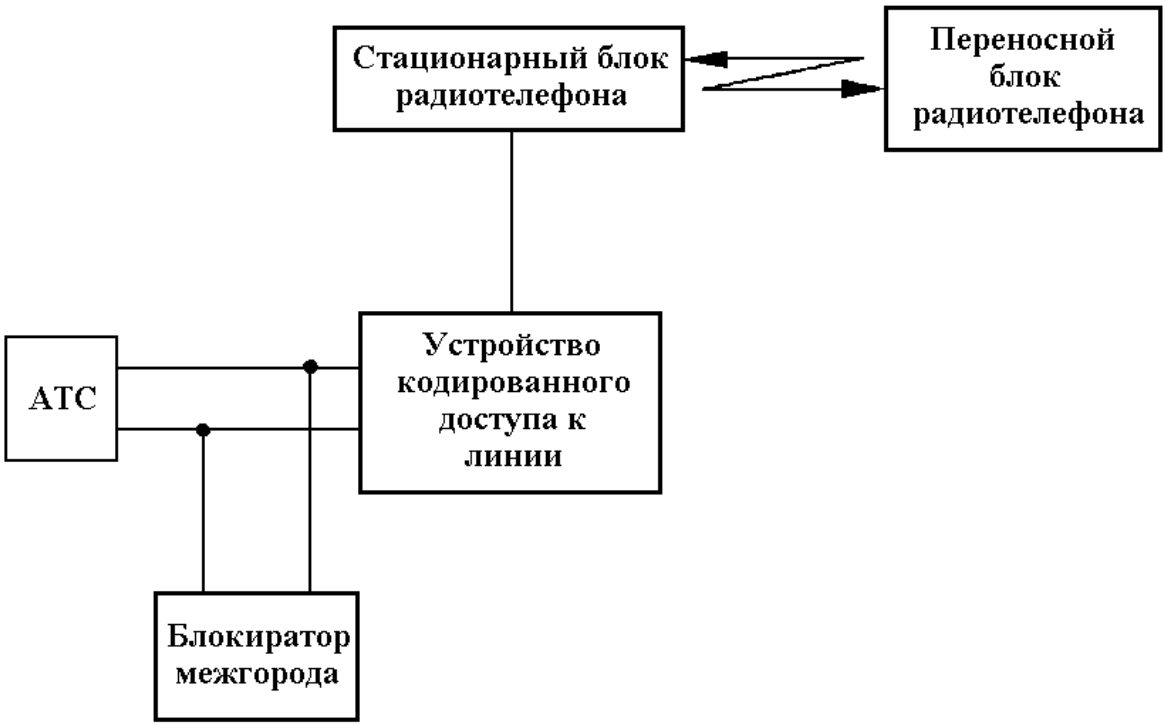

Рис. 170. Схема защиты радиотелефона

Радикальным путем решения сложившейся ситуации стало появление радиотелефонов, отвечающих стандарту DECT, близкому по принципам построения стандарту GSM, используемому в сотовой связи.

12. ТЕХНИЧЕСКИЕ СРЕДСТВА ПРОСТРАНСТВЕННОГО И ЛИНЕЙНОГО ЗАШУМЛЕНИЯ

По принципу действия все технические средства пространственного и линейного зашумления можно разделить на три большие группы:

- средства создания акустических маскирующих помех:
- средства создания электромагнитных маскирующих помех:
- многофункциональные средства защиты.

Рассмотрим эти средства более подробно.

12.1. Средства создания акустических маскирующих помех

Генераторы шума в акустическом диапазоне

Генераторы шума в речевом диапазоне получили достаточно широкое распространение в практике защиты информации. Они используются для защиты от несанкционированного съема акустической информации путем маскирования непосредственно полезного звукового сигнала. Маскирование проводится «белым» шумом с корректированной спектральной характеристикой.

Примерный вид структурной схемы источника акустического шума приведен на рис. 171. Конструктивно аппаратура включает блок формирования и усиления шумового сигнала и несколько акустических излучателей. В качестве примера таких систем может служить генератор SOUND PRESS.

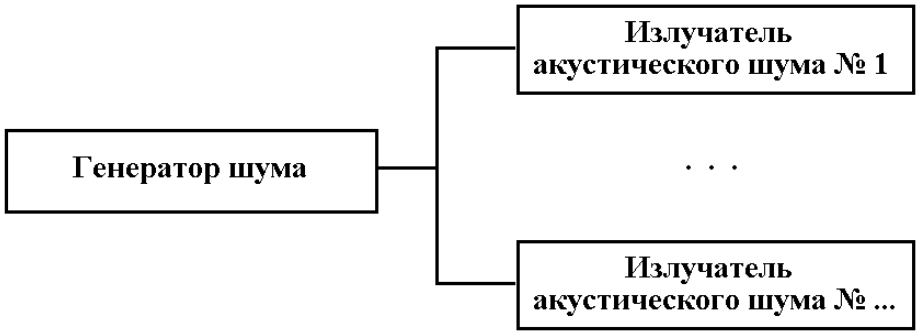

Рис. 171. Структурная схема источника акустического шума

SOUND PRESS – генератор акустического шума с вынесенными источниками излучения.

Основные технические характеристики SOUND PRESS

Мощность шума (max).....	2 Вт
Спектральная мощность шума	0,25 мВт/Гц
Срез спектра шума в НЧ-области	(<2 КГц) –8 дБ/окт.
Полоса равномерной плотности шума...	2 кГц–10 кГц
Дополнительный подъем ВЧ.....	+6 дБ/окт.

Габаритные размеры (две колонки) ..... 80×100×155 мм

В некоторых случаях наличие нескольких излучателей необязательно. Тогда используются компактные генераторы со встроенной акустической системой, например, WNG-023.

WNG-023 – акустический генератор белого шума имеет следующие основные технические характеристики:

Полоса акустической помехи..... 0,1–12 кГц
Вид помехи..... «Белый» шум
Излучаемая мощность ..... до 1 Вт
Встроенный аккумулятор (в комплект входит зарядное устройство)
Питание ..... 220 В/9 В
Габаритные размеры ..... 98×71×30 мм

Главный недостаток применения источников шумов в акустическом диапазоне – это невозможность комфортного проведения переговоров. Практика показывает, что в помещении где «ревет» генератор шума невозможно находиться более 10-15 мин. Кроме того, собеседники автоматически начинают пытаться перекричать средство защиты, снижая эффективность его применения. Поэтому подобные системы применяются для дополнительной защиты дверных проемов, межрамного пространства окон, систем вентиляции и т. д.

Устройства виброакустической защиты

Наиболее эффективным средством защиты помещений, предназначенных для проведения конфиденциальных мероприятий, от съема информации через оконные стекла, стены, системы вентиляции, трубы отопления, двери и т. д. являются устройства виброакустической защиты. Данная аппаратура позволяет в некоторых случаях предотвратить возможное прослушивания с помощью проводных микрофонов, звукозаписывающей аппаратуры, радиомикрофонов и электронных стетоскопов, лазерного съема акустической информации с окон и т. д. Противодействие прослушиванию обеспечивается внесением виброакустических шумовых колебаний в элементы конструкции здания.

Типовая структурная схема устройства виброакустической защиты приведена на рис. 172. Конструктивно аппаратура включает блок формирования и усиления шумового сигнала и несколько акустических и виброакустических излучателей.

Генератор формирует «белый» шум в диапазоне звуковых частот. Передача акустических колебаний на ограждающие конструкции производится при помощи пьезоэлектрических (на основе пьезокерамики) или электромагнитных вибраторов с элементами крепления.

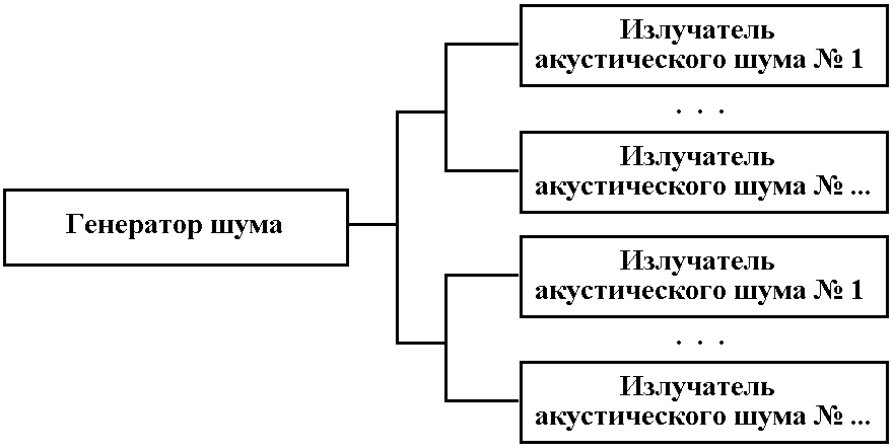

Рис. 172. Структурная схема устройства виброакустической защиты

Конструкция и частотный диапазон излучателей должны обеспечивать эффективную передачу вибрации. Вибропреобразователи возбуждают шумовые виброколебания в ограждающих конструкциях, обеспечивая при этом минимальный уровень помехового акустического сигнала в помещении, практически не влияющий на комфортность проведения переговоров.

Предусмотренная в большинстве изделий возможность подключения акустических излучателей, позволяет «зашумлять» вентиляционные каналы и дверные тамбуры. Как правило, имеется возможность плавной регулировки уровня шумового акустического сигнала.

Стоимость комплекта может составлять от $200 до $3000. Рассмотрим наиболее известные виброакустические генераторы, представленные на российском рынке.

ANG-007S – устройство защиты акустики помещений. Оптимальный режим защиты может быть создан при помощи двух видов вибродатчиков, акустических систем, суммарным количеством до 36, которые подключаются к 12 независимым усилителям с регулируемой мощностью и с возможностью визуального контроля уровня. Наличие встроенного и выносного микрофонов с регулируемой чувствительностью позволяет автоматически включать и выключать усилители мощности при изменениях уровня акустического сигнала.

Основные технические характеристики ANG-007S

Максимальный уровень громкости защищаемой речевой информации:	Не более 80 дБ
Полоса частот сигналов защиты:.....	0,04–15 кГц
Количество усилителей мощности:.....	12
Сопротивление нагрузки усилителя мощности:	8 Ом
Эффективный радиус одного вибропреобразователя: ТК1	1,5 м

ТК3	4,3 м
Питание	Сеть 220 В
Габаритные размеры электронного блока	230×195×63 мм
вибропреобразователя ТК1	10×55 мм
вибропреобразователя ТК3 1	20×55 мм

Модификации ANG-007S:

ANG 007SA – автономный вариант с дополнительным комплектом батарей (время непрерывной работы – 10 ч);

ANG 007SM – модернизированный вариант по индивидуальному заказу;

ANG 007SL – вариант «люкс» с улучшенным дизайном.

NG-502M – генератор виброакустического шума имеет следующие основные технические характеристики:

Максимальный уровень громкости защищаемых речевых сообщений:	Не более 75 дБ
Полоса частот сигнала защиты:	0,2–15 кГц
Количество датчиков:	до 12
Радиус действия одного датчика:	1,5 м
Питание:	Сеть 220 В, 50 Гц
Габаритные размеры: блок-генератора	205×60×155 мм
датчика	32×21 мм

Radel 01 – виброакустический генератор шума. Это устройство представляет собой цифровой двухканальный генератор «белого» шума. Регулировка уровня шума в каждом из каналов осуществляется независимо.

Основные технические характеристики Radel 01

Выходная мощность: канал А	3 Вт
канал В	3 Вт
Полоса излучаемых частот	200–12 000 Гц
Напряжение питания	12 В
Габаритные размеры генератора (электронный блок)	120×90×60 мм
Габаритные размеры контактных излучателей:	
для установки на стены	30×34 мм
для установки на окна	30×28 мм

RNG-01 – генератор акустического «белого» шума имеет следующие основные технические характеристики:

Диапазон частот	100–15 000 Гц
Мощность выходного сигнала (максимальная)	4 Вт
Питание	Сеть 220 В, 50 Гц
Потребляемая мощность	40 Вт
Габаритные размеры	140×127×40 мм

В комплект поставки входят 6 пьезовибраторов с элементами крепления на стены, стекла, трубы и 2 акустические колонки.

SPP-4 – генератор виброакустического шума. Особенностью прибора является генерация шума с автоматически регулируемым уровнем, зависящим от акустического фона помещения. Прибор имеет микропроцессорное управление и многофункциональный индикатор уровня. Три независимых канала акустической защиты помещения. Кроме того, он может быть подключен к телефонной линии для создания линейного зашумления.

К прибору можно подключить: 20 пьезоизлучателей (по 10 к каждому из каналов А и В); 1 вибрационный излучатель типа TRN-2000 или 2 акустических излучателя типа OMS-2000 (или аналогичных) к каналу С.

Каждый из трех каналов может работать в одном из трех режимов генерации шума: нормальный режим «белого» шума; режим «белого» шума со случайной амплитудой; режим «белого» шума с автоматическим управлением уровнем шума.

Основные технические характеристики SPP-4:

Спектр акустического шума прибором по каналам А, В, С и телефонной линии: .	200 Гц-6,3 кГц
Максимальный уровень шума (амплитудное значение):	
на выходе каналов А и В...	15 В
на выходе канала С	2,5 В
на выходе телефонного канала	3 В
Питание:	Сеть 220 В, 50 Гц

VAG-6/6 – виброакустический генератор имеет следующие основные технические характеристики:

Максимальное количество преобразователей	6 шт
Максимальное количество акустических колонок	6 шт
Требуемый импеданс нагрузки на выходе акустического канала.....	Не менее 16 Ом

VNG-006 – устройство защиты помещений от утечки информации по виброканалам. Комплект поставки предусматривает все необходимые установочные элементы для монтажа вибропреобразователей.

Основные технические характеристики VNG-006:

Максимальный уровень громкости защищаемых речевых сигналов.....	Не более 75 дБ
Полоса частот сигнала защиты.....	0,2–15 кГц
Количество вибропреобразователей	6–12 шт.
Эффективный радиус действия одного вибропреобразователя: кирпичная стена	2,5 м
бетонная стена.	3 м

Параметры выхода на акустическую систему:

мощность	3 Вт
импеданс	4–8 Ом
Питание.....	Сеть (220±10 %) В, 50 Гц

«БАРОН» – комплекс виброакустической защиты. Внешний вид представлен на рис. 173.

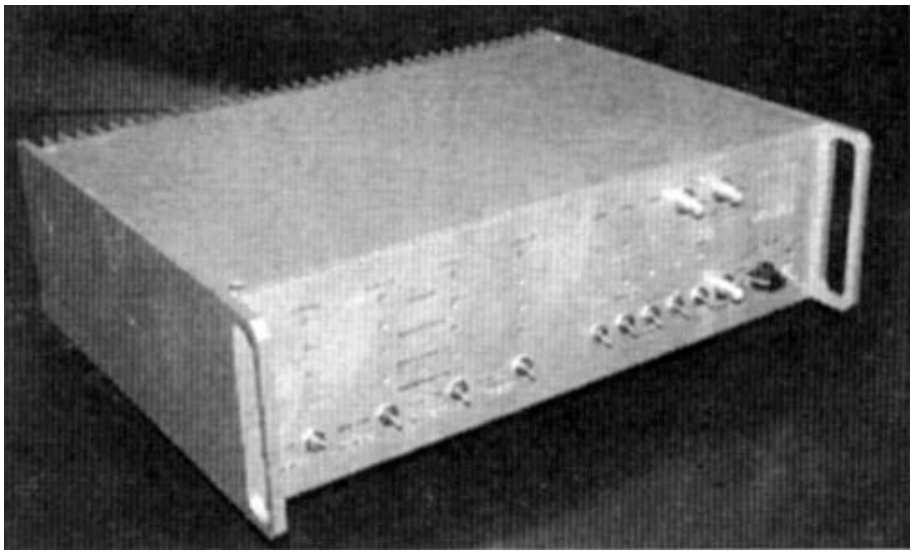

Рис. 173. Комплекс виброакустической защиты «БАРОН»

Основные достоинства прибора:

- возможность формирования помехового сигнала от различных внутренних и внешних источников и их комбинаций. Внутренние источники – генератор шума, 3 независимых радиоприемника. За счет их микширования значительно уменьшается вероятность очистки зашумленного сигнала. Кроме того, наличие линейного входа позволяет подключать к комплексу источники специального помехового сигнала повышенной эффективности;
- одним прибором можно защитить помещения большой площади различного назначения (конференц-залы и т. п.);
- возможность регулировки спектра помехового сигнала для повышения эффективности наведенной помехи с учетом особенностей используемых вибро- и акустических излучателей и защищаемых поверхностей;
- наличие 4 независимых выходных каналов с раздельными регулировками для оптимальной настройки помехового сигнала для различных защищаемых поверхностей и каналов утечки;
- достижение максимальной эффективности подавления при минимальном паразитном акустическом шуме в защищаемом помещении за счет вышеперечисленных возможностей настройки комплекса;

- возможность подключения к каждому выходному каналу различных типов вибро- и акустических излучателей и их комбинаций за счет наличия низкоомного и высокоомного выходов. Это также позволяет использовать комплекс для замены морально устаревших или вышедших из строя источников помехового сигнала в уже развернутых системах виброакустической защиты без демонтажа и замены установленных виброакустических излучателей;
- наличие системы беспроводного дистанционного включения комплекса.

Основные технические характеристики «БАРОН»

Выходная мощность..... 15 Вт на 4 канала
Количество полос регулировки по частоте 3 (250, 1000, 4000 Гц)
Диапазон частот усилителей..... 150 Гц-15 кГц
Источники помехового сигнала:
Внутренние: 3 радиоприемника FM-диапазона; 1 генератор шума
Внешний: через линейный вход
Дальность действия дистанционного управления: 30 м
Питание ..... Сеть 220 В, 50 Гц.

«СОНАТА-АВ» – виброакустический генератор шума. Состоит из двух независимых генераторов шума, каждый из которых может быть оперативно настроен на выдачу либо аудио-, либо вибропомехи калиброванной интенсивности.

Основные технические характеристики «СОНАТА-АВ»

Количество независимых каналов..... 2 шт
Максимальное количество виброизлучателей
типа ВИ-45г30 на 1 выходе ..... 6 шт
типа SB66 (8 Ом) на 1 выходе..... до 8 шт
Размах напряжения на виброизлучателе.... Не менее 100 В
Размах напряжения на аудиоизлучателе.... Не менее 1 В
Питание ..... Сеть 220 В, 50 Гц
Продолжительность непрерывной работы изделия до 24 ч
Габаритные размеры основного блока..... 135×65×155 мм

«ФОН-В» – система виброакустического зашумления. Используемые в системе генератор ANG-2000, вибродатчики TRN-2000 и TRN-2000M и оригинальные металлоконструкции для крепления вибродатчиков обеспечивают эффективное зашумление строительных конструкций. Монтаж и демонтаж системы осуществляется без повреждения строительных конструкций и элементов отделки интерьера.

Основные технические характеристики «ФОН-В»:

Диапазон частот ..... 250–5000 Гц
Радиус действия вибродатчика..... Не более 5 м

Площадь помещения, защищаемая системой	до 25 кв. м
Возможность расширения	до 36 кв. м
Количество в упаковке и вес:	
«Фон-В1»	1 шт - 14 кг
«Фон-В2»	2 шт по 12 кг
Минимальное время монтажа/демонтажа системы силами трех человек	Не более 30 мин

Монтаж системы виброакустического зашумления осуществляется достаточно просто. Главная проблема заключается в определении нужного количества датчиков и их взаимного расположения на ограждающей конструкции. Дело в том, что приводимые в технических характеристиках площади, перекрываемые одним излучателем, достаточно условные, а такие параметры, как материал (из которого изготовлена стена, дверь, потолок и т. д.), толщина конструкции, наличие полостей, качество крепления оказывают большое влияние на эффективность зашумления.

В связи с высокой стоимостью генераторов шума нежелательно приобретение лишнего оборудования, поэтому целесообразно проводить предварительные измерения параметров ограждающих конструкций, и только после этого определять необходимый тип генератора и количество датчиков, а также места их расположения. После завершения монтажных работ следует осуществлять контроль эффективности системы пространственного и линейного зашумления. При этом надо ориентироваться на то, что восстановить перехваченное сообщение практически невозможно, если уровень помехи более чем в 10 раз превышает уровень сигнала во всем частотном диапазоне (отношение сигнал/помеха менее – 20 дБ).

Технические средства ультразвуковой защиты помещений

Они недавно появились в продаже и не успели зарекомендовать себя как надежные средства технической защиты акустической информации. Отличительной особенностью этих средств является воздействие на микрофонное устройство и его усилитель достаточно мощным ультразвуковым сигналом (группой сигналов), вызывающим блокирование усилителя или возникновение значительных нелинейных искажений, приводящих в конечном счете к нарушению работоспособности микрофонного устройства (его подавлению).

Поскольку воздействие осуществляется по каналу восприятия акустического сигнала, то совершенно не важны его дальнейшие трансформации и способы передачи. Акустический сигнал подавляется именно на этапе его восприятия чувствительным элементом. Все это делает комплекс достаточно универсальным по сравнению с другими средствами активной защиты. При

этом не происходит существенного снижения эргономических характеристик помещения. Рассмотрим пример такого изделия.

«ЗАВЕСА» – комплекс ультразвуковой защиты акустических сигналов (см. внешний вид на рис. 174). В минимальной комплектации обеспечивает защиту в объеме до 27 куб. м. Стандартная конфигурация комплекса – двухканальная. При необходимости он имеет возможность наращивания до 4, 6, 8 и т. д. канальных версий.

Однако ультразвуковые комплексы на один-два порядка (более $10 000) дороже своих акустических аналогов и имеют небольшой радиус действия.

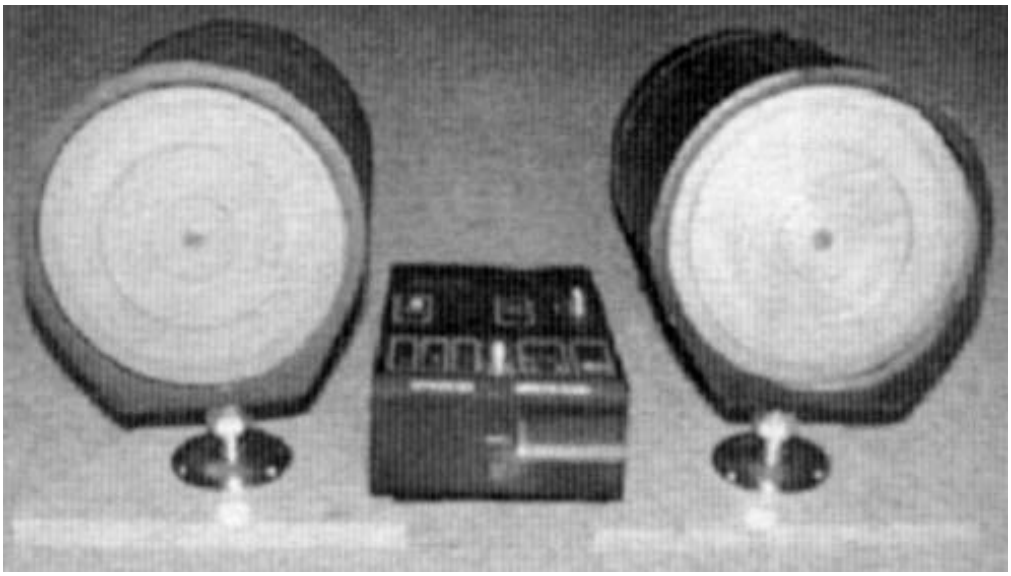

Рис. 174. Комплекс ультразвуковой защиты «ЗАВЕСА»

Принципиальная схема простейшего генератора «белого» шума [29], способного «закрыть» весь диапазон звуковых волн, представлена на рис. 175.

Непосредственно генератор выполнен на транзисторах *VT1* и *VT2* (могут быть марки КТ805А, КТ805А, Б или из серии КТ601). Амплитуда шумовой составляющей регулируется потенциометром *R4*. Формируемый сигнал через разделительный конденсатор *C3* подается на вход усилителя модулятора (база транзистора *VT3*). В исходном состоянии этот транзистор закрыт напряжением, поступающим на его эмиттер с делителя на резисторах *R12, R13* через *R11, R9*. Конденсатор *C5* при этом заряжен до напряжения, запирающего транзистор.

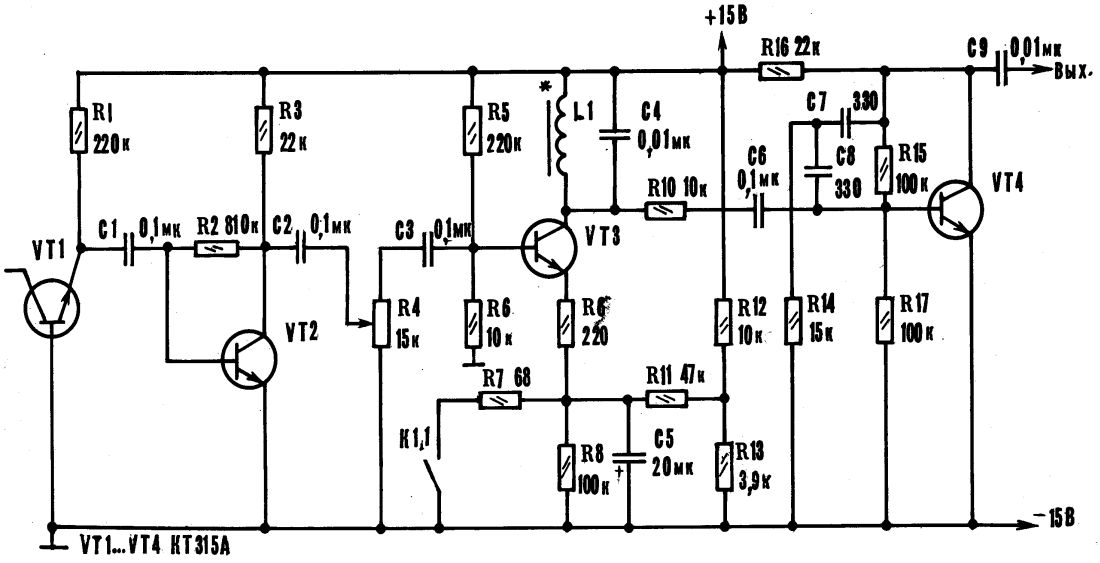

Рис. 175. Принципиальная схема источника маскирующих помех: генератор «белого» шума и усилитель-модулятор

При замыкании тумблера *K1.1* (вынесен за пределы платы и может быть установлен в любом удобном месте) конденсатор *C5* быстро разряжается через резистор *R7*. Транзистор *VT3* при этом открывается, и появляется на его выходе усиленный шумовой сигнал. Открытое состояние транзистора будет поддерживаться до тех пор, пока тумблер замкнут. При размыкании тумблера конденсатор *C5* вновь начинает заряжаться, что приводит к запиранию транзистора *VT3*. Резонансный контур *L1, C4,* включенный в цепь коллектора *VT3*, позволяет подобрать полосу частот, необходимую для перекрытия, спектра маскируемого сигнала. На транзисторе *VT4* собран согласующий усилитель.

Для подачи питающего напряжения можно использовать стандартный источник питания или сделать его самому, используя схему, приведенную на рис. 176.

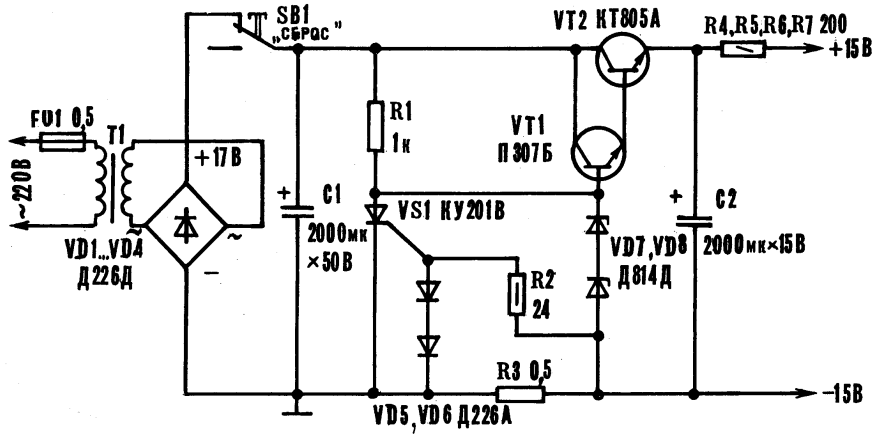

Рис. 176. Блок питания генератора

12.2. Средства создания электромагнитных маскирующих помех

Технические средства создания электромагнитных маскирующих помех (генераторы шума) делятся на средства пространственного и линейного зашумлений.

Технические средства пространственного зашумления

Предназначены для маскировки информативных побочных электромагнитных излучений и наводок персональных ЭВМ и периферийных устройств, а также другой оргтехники посредством создания помех в широкой полосе частот (как правило, от 1 до 1000 МГц). Однако серьезным недостатком их применения является создание непреднамеренных помех широкому классу радиоэлектронных устройств, расположенных в непосредственной близости от передатчика маскирующих излучений. Так, например, генератор пространственного зашумления делает невозможным прием пейджинговых сообщений, телевизионных программ, парализует работу мобильной связи и т. д. То есть применение данной аппаратуры может быть затруднено в связи с ограничениями по электромагнитной совместимости.

В некоторых случаях производители декларируют возможность подавления радиозакладных устройств. Естественно, теоретически это возможно, но уровень излучения генератора шума должен составлять величину 10-40 Вт, а выходная мощность закладки не должна превышать 20 мВт (при широкополосной частотной модуляции) или 10 мВт (при узкополосной частотной модуляции). Конечно, если речь не идет о приемниках сигналов дистанционного управления в радиозакладках, которые бесспорно подавляются.

Обычно стоимость представленных на рынке генераторов колеблется от $250 до $3000 . Рассмотрим некоторые типы таких.

Bawler 01 – генератор шума имеет следующие основные технические характеристики:

Диапазон рабочих частот	20–1000 МГц
Выходная мощность.....	1,5–2,5 Вт
Потребляемый ток, не более (при 12 В).....	0,3 А
Напряжение питания	9 В
Питание	Сеть 220 В, 50 Гц; 12 В

Radioveil – генератор шума. Внешний вид показан на рис. 177.

Полоса шумовой помехи (–10 дБ)	30 МГц–1000 МГц
Средняя спектральная мощность.....	9 мВт/1 МГц
Мощность выходного сигнала	9 Вт
Потребляемый ток.....	1 А
Напряжение питания.....	24–36 В
Габаритные размеры	170×110×80 мм

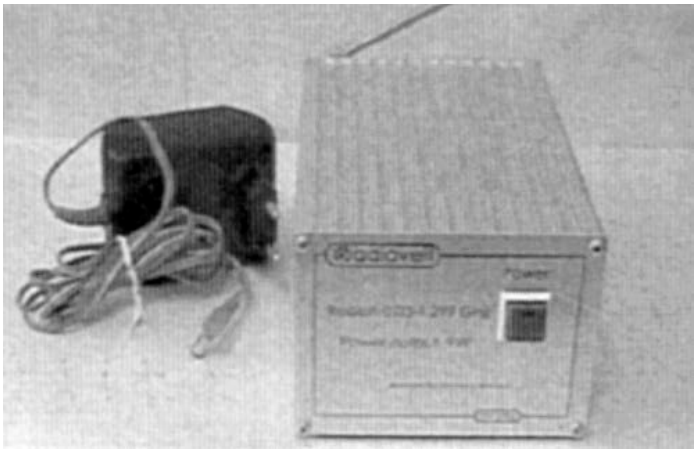

Рис. 177. Генератор пространственного зашумления Radioveil

Основные технические характеристики Radioveil

SP-21B («Баррикада-1») – портативный генератор радиошума (см. рис. 178). Генератор обеспечивает гарантированное подавление в радиусе приблизительно 5 м вокруг телескопической антенны (по полусфере) сигналов следующих типов:

- излучений радиомикрофонов любого типа с модуляцией WFM и мощностью до 50 мВт;
- сигналов дистанционного управления на включение антенны радиомикрофонов любого типа.

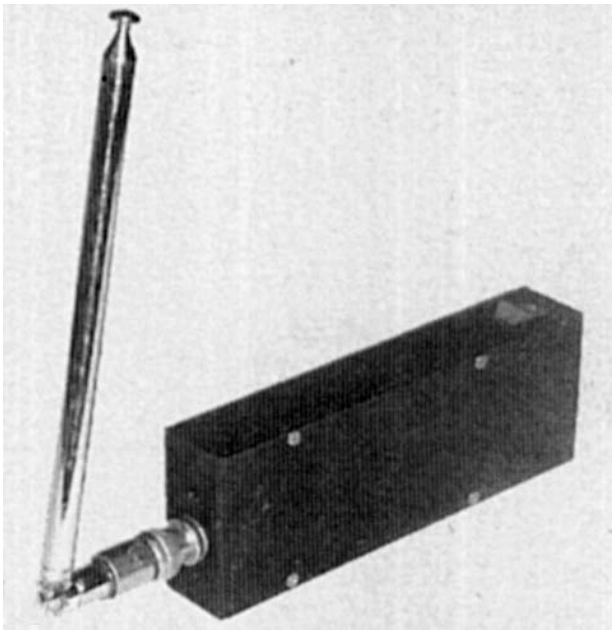

Рис. 178. Генератор пространственного зашумления SP-21B

Отличительной особенностью является обеспечение «белого» шума и наличие телескопической антенны, что в сопряжении с портативностью генератора определяет возможность его использования в любых условиях, в том числе и в автомобилях.

Основные технические характеристики SP-21B («Баррикада-1»)

Диапазон частот ..... 5 МГц-1 ГГц
Антенна ..... Телескопическая
Уровень сигнала на выходе..... Не менее 45 дБ
Условия эксплуатации:
температура окружающей среды..... 0-40ºС
относительная влажность при + 25ºС Не более 85 %
атмосферное давление ..... 750±40 мм рт. ст.
Питание ..... 12 В
Ток потребления от источника постоянного тока Не более 350 мА
Габаритные размеры ..... 165×65×25 мм
Масса ..... Не более 0,3 кг

SEL SP-21B2 «Баррикада-2» – портативный генератор радиошума. По своим массогабаритным характеристикам аналогичен «Баррикаде-1». Генератор обеспечивает: защиту от подслушивающих устройств с радиоканалом мощностью до 20 мВт; подавление приемников сигналов дистанционного управления по радиоканалу в радиусе не менее 30 м.

Основные технические характеристики SEL SP-21B2 «Баррикада-2»

Диапазон зашумления:
от телескопических антенн ..... 30–1000 МГц
от стационарной антенны..... 100 кГц–80 МГц
Интегральное значение выходной мощности:
при телескопических антеннах, выход 1/2 9–12 Вт/15–20 Вт
при стационарной антенне ..... 4 Вт
Потребляемая мощность ..... Не более 160 Вт
Питание ..... 220 В, 50 Гц; 12 В, 10 А
Габаритные размеры ..... 330×220×190 мм
Масса ..... Не более 5 кг

«ГНОМ-3» – стационарный генератор шума (см. рис. 179).

Диапазон частот шумового сигнала..... 10 кГц...1 ГГц
Антенны: ..... Рамочные, монтируемые в трех плоскостях
Уровень шумового сигнала на выходных разъемах генератора в диапазонах частот:
10-150 кГц (при полосе пропускания приемника 200 Гц) ≥ 70 дБ
150 кГц-30 МГц (при полосе пропускания приемника 9 кГц) ≥ 70 дБ
30-400 МГц (при полосе пропускания приемника 120 кГц) ≥ 75 дБ

0,4-1 ГГц (при полосе пропускания приемника 120 кГц) ≥70 дБ
Питание ..... Сеть 220 В, 50 Гц

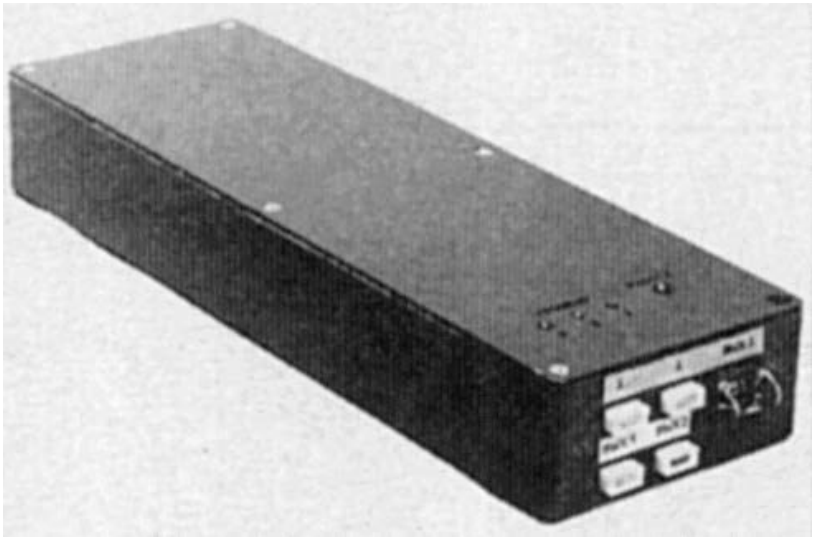

Рис. 179. Генератор пространственного зашумления «ГНОМ-3»

Основные технические характеристики «ГНОМ-3»

ГШ-1000 – стационарный генератор шума (рис. 180). Обеспечивает маскировку побочных электромагнитных излучений устройств вычислительной техники, размещенных на площади 40 кв. м. Устройство имеет индикацию контроля работоспособности, оборудовано разъемом для подключения внешнего контрольного или управляющего устройства, позволяющего автоматически блокировать работу периферийных систем вычислительной техники в случае возникновения неполадок в работе генератора.

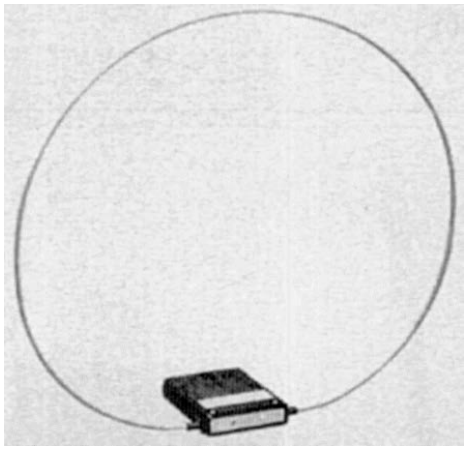

Рис. 180. Генератор ГШ-1000

Основные технические характеристики ГШ-1000

Диапазон частот ..... 0,1-1000 МГц
Включение..... Вместе с ПЭВМ
Потребляемая мощность..... 5 Вт
Спектральная мощность шума на расстоянии 1 м
в диапазоне 0,1-100 МГц ..... Не менее 60 дБ
в диапазоне 100-300 МГц..... Не менее 70 дБ
в диапазоне 300-500 МГц ..... Не менее 45 дБ

в диапазоне 500-1000 МГц ..... Не менее 25 дБ
Питание ..... От шины компьютера

«СМОГ» – генератор шума. Бескорпусной генератор шума, устанавливаемый в свободный слот системного блока ПЭВМ. Предназначен для создания активной защиты информации в вычислительных машинах типа IBM PC/AT286, 386, 486 и периферийного оборудования. Сокращает размер контролируемой зоны до нескольких метров. Программное обеспечение генератора шума функционирует в средах MS DOS, Windows и обеспечивает:

- контроль наличия устройства защиты в ПЭВМ;
- контроль исправности устройства защиты и антенной системы;
- прерывание обработки информации в ПЭВМ при неисправности устройства защиты и антенной системы;
- возможность включения/выключения генератора с клавиатуры ПЭВМ.

Основные технические характеристики «СМОГ»

Диапазон частот.....1 кГц...1000 МГц
Питание .....от ПЭВМ
Интерфейс с ПЭВМ.....ISA
Антенные системы .....рамочные (в виде подставки под дисплей и принтер); дипольная (в виде одиночного провода, закрепляемого вдоль шнура системного блока)

УАЗИ – устройство активной защиты информации. Предназначено для активной защиты информации от перехвата средствами радиоэлектронного контроля. Работает на две телескопические излучающие антенны, а при необходимости закрытия диапазона частот 100 кГц-80 МГц рекомендуется дооборудовать помещения дополнительными рамочными антеннами из изолированного провода, проложенного по периметру стен. Для подключения антенн в изделии предусмотрен специальный выход.

Основные технические характеристики УАЗИ

Диапазон частот..... 0–1000 МГц
Интегральное значение выходной мощности:
выход 1 ..... 9-15 Вт
выход 2 ..... 15-20 Вт
Мощность в полосе 50-200 кГц на частотах
150 МГц (выход 1) и 450 МГц (выход 2) ... Не менее 40 мВт
Полоса частот, соответствующая максимальной выходной мощности
выход 1 ..... 80-300 МГц
выход 2 ..... 400-500 МГц
Спектральная плотность мощности
в указанной полосе..... Не менее –38 дБ/Гц

Относительное ослабление выходной мощности
в диапазонах частот 0,1...80 МГц и 500...850 МГц Не более 36 дБ
Питание ..... 220 В, 50 Гц; 12 В
Потребляемая мощность ..... Не более 160 Вт

ШАТЕР-К – генератор шума. Обеспечивает постоянный контроль работоспособности генераторов и блока питания с выдачей сигнализации во внешнюю цепь.

Основные технические характеристики ШАТЕР-К

Выходная мощность сигнала в излучателе Не менее 3 мВт
Излучаемые уровни поля Не превышают норм ГОСТ 121006–84
Диапазон частот..... Не менее 0,5-1000 МГц
Неравномерность спектральной характеристики
выходного сигнала ..... Не более 30 дБ на октаву в рабочем диапазоне частот
Питание ..... (220±22) В, (50±2) Гц
Потребляемая мощность ..... Не более 35 Вт
Габаритные размеры, не более
блок питания..... 255×190×120 мм
генератор..... 220×60×40 мм
излучатель..... 1800 мм
Масса с упаковкой..... Не более 20 кг

При монтаже генераторов шума, работающих в НЧ-диапазоне (до 30 МГц) особую сложность вызывает размещение многометровых антенн в различных плоскостях.

Для контроля эффективности зашумления целесообразно проверять уровень помехового сигнала в заданном частотном диапазоне и сравнивать его с уровнями ПЭМИ и излучений микроваттных специальных технических средств негласного съема информации. Для этого удобно использовать анализаторы спектра.

Средства создания маскирующих помех в коммуникационных сетях

Выше было отмечено, что *технические средства линейного зашумления* условно можно разбить на две группы:

- средства создания маскирующих помех в коммуникационных сетях (телефонных, сигнализации и т. д.);
- средства создания маскирующих помех в сетях электропитания.

Принцип их действия основан на генерации в линию шумоподобных сигналов, созданных аналоговым или цифровым способом. Могут выступать как самостоятельными средствами защиты, так и составной частью более сложных универсальных средств.

«ТУМАН-1» – односторонний маскиратор телефонных сообщений (см. рис. 181). Обеспечивает защиту конфиденциальной информации, принимаемой от корреспондента по телефону на городских и местных (внутренних) линиях. Метод защиты передаваемой информации основан на зашумлении речевого диапазона частот на основе использования псевдослучайной последовательности (ПСП) в тракте соединения абонентов. Выделение полезного сигнала осуществляется абонентом, имеющим маскиратор, путем компенсации созданной им ПСП. Прибор сертифицирован Гостехкомиссией России (сертификат № 187).

Рис. 181. Устройство линейного зашумления «ТУМАН-1»

Принцип работы с устройством заключается в следующем. Абонент № 1, имеющий односторонний маскиратор, получает входной звонок от абонента № 2, не имеющего в общем случае такого маскиратора (в том числе таксофон, сотовый телефон). В момент передачи важных сообщений, требующих защиты (о чем абонент № 2 извещает открытым текстом), абонент № 1 подключает к линии маскиратор речи, создающий достаточно интенсивный шум. Этот шум слышит абонент № 2, но продолжает разговор, не меняя голоса. В отличие от него абонент № 1 шума не слышит, он воспринимает «чистую» речь, так как шум при приеме автоматически компенсируется.

К сожалению, маскиратор осуществляет защиту только речи абонента № 2, а телефонная связь осуществляется в симплексном режиме.

Основные технические характеристики «ТУМАН-1»

Создаваемое соотношение сигнал/шум в линии –	30 дБ
Напряжение парафазного ПСП маскирующего сигнала	Не менее 15 В
Ток синфазного ПСП-сигнала в телефонной линии	Не менее 5 мА
Величина остаточного постоянного напряжения в телефонной линии при разговорном режиме	Не более 0,6 В

Электропитание	220 В, 50 Гц
Потребляемая мощность.....	Не более 15 Вт
Габаритные размеры	68×176×170 мм

NG-301 – устройство защиты телефонных переговоров от прослушивания. Предназначено для защиты телефонных переговоров от прослушивания с помощью средств негласного съема информации. В основе работы лежит принцип подачи в телефонную линию шумового маскирующего сигнала (см. рис. 182).

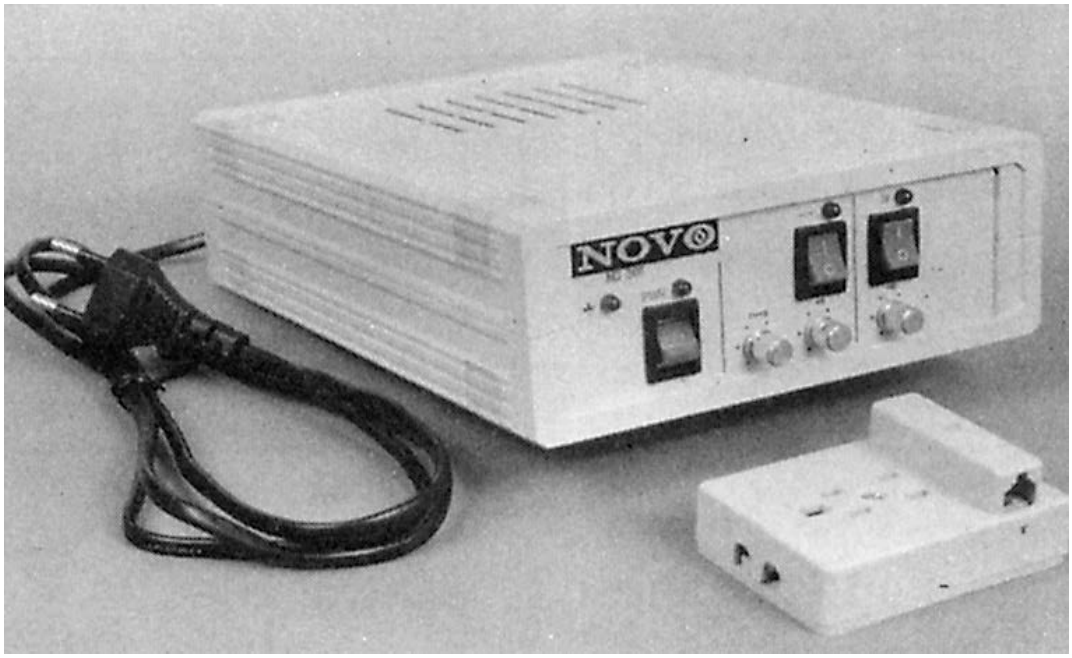

Рис. 182. Устройство линейного зашумления NG-301

Устройство обеспечивает эффективное противодействие следующим средствам негласного съема информации:

- радиопередатчикам, включаемым в телефонную линию последовательно и параллельно;
- индукционным датчикам, устанавливаемым на один провод телефонной линии;
- аппаратуре магнитной записи, подключаемой к телефонной линии с помощью контактных или индукционных датчиков;
- телефонным аппаратам, факсам, модемам, негласно подключаемым к телефонной линии.

Основные технические характеристики NG-301

Тип воздействия	Зашумление
Отношение сигнал/шум в устройстве прослушивания	Не хуже 20 дБ
Отношение сигнал/шум в телефонном аппарате	Не менее 14 дБ

Питание ..... 220 В, 50 Гц
Габаритные размеры ..... 160×60×220 мм

SEL SP-17/T – генератор шума для стандартных телефонных линий. Обеспечивает защиту стандартной телефонной линии пользователя (до АТС) от прослушивания с использованием телефонных передатчиков любого типа и мощности независимо от способа их подключения, средств магнитной записи и параллельных телефонных аппаратов. Принцип действия – создание помех в виде низкочастотного цифровым способом образованного шума с широким спектром. Генератор не требует подстройки, а также специальных навыков в установке и эксплуатации.

«СОНАТА-03» – прибор защиты телефонной линии. Обеспечивает подавление ЗУ, непосредственно подключаемых к телефонной линии, путем постановки активных помех.

Основные технические характеристики «СОНАТА-03»

Относительное значение уровня маскирующей помехи к уровню полезного сигнала ..... Не менее 35–40 дБ
Питание ..... 220 В, 50 Гц
Время непрерывной работы ..... Не менее 20 ч
Габаритные размеры моноблока..... 115×55×50 мм

Средства создания маскирующих помех в сетях электропитания

Для защиты электросетей переменного тока 220 В, 50 Гц от их несанкционированного использования для передачи перехваченной с помощью специальных технических средств речевой информации используются сетевые генераторы шума.

Устройство конструктивно представляет собой задающий генератор «белого» шума, усилитель мощности и блок согласования выхода с сетью 220 В. Как правило, используется диапазон 50-500 КГц, но иногда он расширяется и до 10 МГц. Данные генераторы шума действительно являются эффективным средством борьбы с техническими средствами негласного съема информации и стоят от $200 до $400. В некоторых случаях используется комбинированная аппаратура обнаружения/подавления (генератор включается в режим подавления при превышении ВЧ-сигнала в электросети выше установленного порога).

NG-201 – генератор шума сетевой. Имеет встроенную систему самодиагностики со световой и звуковой сигнализациями нарушения работоспособности. Обеспечивает высокую эффективность защиты, не требуя при этом специальной подготовки пользователей.

Основные технические характеристики NG-201

Полоса сигнала защиты ..... 30-800 кГц
Интегральная мощность сигнала..... 2 Вт

Питание ..... 220 В, 50 Гц
Габаритные размеры ..... 220×110×50 мм

NG-401 – генератор шума сетевой (см. рис. 183). Принцип действия основан на подаче в защищаемую сеть сложного шумоподобного сигнала с цифровым формированием.

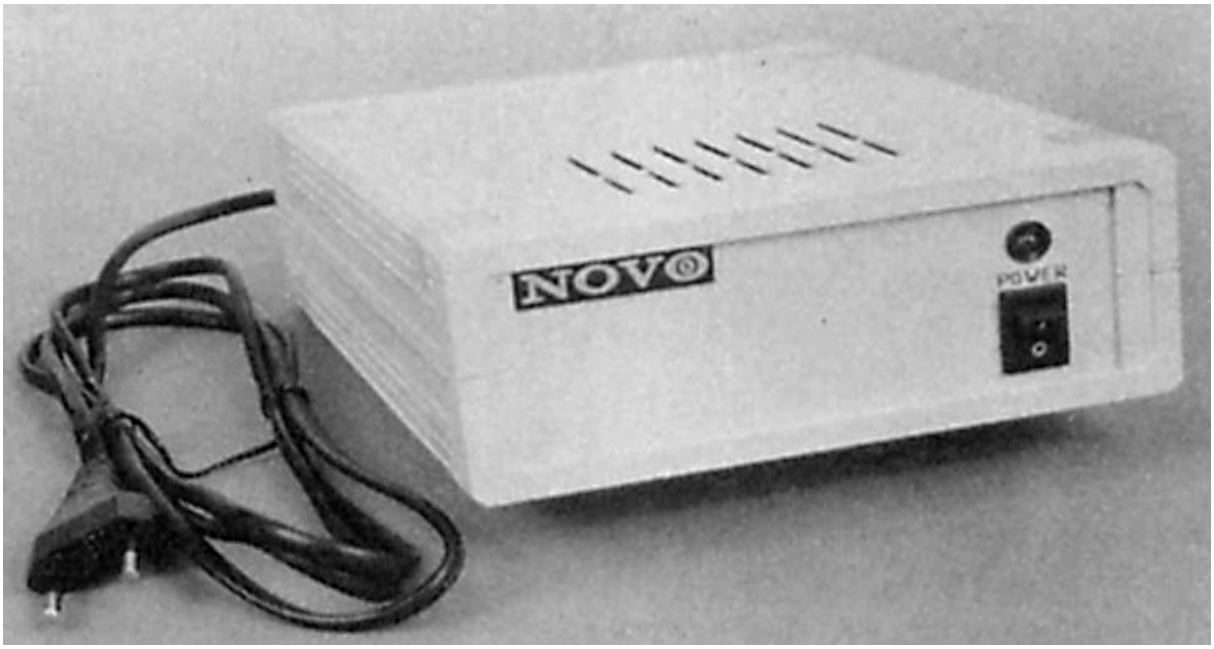

Рис. 183. Генератор шума сетевой NG-401

Основные технические характеристики NG-401

Гарантированная полоса частот сигнала защиты 80-500 кГц
Мощность сигнала защиты..... 5 Вт
Питание ..... Сеть 220 В
Габаритные размеры ..... 205×60×155 мм

NG-402 – генератор шума сетевой. Свипирующий генератор «белого» шума предназначен для защиты электросетей переменного тока 220 В, 50 Гц от несанкционированного их использования для передачи речевой информации. Представляет собой модификацию изделия NG-401 и также позволяет защищать одновременно три фазы силовой линии. Принцип действия основан на подаче в защищаемую сеть сложного шумоподобного сигнала с цифровым формированием.

Основные технические характеристики NG-402

Гарантированная полоса частот сигнала защиты 80...500 кГц
Мощность сигнала защиты..... 5 Вт
Питание ..... Сеть 220 В
Габаритные размеры ..... 205×60×155 мм

«СОПЕРНИК» – генератор шума сетевой. Предназначен для обнаружения и подавления (в автоматическом режиме) устройств несанкционированного съема информации, использующих для передачи данных сеть 220 В.

Прибор рассчитан на постоянную работу в дежурном режиме. «Соперник» постоянно сканирует и анализирует сеть. При появлении в ней высокочастотной составляющей загорается красная светодиодная линейка, показывающая уровень сигнала, который присутствует в сети, и сразу же загорается зеленая светодиодная линейка, указывающая на уровень шумового сигнала, генерируемого прибором в качестве противодействия. При значении ВЧ-сигнала ниже определенного уровня прибор автоматически переходит в ждущий режим.

Основные технические характеристики

Полоса контролируемых частот	30 кГц-1,2 МГц
Порог регистрации сигнала.....	0,7 В
Максимальная плотность шума генерируемой помехи:	0,15 Вт/10 кГц
Ширина спектра шума (на уровне – 3 дБ)	5 кГц-1,5 МГц
Индикация принимаемого шума – линейная по амплитуде	0,2 В/деление
Индикация генерируемого шума – линейная по мощности	0,3 Вт/деление
Мощность шума	6 Вт
Потребляемая мощность.....	10 Вт
Габаритные размеры	37×63×118 мм

Порог срабатывания прибора выбран таким образом, чтобы не происходило срабатывания на паразитные наводки.

SP-41C – генератор шума сетевой имеет следующие основные технические характеристики:

Амплитуда помехи:

в диапазоне 50-500 кГц..... Не менее 10 В

в диапазоне 0,5-5 МГц ..... Не менее 1 В

Мощность помехового сигнала ..... 5 Вт

Питание ..... 220 В

Габаритные размеры ..... 155×125×40 мм

Масса ..... 71,2 кг

«СОНАТА-С1» – генератор шума сетевой имеет следующие основные технические характеристики:

Время выхода изделия в рабочий режим после включения	Не более 1 с
Минимальное сопротивление нагрузки	4 Ом
Действующее значение напряжения помехи на нагрузке	Не менее 10 В
Диапазон частот помехи	0,01-3 МГц
Питание	220 В, 50 кГц
Продолжительность непрерывной работы	24 ч

Габаритные размеры..... 153×135×65 мм

«ЦИКАДА-С» – устройство информационной защиты электросети. Формируемый изделием широкополосный маскирующий сигнал гарантированно защищает электросеть в диапазоне частот 80 кГц-10 МГц на удалении до 300 м по длине проводки. Изделие не создает помех ПЭВМ и другим устройствам бытовой электроники.

Основные технические характеристики

Выходная мощность..... 5 Вт
Питание ..... 220 В, 50 Гц
Габаритные размеры ..... 160×140×60 мм
Масса ..... 1 кг

«ЦИКАДА-С3» – устройство информационной защиты электросети. Соответствует техническим характеристикам изделия «Цикада-С» с дополнительным обеспечением подачи маскирующего сигнала в трехфазную электросеть, организованную по схеме «звезда».

Основные технические характеристики

Габаритные размеры ..... 170×176×68 мм
Масса ..... 1,8 кг

В большинстве случаев монтаж сетевых генераторов шума не является сложной проблемой, достаточно включить прибор в сеть и, в некоторых случаях, провести несложные регулировки. Однако в ряде помещений могут использоваться несколько вводов по питанию (подключение от разных фаз розеток и освещения, специальное стабилизированное питание для ПЭВМ и т. д.) и тогда необходимо защищать их все.

12.3. Многофункциональные средства защиты

При практической организации защиты помещения от утечки информации по техническим каналам необходимо комплексное использование различных устройств безопасности: акустических, виброакустических, сетевых генераторов шума и источников электромагнитного маскирующего излучения. При этом можно пойти следующими тремя путями:

- подбором различных устройств защиты информации и их автономным использованием;
- объединением различных устройств защиты информации в единый комплекс путем применения универсального блока управления и индикации;
- использованием готовых комплектов.

Рассмотрим особенности каждого из этих путей.

В первом случае возможен подбор оптимального по техническим, эргономическим и стоимостным параметрам комплекса аппаратуры. Однако

включение его потребует от пользователя последовательного включения всех источников шума и индивидуального контроля их работоспособности, что не всегда удобно.

Во втором случае используется готовый пульт управления, устраняющий описанный выше недостаток, например, «Соната-ДУ».

«СОНАТА-ДУ» – блок дистанционного управления комплексом создания маскирующих помех (см. рис. 184). Он предназначен для дистанционного скрытного включения/выключения комплекса технических средств защиты информации, имеющих сетевое электропитание.

Рис. 184. Блок дистанционного управления комплексом создания маскирующих помех «Соната-ДУ»

Основные технические характеристики «Соната-ДУ»

Максимальная мощность коммутируемой нагрузки 100 Вт
Вид канала управления..... Радиоканал, ИК-канал
Питание ..... Сеть 220 В, 50 Гц
Продолжительность непрерывной работы изделия до 24 ч
Габаритные размеры основного блока..... 135×65×155 мм

Примечание: благодаря наличию встроенной системы самопрограммирования для управления устройством может быть использован любой пульт ДУ от бытовых устройств (телевизоров, кондиционеров) либо практически любой брелок автосигнализации.

Однако не всю аппаратуру различных производителей возможно включать с помощью универсальных пультов.

Рассмотрим *третий путь* – использование готовых многофункциональных комплексов – на следующих примерах.

«ГРОМ-ЗИ-4» – многофункциональный генератор шума. Предназначен для защиты от утечки за счет побочных электромагнитных излучений средств оргтехники, а также для создания помех устройствам несанкционированного съема информации с телефонных линий и электрических сетей. Выполнение указанных функций обеспечивается генератором независимо друг от друга.

При защите телефонных переговоров от подслушивания генератор размывает спектр акустических сигналов в телефонной линии. Работа генератора при зашумлении радиодиапазона осуществляется на съемную телескопическую антенну. При зашумлении крупногабаритных объектов (вычислительных центров, терминальных залов и т. п.) целесообразно использование нескольких комплектов «Гром-ЗИ-4» с антеннами, ориентированными в трех взаимно перпендикулярных плоскостях.

Основные технические характеристики «ГРОМ-ЗИ-4»

Полоса частот помехового сигнала при зашумлении радиодиапазонов ..... 20-1000 МГц

Типовое значение напряженности поля помех, создаваемого генератором, относительно 1 мкВ/м:

в диапазоне 20...60 МГц ..... 60 дБ

в диапазоне 60...300 МГц ..... 90 дБ

в диапазоне 300...1000 МГц ..... 40 дБ

Полоса частот помехового сигнала при зашумлении электросети ..... 100-1000 кГц

Напряжение помехового сигнала в электросети относительно 1 кВ ..... Не менее 60 дБ

Напряжение помехового сигнала, создаваемого в телефонной линии: на частоте 20 Гц ..... 2,5 В

в полосе частот 15-25 кГц ..... 0,5 В

Время непрерывной работы ..... 8 ч

«ГРОМ-ЗИ-6» – генератор шума (см. рис. 185). Предназначен для защиты переговоров от утечки информации по телефонной линии и электрической сети. Прибор защищает участок линии от телефонного аппарата до автоматической телефонной станции, а также блокирует устройства, использующие электрическую сеть помещения в качестве канала утечки информации.

Принцип действия прибора основан на маскировке спектра речи широкополосным шумом. Прибор предотвращает прослушивание телефонного аппарата устройствами, работающими по принципу ВЧ-навязывания, а также реагирующими на поднятие трубки телефонного аппарата.

Рис. 185. Генератор шума «ГРОМ-ЗИ-6»

Генератор может работать в автоматическом и неавтоматическом режимах. В автоматическом режиме контролирует напряжение линии и включает защиту при поднятии трубки телефонного аппарата и снижении напряжения линии в случае подключения к ней параллельного телефона или подслушивающего устройства. Прибор имеет сертификат ФСТЭК.

Основные технические характеристики

Максимальное значение напряжения, генерируемого прибором
по телефонной линии в диапазоне частот 6-40 кГц: Не менее 3 В
Отношение напряжения помех, генерируемых прибором в линию,
к напряжению помех на клеммах телефонного аппарата: Не менее 30 дБ
Диапазон регулировки тока линии:..... Не менее 10 мА
Напряжение помех, генерируемых прибором
в электросеть относительно 1 мкВ:
в диапазоне частот 0,1-1 МГц..... Не менее 60 дБ
в диапазоне частот 1-5 МГц..... Не менее 30 дБ
Время непрерывной работы..... 8 ч

Генераторы **«ГРОМ-ЗИ-4»** и **«ГРОМ-ЗИ-6»** стоят $500-$600, но не имеют всех необходимых функций (например, виброакустического шума) и их придется дополнять аппаратурой других производителей.

Существуют и другие универсальные комплексы. В качестве примера рассмотрим систему комплексной защиты «Скит».

«СКИТ» – многофункциональный комплекс защиты. Он обеспечивает защиту от утечки информации за счет ПЭМИН (в соответствии с требованиями Гостехкомиссии России); от утечки информации по виброакустическому каналу. Кроме того, осуществляет обнаружение и подавление до трех одно-

временно работающих специальных технических средств разведки с радиоканалом и управляется по ИК-каналу при помощи пульта ДУ.

В состав этого комплекса входят:

«СКИТ-СК» – автоматический скоростной коррелятор – подавитель радиомикрофонов ($1200);

«СКИТ-УМ» – усилитель мощности генератора прицельной помехи ($450);

«СКИТ-Ш» – широкополосный генератор электромагнитных помех ($280);

«СКИТ-Т» – широкополосный генератор помех для телефонных и слаботочных линий ($320);

«СКИТ-С» – широкополосный генератор помех для силовой сети электропитания ($210);

«СКИТ-ВА» – генератор виброакустических помех речевого диапазона частот с комплектом датчиков, 8 шт. ($430);

«СКИТ-К» – дистанционно-управляемый коммутатор средств защиты ($280);

Камуфлированный ИК-приемник сигналов дистанционного управления ($95).

Независимо от типа применяемых систем линейного и пространственного зашумления порядок работы с ними должен быть следующим:

- Определяются возможные технические каналы утечки информации;
- Устанавливается степень их опасности и потенциальная возможность перехвата информации;
- Определяются требования к аппаратуре защиты (типы и количество генераторов шума и датчиков, возможность их сопряжения и т. д.);
- Разрабатывается технический проект объекта в защищенном исполнении;
- Осуществляется монтаж закупленного оборудования;
- Проводится комплексный технический контроль эффективности принятых мер;
- Проводится периодический контроль работоспособности аппаратуры.

13. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ

Проблемы защиты информации волновали человечество с незапамятных времен. Так, первые системы шифров ученые встречают в Древнем Египте и Древней Греции, Риме и Спарте. Заботились о секретности информации и правители Венеции еще в XVI веке. Без знания специального ключа нельзя прочитать труды многих ученых средневековья – одни боялись преследования инквизиции, другие заботились о пальме первенства, третьи хотели, чтобы их знания достались только ученикам. Примеры достаточно сложных зашифрованных текстов археологи встречают и в русских памятниках XII–XIII веков. Первые технические системы начали разрабатываться сразу после изобретения телефона. Так, в США уже в 1875 году была подана заявка на изобретение, относящееся к закрытию телефонной связи. Да и по сегодняшний день радикальной мерой защиты каналов связи остается использование криптографических методов закрытия информации.

В настоящее время все системы кодирования информации являются электронными системами и реализуют два принципиально различных метода – аналоговое преобразование параметров речи и цифровое шифрование [29]. Рассмотрим оба способа защиты на примерах передачи речевой информации.

13.1. Аналоговое преобразование

При таком способе защиты изменяют характеристики передаваемой информации таким образом, чтобы результирующий сигнал становился неразборчивым, но занимал ту же полосу частот, что и исходный. Это дает возможность без проблем передавать открытую и защищенную информацию по одним и тем же каналам связи. Для реализации аналогового преобразования используют следующие виды преобразований: частотную инверсию; частотную и временную перестановки.

Инверсия частотного спектра.

Наиболее широкое распространение получила *инверсия частотного спектра*. Например, известно, что при амплитудной модуляции спектр сигнала имеет вид, представленный на рис. 186.

Вся информация сосредоточена в боковых составляющих слева и справа от несущей частоты. В передающем устройстве одна из полос подавляется фильтром, а другая усиливается, инвертируется (спектральные составляющие меняются местами) и подается в канал связи (см. рис. 187).

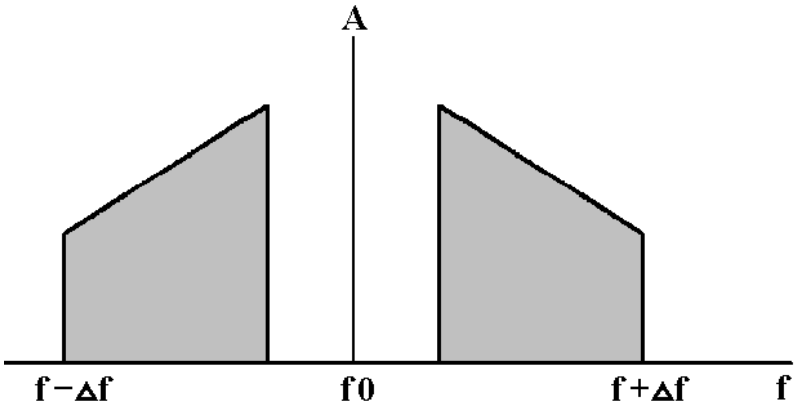

Рис. 186. Спектр амлитудно-модулированного сигнала

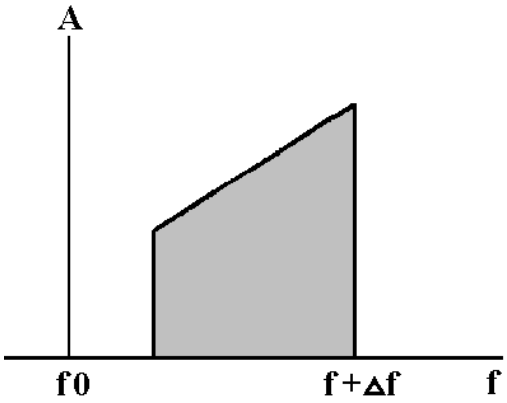

Рис. 187. Система с инвертируемым спектром

Случайно подключившийся к линии человек не сможет ничего разобрать в таком сигнале, кроме невнятного бормотания. Однако корреспондент, которому адресовано это сообщение, примет его нормально, так как его приемник вновь преобразует сигнал с инвертированным спектром в первоначальный.

Временная перестановка

В более сложных системах *с временной перестановкой* речь дробится на определенные, равные по длительности временные участки (интервалы коммутации) продолжительностью от 0,2 до 0,6 с. В пределах этого участка происходит дополнительное дробление на более мелкие участки длительностью 30-60 мс. Всего таких маленьких участков речи может быть от нескольких единиц до нескольких десятков. Эти информационные интервалы до передачи в линию связи записываются в каком-либо запоминающем устройстве, перемешиваются между собой по определенному закону, после чего сформированный таким образом сигнал передается в линию связи. На приемном

конце линии связи, где алгоритм перемешивания известен, осуществляется обратный процесс «сборки» исходного сигнала (см. рис. 188).

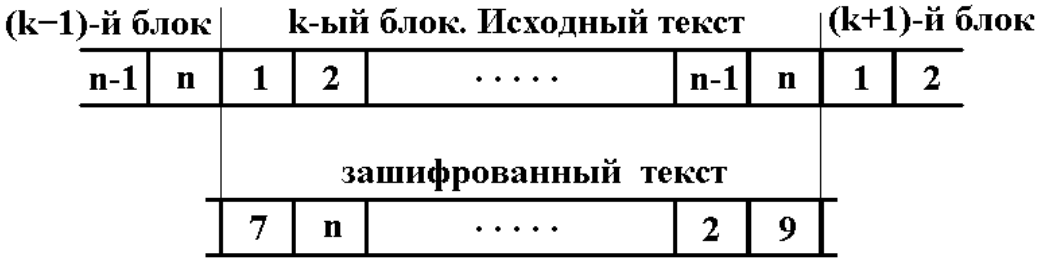

Рис. 188. Пример реализации временной перестановки в передаваемом сообщении

К преимуществам этого вида закрытия относится относительная простота технической реализации устройства, а следовательно, низкая стоимость и малые габариты, возможность передачи зашифрованного речевого сигнала по стандартному телефонному каналу и хорошее качество восстанавливаемого исходного сигнала. Главным недостатком метода является его довольно низкая стойкость к несанкционированному восстановлению. Вследствие того, что сигнал является непрерывным, у дешифровщика после записи и выделения участков (а это легко сделать, так как в состав сигнала приходится вводить метки, определяющие начало участков) появляется возможность осуществить декодирование даже без знания примененной системы ключей. Обычно пытаются осуществить «стыковку» участков таким образом, чтобы обеспечить непрерывность сигнала на стыках. При тщательной и кропотливой работе это часто удается сделать, однако скорость восстановления «нормального» сигнала без специальной техники исключительно мала. Поэтому такое закрытие есть смысл применять только в тех случаях, когда информация является не слишком ценной или когда ее значимость теряет свою актуальность через относительно небольшой промежуток времени.

Частотная перестановка

Несколько более стойкое кодирование получается, когда тот же принцип дробления и перемешивания применяется в отношении частоты (*частотная перестановка*). В этом случае с помощью системы фильтров вся полоса частот стандартного телефонного сигнала делится на некоторое количество частотных полос, которые перемешиваются в заданном порядке. Как правило, такое перемешивание осуществляется по псевдослучайному закону, реализуемому генератором ключа. Перемешивание частотных полос осуществляется со скоростью 2-16 циклов в секунду, то есть одна комбинация длится 60-500 мс, после чего она заменяется следующей. В свою очередь,

спектры этих сигналов могут находиться как в прямом, так и в инверсном виде. В ходе разговора кодовые комбинации могут меняться с некоторой цикличностью, однако при этом должна осуществляться их жесткая синхронизация. Принцип частотных перестановок показан на рис. 189.

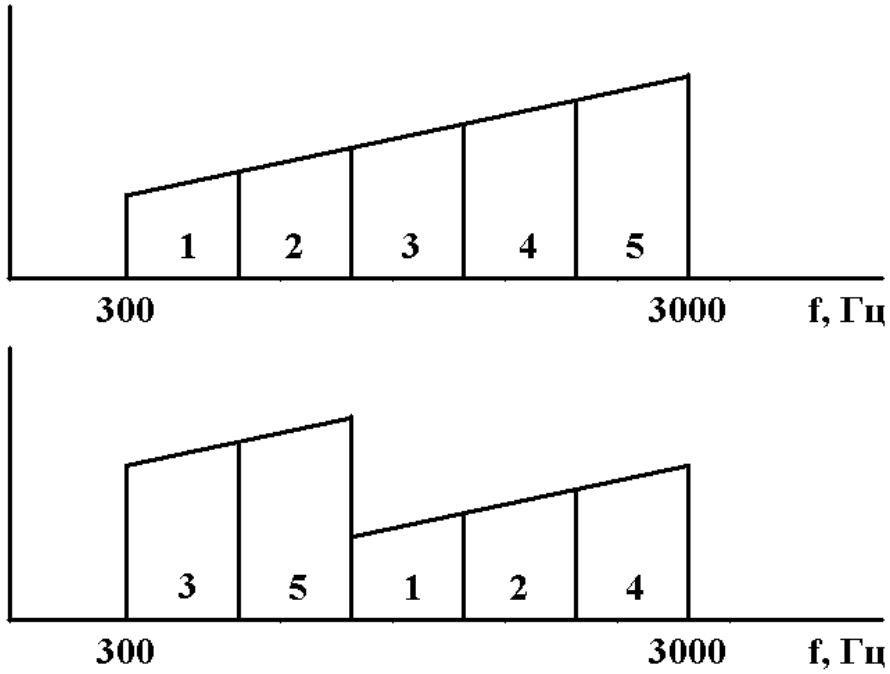

Рис. 189. Частотные перестановки в спектре передаваемого сигнала

Аналоговые скремблеры

Наиболее высокий уровень стойкости при аналоговом кодировании получается с помощью объединения как временных, так и частотных перестановок. При этом временные манипуляции разрушают смысловой строй, а частотные преобразования перемешивают гласные звуки. Количество частотных полос обычно берется не больше 5-6.

Устройства, которые реализуют вышеописанные операции, получили название аналоговых скремблеров.

Если вам понравился данный способ защиты и вы решили приобрести аналоговый скремблер, то при выборе такого типа устройств в первую очередь, обратите внимание не на число возможных ключевых комбинаций (изюминка любой рекламы), а на сложность преобразований, которые в нем применены.

В простейших скремблерах, защищающих лишь от прямого прослушивания, дилетантами, используются только частотные перестановки и инверсии (число каналов не превышает 4, интервалы коммутации – постоянны).

В скремблерах среднего класса, обеспечивающих гарантированную стойкость на время в несколько часов, применяются частотно-временные перестановки с числом частотных каналов от 5 до 10.

В сложных скремблерах, обеспечивающих стойкость на несколько дней, должны быть переменными интервалы коммутации, использоваться частотно-временные перестановки с большим (более 10) количеством частотных каналов и переставляемыми временными интервалами. Число возможных ключевых комбинаций должно быть более 10^{15} .

Следует обращать внимание и на то, какой вид связи поддерживает скремблер:

- *Симплексный* (передача информации только в одном направлении);
- *Полудуплексный* (поочередный обмен информацией);
- *Дуплексный* (одновременный двусторонний обмен).

Данное обстоятельство, в сочетании с человеческим фактором, иногда оказывает существенное влияние на защиту информации. В качестве примера можно привести следующий интересный факт, взятый из книги, с цитаты из которой мы начали это раздел.

«Мубарак (президент Египта) недолюбливал закрытую систему телефонной связи, поставленную Соединенными Штатами. Она представляла собой аппарат с ручным переключением на «разговор» и «прослушивание» (симплексный скремблер). При пользовании им вести одновременный обмен мыслями было невозможно, поэтому Мубарак предпочитал обычный телефон. Администрацией США было отдано распоряжение об усилении сбора информации разведывательными службами в Египте, особенно АНБ при помощи спутников. 10 октября рано утром был перехвачен телефонный разговор Мубарака со своим министром иностранных дел, и через полчаса это совершенно секретное сообщение поступило в Ситуационную комнату Белого дома».

Практика показывает, что для деловых бесед, а не отдачи команд, необходимо использовать только скремблеры, работающие в дуплексном режиме с максимально упрощенной системой управления (в наилучшем случае переключение должно осуществляться нажатием одной кнопки).

Примером неплохого скремблера, реализующего вышеописанные алгоритмы, может служить устройство компании Thomson-CSF.

TRS 769 – аналоговый скремблер. Производит запись речевого сигнала в электронную память с последующим образованием выборок из 24-мс сегментов, которые, в свою очередь, рассеиваются с помощью специально генерируемой псевдослучайной последовательности с образованием 14 групп. Далее сигнал объединяется с обратным псевдослучайно распределенным спектром, что еще больше защищает исходное сообщение. Амплитуды

сегментов речевых сигналов поддерживаются на уровне ниже среднего уровня обычных звуков речи. Применение такого метода позволяет создать полную неопределенность относительно положения по времени каждого сегмента, повышая тем самым уровень защиты системы. Более того, сам закон, управляющий временной обработкой речевого сигнала, меняется от сегмента к сегменту неповторяющимся и непредсказуемым способом, поскольку он тоже контролируется сигналами псевдослучайной последовательности.

13.2. Цифровое шифрование

Теперь, рассмотрим цифровой способ закрытия, при котором речевой непрерывный сигнал предварительно преобразуется в дискретный вид [13]. Согласно одной из основных теорем теории информации, любой непрерывный сигнал может быть без потерь заменен последовательным набором своих мгновенных значений, если они берутся с частотой, не менее чем в 2 раза превышающей самую высокочастотную составляющую этого сигнала. Для стандартного телефонного канала это означает, что такая дискретизация должна происходить с частотой не менее 6 кГц, так как верхняя частотная составляющая телефонного сигнала ограничивается верхним частотным пределом телефонного канала, равным всего 3 кГц.

Дискретизация непрерывного сигнала

Максимальное расстояние между точками *t1, t2, t3* ... на временной оси (рис. 190) не должно превышать T=1/2F, где F – максимальная частотная составляющая непрерывного сигнала. В этом случае непрерывная кривая полностью описывается последовательностью дискретных значений $[A_i]$ и временным интервалом *t*.

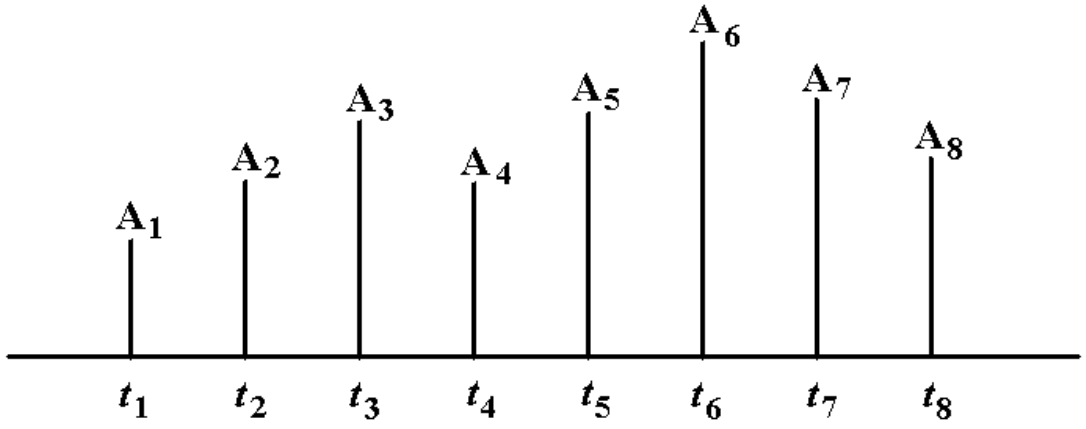

Рис. 190. Пример временной дискретизации непрерывного сигнала

Если мы представим эти значения в виде набора чисел, то переведем сигнал в цифровую форму. Теперь эти числа можно будет легко зашифровать

любым известным способом. В этом плане способ цифрового шифрования является более универсальным, и на рынке предлагаются такие типы скремблеров, которые могут шифровать все виды передаваемой информации – от буквенно-цифровой до изображений. При этом все предварительно преобразуется в цифровую форму. В канал связи выдается набор дискретных знаков (как правило, нулей и единиц).

Однако и здесь возникают некоторые особенности. *Первая особенность* – это необходимость быстрой выработки огромного объема символов шифра, естественно, если мы хотим сохранить высокое качество сигнала. В самом деле, если нам надо передать минимально необходимые 6000 мгновенных значений сигнала в секунду, а его динамический диапазон равен, скажем, 20 дБ (это означает, что максимальная амплитуда сигнала в 10 раз больше его минимального значения), то в 1 с нам нужно сформировать не менее 6000×4 = 24000 двоичных знаков шифра (дело в том, что для представления 10 в двоичной системе счисления нам требуется 4 двоичных знака), то есть скорость формирования шифра и передачи кодированной информации в линию в этом случае должна быть не менее 24 кбит/с, что достаточно проблематично осуществить по стандартному телефонному каналу.

Следовательно, *второй особенностью* при цифровом шифровании речевого сигнала является требование наличия гораздо более широкой полосы частот для передачи двоичного сигнала в зашифрованном виде, чем имеется у стандартного телефонного канала. Это сильнейшее ограничение на применение цифрового шифрования, работающего по такой схеме.

Только использование специфичных характеристик речевого сигнала и применение различных сложных технических и математических способов позволяют резко сузить требуемую полосу и передать зашифрованный цифровым способом речевой сигнал по стандартному телефонному каналу.

Преобразование речевого сигнала

Обычно для преобразования речевого сигнала используется так называемый вокодер – устройство, выделяющее существенные параметры речи и преобразующее их в цифровую форму. Однако в этом случае, хотя речь и сохраняет требуемую разборчивость, опознать собеседника по тембру голоса часто бывает затруднительно, так как голос воспроизводится речевым синтезатором и имеет однообразный «металлический» оттенок. Правда, если для сигнала, зашифрованного цифровым способом, использовать канал с широкой полосой (волоконно-оптическую линию или радиорелейную связь), то можно сделать качество речевого сигнала достаточно высоким.

Для нормальной работы телефона с устройством защиты на отечественных телефонных каналах скорость передачи информации на выходе блока

шифрации, а значит и вокодера, не должна превышать 4800 бит/с. При этом слоговая разборчивость достигает 99 % при вполне удовлетворительной узнаваемости голоса абонента. Кстати, обычный телефонный канал считается каналом среднего качества, если обеспечивает слоговую разборчивость порядка 85-88 %.

По результатам ряда исследований на московских телефонных линиях получены следующие данные: нормальную работу на скорости передачи 2400 бит/с обеспечивают почти 90 % каналов связи, на скорости 4800 бит/с – уже только 60 % и на скорости 9600 бит/с – всего 35 %. Следовательно, наиболее надежную работу обеспечит аппаратура со скоростью передачи информации 2400 бит/с. В идеале слоговая разборчивость должна быть не хуже, чем в обычном телефонном канале.

Синхронизация и ввод ключей

При цифровом шифровании речевого сигнала сложной проблемой (вследствие высоких скоростей передачи информации) является и проблема ввода ключей, а также проблема синхронизации. Необходимо добиться того, чтобы шифраторы на приемном и передающем концах линии связи начинали работать строго одновременно и не уходили ни на один такт во время всего сеанса. При этом должны сохраниться такие ценные качества телефонной связи, как удобство ведения разговора и быстрота вхождения в связь. Это удается достичь только за счет существенного усложнения аппаратуры, зачастую с введением в ее состав устройств компьютерного типа. Поэтому пусть вас не удивляет очень высокая стоимость хорошего цифрового скремблера.

Зато к несомненным достоинствам систем с цифровым шифрованием можно отнести высокую надежность закрытия информации, особенно при использовании стандартизированных на государственном уровне алгоритмов шифрования таких, как DES (США) и ГОСТ 28147-89 (Россия).

Алгоритм DES (Data Encryption Standard) стал результатом плодотворного сотрудничества трех организаций – Национального бюро стандартов (NBS), Управления национальной безопасности (NSA) и фирмы IBM. Он стал одним из первых «открытых» шифроалгоритмов, схемы которого были опубликованы еще 17 марта 1975 года. Секретными для него являются только ключи, с помощью которых осуществляется кодирование и декодирование информации.

Другим преимуществом систем цифрового кодирования является возможность применения открытого распределения ключей: в такой аппаратуре перед каждым сеансом связи передатчик и приемник автоматически обмениваются открытыми ключами, на основе которых вычисляется секретный се-

ансовый ключ. Использование этого метода снимает проблему изготовления и рассылки ключей, а также исключает утечку информации из-за недобросовестного хранения и обращения с ключевыми носителями. Недостатками устройств этого класса являются техническая сложность, неустойчивая работа в каналах с большим затуханием и низкая узнаваемость голоса абонента.

При ведении переговоров работа генератора псевдослучайной последовательности происходит по заданному алгоритму, причем начальная установка для каждого нового разговора вырабатывается и устанавливается в шифраторе заново сразу после ввода ключа, при этом в хорошем скремблере синхронизация осуществляется настолько быстро, что собеседники этого просто не замечают. Выпускаются также универсальные телефонные шифраторы, которые могут работать с различными видами линий связи. При этом степень закрытия остается одинаково высокой, а качество речи тем выше, чем шире полоса пропускания канала. Такая универсальность достигается с помощью модемов и дополнительных связных устройств (рис. 191).

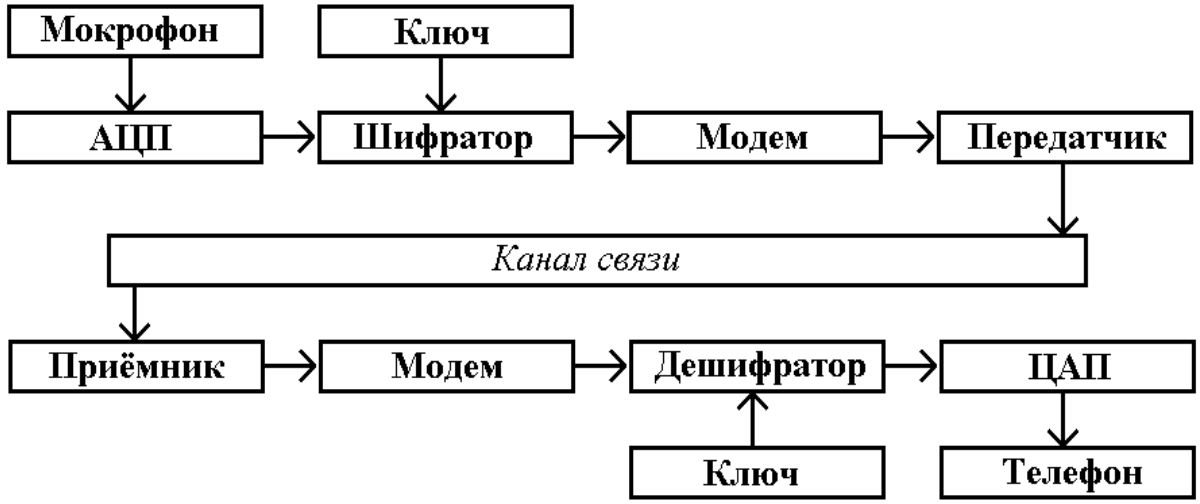

Рис. 191. Схема организации закрытого канала связи

Сравнительная оценка аналогового и цифрового закрытия сигналов

В табл. 33 приведена сравнительная характеристика двух принципов закрытия речевого сигнала (аналогового и цифрового). Преимущества цифрового метода шифрования над аналоговым хорошо видны из таблицы. Однако они достигаются за счет отказа в большей части случаев от стандартного телефонного канала или за счет применения сложной и очень дорогостоящей аппаратуры. Ясно, что когда интенсивность переговоров невысока, применение таких устройств может стать экономически неоправданным.

Таблица 28.

Характеристики	Вид преобразования	
	Аналоговое	Цифровое
Наличие переговоров в линии связи	Есть отчетливые признаки	Нет никаких признаков, так как при отсутствии переговоров в линию идет чистый шифр
Распределение амплитуды сигнала	Есть ритм и громкость	Однородная двоичная последовательность
Остаточная разборчивость	Есть признаки начала слова и фразы, паузы	Постоянный однородный шум
Кратковременный спектр сигнала	Спектральные характеристики неоднородны	Однородный

Основной характеристикой цифровых шифраторов является применение того или иного криптографического алгоритма. При этом надежность алгоритма считается высокой, если число ключевых комбинаций более 10^{25}. Следует помнить, что длина ключа у таких устройств порядка 30 цифр, что крайне затрудняет его ввод с клавиатуры. Следовательно, при приобретении оборудования необходимо обращать внимание на то, в какой форме выполнен ключевой носитель, насколько он надежен и прост в обращении. Если вы, например, купили более дешевый прибор с ручным вводом ключа, то при необходимости срочно позвонить, набирая номер, не давайте волю эмоциям – «нервные клетки не восстанавливаются».

13.3. Технические средства

Защита телефонных переговоров

Государственные органы всех стран также существенное внимание уделяют защите телефонных переговоров. Так, главным направлением деятельности по защите линий связи Агентство национальной безопасности (АНБ) США считает установку во всех правительственных учреждениях и на фирмах подрядчиках Пентагона специальных защищенных телефонных аппаратов по программе STU (Secure Telefon Unit). В настоящее время наиболее распространены изделия третьего поколения типа **STU-3**, причем в некоторых компаниях установлено более 100 комплектов. Всего в США используется более 700 тысяч телефонов данного типа (цена порядка $2000).

Телефон **STU-3** внешне похож на обычный телефонный аппарат, но он дает возможность вести телефонные переговоры как в открытом режиме, так и в защищенном со скоростью обмена цифровой информацией 2400 бит/с.

Ключи для сотрудников правительственных учреждений изготовляются в АНБ, а для фирм-подрядчиков – корпорацией GTE.

Для включения аппарата в защищенный режим пользователь вставляет ключ (в виде пластиковой карточки) в приемное устройство телефона. В память ключа занесены следующие идентификационные данные: фамилия и имя пользователя; название фирмы; высший гриф секретности информации, к которой он допущен.

Когда связь установлена, идентификационные данные пользователя и категория его допуска высвечиваются на дисплее аппарата его собеседника. Аппаратура рассчитана на 4 уровня секретности. Переход в закрытый режим может осуществляться как до начала, так и в процессе разговора. После того как оба абонента вставили свои ключи в аппарат и нажали кнопку «защита», идентификационные данные каждого ключа направляются в компьютер АНБ, где проверяется, не происходила ли утрата одного из ключей.

В настоящее время выпускается большое количество дополнительных устройств к аппаратуре **STU-3**. Так, компания «Моторола» изготовляет портативные модели телефонов **STU-3** для сотовых систем мобильной связи, но стоимость их около $10 000.

В России также ведутся работы по массовому внедрению специально разработанной техники в государственные организации и фирмы, работающие с ними. Так, на проходившей в 1995 году выставке «Связь-Экспоком», были представлены междугородняя АТС «**Фобос-КМ**» и учрежденческая АТС «**Сателлит**», где циркулирующая информация защищена от утечек как техническими, так и криптографическими методами.

Отечественный аналог STU «**Гамма**», хотя внешне неказист, но по словам разработчиков, сравним по процессорной мощности с пятью «пентиумами» и обеспечивает практически абсолютную конфиденциальность переговоров.

Защита информации при факсимильной и телексной связи

Разработана аппаратура для закрытия передачи информации по *факсимильной* и *телексной* связи.

FSR-2000 – факсовый шифратор. Подключается между факсимильным аппаратом и розеткой. Шифрующее устройство работает автоматически, при этом специальная функция идентификации (до сотни фамилий и телефонных номеров) позволяет выбрать шифрующее устройство адресатов для проведения обмена информацией. Кроме того, аппаратура сообщает о наличии на набранном номере шифрующего устройства. Габариты изделия не превышают 305×250×64 мм, вес –2,5 кг. Более поздняя модификация FSR-3000 использует стандартный алгоритм DES.

Абонентские терминалы для передачи конфиденциальных данных

Некоторое распространение получили абонентские терминалы, предназначенные для передачи конфиденциальных данных и буквенно-цифровых текстов по телефонной сети общего назначения, а также через УКВ-радиостанцию.

«Исса» – многофункциональное кодирующее устройство. Устройство конструктивно выполнено в корпусе «дипломата» (габариты 480×340×100 мм), имеет клавиатуру, дисплей, адаптеры для акустического подключения к трубке телефонного аппарата. Ввод данных может производиться как со встроенной клавиатуры, так и из внешней ПЭВМ. Скорость передачи данных 600 или 1200 бит/с. Время передачи 2560 знаков – не менее 1,5 мин. Аппаратура обеспечивает невозможность прочтения информации в линии связи без знания пароля в течение 2 лет. Длина пароля – 32 знака. Питание возможно как от сети 220 В, так и от встроенного аккумулятора. Вес устройства – не более 7 кг.

Практические советы по выбору скремблера

Следует отметить, что, судя по высказываниям специалистов подразделения «Группы А» (в АНБ она отвечает за анализ и дешифровку перехваченных сигналов российских радиостанций), в последнее время США не удалось раскрыть ни одного из основных российских шифров.

В связи с внедрением техники закрытия телефонных сообщений высокого качества и в коммерческую область успехи аналитического дешифрирования в АНБ этих материалов тоже носят весьма ограниченный характер. В целом, с началом 80-х годов четко обозначилась тенденция: усилия по дешифровке дают все меньше и меньше результатов. Для добывания условной единицы информации приходится затрачивать все больше и больше средств. Как видите, криптозащита – «крепкий орешек» даже для государственных структур. Приведём несколько практических советов по выбору скремблера:

- не покупайте дешевые модели, поверьте – это пустая трата денег, так как в них очень простые методы закрытия сигнала и надо 2–3 мин для адаптации подслушивающей аппаратуры среднего класса;
- не берите самоделок – работа с ними стоит в одном ряду с Танталовыми муками, поскольку уже после нескольких сеансов вхождение в синхронизм будет осуществляться с очень большой задержкой;
- при выборе конкретной модели не следует доверять рекламе, а лучше посоветуйтесь с нейтральным экспертом.

По уровню защиты хороши скремблеры московской фирмы «Максом» серии **СКР** (аналого-цифровой способ преобразования сигнала). Однако эти, в принципе очень надежные приборы, довольно сложны в эксплуатации.

Абонент не только должен манипулировать четырьмя кнопками, но и постоянно следить за индикатором, что требует определенных навыков в работе и практически не дает сосредоточиться на разговоре (цена $400–$800).

Зеленоградская фирма «АНКАД» выпустила очень удачный скремблер «**Орех-А**». Прибор не бросается в глаза, поскольку выполнен в виде подставки под телефонный аппарат и имеет только одну кнопку. Это изделие смело может претендовать на оценку одного из лучших отечественных приборов данного класса по критерию стоимость/эффективность (цена около $400). Внешний вид скремблера представлен на рис. 192.

Рис. 192. Скремблер «Орех-А»

Для абонентов сотовой связи также существуют специально разработанные скремблеры, которые закрепляются непосредственно на трубке и кодируют акустический сигнал. Внешний вид такого устройства (**ASC-2**) приведен на рис. 193.

Рис. 193. Маскиратор речи «ASC-2»

Защита телефонов с радиоудлинителями

Рассмотрим обеспечение безопасности телефонов с радиоудлинителями. Всего 10 лет назад домашние беспроводные телефоны были в диковинку, теперь они широко используются в наших квартирах и офисах, вытесняя своих предшественников, намертво привязанных к телефонной розетке. Перечислять все достоинства таких аппаратов смысла нет – они очевидны. Но, как это часто бывает, достоинства не обходятся без недостатков. Главная проблема домашних беспроводных радиотелефонов – радиопомехи. Многие слышали о том, что при включении телефона перестает работать телевизор, притом на самом интересном месте. Но это еще полбеды. Гораздо хуже, когда сигнал вашего радиотелефона перехватят «доброжелатели». Как уже говорилось выше, наличие такого аппарата у поднадзорного лица – «голубая мечта» любого специалиста по промышленному шпионажу. Существует несколько методов, позволяющих частично решить эту проблему, но мы не будем на них останавливаться, поскольку задача легко решается радикально.

В 1992 году был разработан новый стандарт для беспроводной телефонной связи. Он получил название DECT (Digital Enhanced Cordless Telecom-munications, что означает «Цифровая усовершенствованная беспроводная связь»). Кратко охарактеризовать этот стандарт можно так: «младший брат GSM». Хотя несколько отличий все-таки есть, но по сути это очень близкие технологии.

Мощность передатчиков в трубке и базе очень низкая (10 мкВт), что, с одной стороны, повышает скрытность и гарантирует безопасность для здоровья людей, но, с другой – ограничивает дальность действия (около 50 м – в помещении). Но, конечно, главные достоинства стандарта DECT, как и его «старшего брата», заключаются в высоком качестве связи и ее надежной защищенности от прослушивания и «подсадок» от других телефонов. Внешне аппарат стандарта DECT очень напоминает обычный домашний радиотелефон (рис. 194) и совершенно не отличается от последнего по правилам пользования.

Рис. 194. Телефонный аппарат Spree стандарта DECT

Защита УКВ-радиосвязи

Наша информация о системах криптозащиты будет неполной, если не поднять вопрос, который очень часто задают начальники достаточно солидных служб безопасности: как защитить УКВ-радиосвязь, используемую для диспетчерских нужд при охране объектов, сопровождении транспортных средств, проведении каких-либо мероприятий и т. д. Доводим до сведения заинтересованных лиц, что для этих целей разработано несколько моделей специальных скремблеров. Большинство из них реализует частотную инверсию сигнала, и все они имеют очень близкие параметры и устанавливаются в корпусе радиостанции.

Одними из первых на рынке появились приборы фирмы Selectone такие, как **SS-20** и более поздняя модель **ST-022**. Скремблеры работают в диапазоне частот 300...4000 Гц и обеспечивают инверсию сигнала относительно 8 номиналов частот. Габариты – 39×21×14 мм. Стоимость – около $50.

Скремблеры фирмы Midian типа **VPV** имеют 15 частот инверсии и стоят от $35 до $75.

Более сложное преобразование сигнала происходит в разработанных НТЦ «ИНТЕРВОК» скремблерах типа «**Сонет**». Здесь спектр речевого сигнала делится на две части, каждая из которых разворачивается вокруг своих средних частот. Приборы имеют очень малые размеры (15×15×6,5 мм) и легко устанавливаются внутри корпуса практически любых радиостанций. Стоимость (включая установку) – от $50 до $80.

Таким образом, для пользователя на рынке спецтехники представлен достаточно широкий выбор. Вместе с тем желающим приобрести средства УКВ-связи, обеспечивающие защиту информации, хотелось бы все-таки рекомендовать при закупке подходить к проблеме комплексно, то есть на начальном этапе четко определиться по уровню защиты. Помните – аналоговые скремблеры никогда не обеспечат защиту от преднамеренного прослушивания ваших переговоров, если используется специальная аппаратура перехвата. При этом финансовые затраты лиц, ведущих съем информации, не будут являться для них препятствием (стоимость профессиональной аппаратуры для перехвата сигнала, закрытого таким скремблером или открытого, не изменится). Для действительно надежной защиты информации в радиоканалах необходимо использовать станции с передачей сигнала в цифровой форме. Такую защиту может обеспечить применение более дорогих цифровых радиостанций или использование цифровых устройств защиты информации для аналоговых систем. Подобная аппаратура уже выпускается рядом организаций.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК.

Рекомендуемая основная литература.

1. Акустика: Справочник. / *Ефимов А.П., Никонов А.В., Сапожников М.А., Шоров В.Й.* / Под ред. М.А. Сапожкова. 2-е изд., перераб. и доп.— М.: Радио и связь, 1989. — 336 с.
2. *Вартанесян В. А.* Радиоэлектронная разведка. – М.: Воениздат, 1991.– 254 с.
3. *Верещагин И.К., Косяченко Л.А., Кокин СМ.* Введение в оптоэлектронику: Учебное пособие для втузов.— М.: Высшая школа, 1991. — 191 с.
4. *Волин М. Л.* Паразитные процессы в радиоэлектронной аппаратуре. М: «Радио и связь», 1981, 296 с.
5. *Гауэр Дж.* Оптические системы связи / Пер. с англ. — М.: Радио и связь, 1989. — 504 с.
6. *Гольдштейн ЛД., Зернов Н.В.* Электромагнитные поля и волны. Изд. 2-е, перераб. и доп.— М.: Сов. радио, 1971.— 664 с.
7. Закон Р Ф «О государственной тайне» от 21 июля 1993 г. № 5485-1.
8. Закон РФ «Об информации, информатизации и защите информации» (в редакции от 20.02.95 г. № 24–Ф3).
9. *Зима В.М., Молдовян А.А., Молдовян Н.А.* Безопасность глобальных сетевых технологий. – СПб: Издательство Санкт-Петербургского университета, 1999. - 368 с.
10. *Лагутин В. С., Петраков А. В.* Утечка информации в телефонных каналах. М.: Энергоатомиздат, 1996, 304 с.
11. *Лысов А. В., Остапенко А. Н.* Промышленный шпионаж в России: методы и средства.– СПб.:Лаборатория ППШ, 1994.–71 с.
12. *Лысов А. В., Остапенко А. Н*. Телефон и безопасность.– СПб, Лаборатория ППШ, 1995.– 105 с.
13. *Молдовян А.А., Молдовян Н.А., Гуц Н.Д., Изотов Б.В.* Криптография: скоростные шрифты. - СПб.: БХВ - Петербург, -2002. – 496 с.
14. Организация и современные методы защиты информации. /Под общей редакцией *С. А. Диева и А. Г. Шаваева*/. М.: Концерн «Банковский Деловой Центр», 1998, 472 с.
15. *Петраков А. В.* Основы практической защиты информации. М.: Радио и связь, 1999, 368 с.
16. *Петраков А. В., Дорошенко П. С., Савлуков Н. В.* Охрана и защита современного предприятия. М.: Энергоатомиздат, 1999, 568 с.
17. Петровский В.И., Седельников Ю.Е. Электромагнитная совместимость радиоэлектронных средств: Учебное пособие для вузов. — М.: Радио и связь, 1986. — 216с.

18. Радиовещание и электроакустика: Учебник для вузов / Под ред. проф. М.В. Гитлица. — М.: Радио и связь, 1989.— 432 с.
19. *Сапожков М.А.* Электроакустика: Учебник для вузов.— М.: Связь, 1978. — 272 с.
20. Совместимость радиоэлектронных средств электромагнитная. Термины и определения. ГОСТ 23611—79. М.: Госкомитет СССР по стандартам.— 1979.— 8 с.
21. *Спесивцев А.В., Вегнер А, Кругляков А.Ю.* Защита информации в персональных ЭВМ. — М.: Радио и связь, МП «Веста», 1992. — 192 с.
22. Технические методы и средства защиты информации/*Ю. Н. Максимов, В. Г. Сонников, В. Г. Петров* и др. СПб.: ООО «Издательство Полигон», 2000.—320 с.
23. *Торокин А. А.* Основы инженерно-технической защиты информации. М: «Ось-89», 365 с.
24. *Халяпин Д. Б., Ярочкин В. И.* Основы защиты информации.– М.:ИПКИР, 1994.– 125 с.
25. *Хорев А. А.* Защита информации от утечки по техническим каналам утечки информации. Часть 1. Технические каналы утечки информации. М.: Гостехкомиссия России, 1998, 320 с.
26. *Хорев А. А.* Методы и средства поиска. Электронные устройства перехвата информации. М.: МО РФ, 1998, 224 с.
27. *Хорев А. А.* Способы и средства защиты информации.– М.: МО РФ, 1998.–316 с.
28. Электромагнитная совместимость радиоэлектронных средств и непреднамеренные помехи. Пер. с англ. Вып. 1-3. М.: «Советское радио», 1977, 1978, 1979.
29. Энциклопедия промышленного шпионажа/ *Ю.Ф. Каторин, Е.В. Куренков, А.В. Лысов, А.Н. Остапенко* / под общ. ред. Е.В. Куренкова – С.-Петербург: ООО «Издательство Полигон», 1999, -512с.
30. *Ярочкин В. И.* Технические каналы утечки информации.– М.:ИПКИР, 1994. – 106 с.

Дополнительная литература.

31. *Абалмазов Э. И.* Направленные микрофоны: мифы и реальность// Системы безопасности, август-сентябрь, 1996, с. 98–100.
32. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Руководящий документ. Гостехкомиссия России. М.: 1995. — 36с.
33. *Агеев А. С.* Организация работ по комплексной защите информации //Информатика и вычислительная техника.– 1993, № 1,2, с. 71–72.
34. *Аксенов Л.* Осторожно. Вас подслушивают //Новости разведки и контрразведки.– 1995.– № 7–8 (40-41).– с. 13.
35. *Альбац Е.* Мина замедленного действия. – М.: Русслит, 1992.– 416 с.
36. *Андрианов В. И., Соколов А. В.* Шпионские штучки-2, или как сберечь свои секреты.– СПб.: Лань, 1997.– 348 с.
37. *Андрианов В. И.* и др. Шпионские штучки и устройства для защиты объектов и информации.– СПб.: Лань, 1995.–272 с.
38. Атакующая спецтехника «RV» украинской фирмы «ВЕЧЕ».– Защита информации.– № 2.– 1994.– с. 62–76.
39. *Барсуков В.С., Водолазский В.В.* Интегральная безопасность информационно-вычислительных и телекоммуникационных сетей (Часть 1) // Технологии электронных коммуникаций. Т. 34. М., 1993.-146 с.
40. *Барсуков В. С., Водолазкий В. В.* Современные технологии безопасности. М.: «Нолидж», 2000, 496 с.
41. *Батраков А. С., Минеев В. В.* Прикладная оптика.– МО, 1992.– 518 с.
42. «Благополучная» Германия//Частный сыск. Охрана. Безопасность.– 1995.– № 6.– с. 29.
43. *Боголепов Н.Г.* Промышленная звукоизоляция.— М.: Судостроение, 1987. — 346с.
44. *Болконский В.В.* Аппаратура опросной сигнализации фирмы «СК» Systems, Inc»: Справочное пособие.— СПб.: СПбГААП. 1995.—66 с.
45. *Брусницин Н. А.* Открытость и шпионаж.– М.: Военное издательство, 1991.– 56 с.
46. *Бушминский И.П.* Изготовление элементов конструкций СВЧ.— М.: Высшая школа,1974.—302 с.
47. *Вакин СД., Шустов Л.Н.* Основы радиопротиводействия и радиотехнической разведки.— М.: Сов. радио, 1968.— 448 с.
48. Вакка Д. Безопасность Internet: Пер. с англ. - М.: «Бук Медиа Паблишер». -1998.

49. *Варне Дж.* Электронное конструирование: Методы борьбы с помехами. Пер. С англ. — М.: Мир, 1990. — 238 с.
50. *Василевский В. И.* Реализация современной концепции построения комплексов обнаружения средств негласного съема конфиденциальной информации в последней разработке НПЦ Фирма «НЕЛК» – универсальной базовой поисковой программе FILIN//Системы безопасности.– № 6, ноябрь – декабрь 1996.– С. 66–67.
51. Вашу безопасность обеспечит техника фирмы «НОВО»//Каталог продукции и услуг.– 1995.– 69 с.
52. *Виноградов А. В., Волков В. В.* Спецтехника.– М.: Лаборатория LB бизнеса, 1996.– 13 с.
53. *Волхонский В. В.* Устройства охранной сигнализации. СПб.: Экономпис и культура, 1999, 272 с.
54. *Волхонский В.В., Нейменов М.И.* Телевизионные системы наблюдения и приборы ночного видения. Охрана и безопасность. Курсы ТСО.— СПб.: Экополис и культура, 1994. — 56 с.
55. *Воробьев Е.Д.* Экранирование СВЧ-конструкций.— М.: Сов. радио, 1979.— 134с.
56. *Вудворд Б.* Признание шефа разведки: Пер. с англ.– М.: Политиздат, 1990.– 479 с.
57. *Гавриш В.* Практическое пособие по защите коммерческой тайны. Симферополь: "Таврида", 1994, 112 с.
58. *Гасанов Р. М.* Промышленный шпионаж на службе монополий.– М.: Политиздат, 1989.– 267 с.
59. *Герасимёнко В.А.* Защита Информации в автоматизированных системах обработки данных. Кн. 1, - М. Энергоатомиздат, 1994.— 400 с.
60. *Герасименко В.А., Малюк А.А.* Учебник. Основы защиты информации. М.:ООО Инкомбук, 1997.
61. *Демин В. П., Куприянов А. И., Сахаров А. В.* Радиоэлектронная разведка и радиомаскировка. М.: Изд-во МАИ, 1997, 156 с.
62. *Джамса К.* Модернизация компьютера/Пер. с англ.– Мн.: Попурри, 1997.– 352 с.
63. *Драбкин АЛ., Зузенко ВЛ, Кислое А.Т.* Антенно-фидерные устройства. Изд. 2-е, доп. и перераб.— М.: Сов. радио, 1974.— 536 с.
64. Дунаев С. INTRANET-технологии. WebDBC. CGI. CORBA 2.0. Netscape. Suite. IntraBuilder. Java. JavaScript LiveWire. - М.: «Диалог-МИФИ». - 1997.
65. Закон РФ «Об актах гражданского состояния» (в редакции от 15.11.97 г.).
66. Закон РФ «О безопасности» (в редакции от 05.03.92 г.).

67. Закон РФ «О частной детективной и охранной деятельности» (в редакции от от 11.03.92 г. № 2487–1) //Российская газета, № 100, 30.04.92 г.
68. Закон РФ «О правовой охране программ для электронных вычислительных машин и баз данных».
69. Закон РФ «О связи» (в редакции от 20 .01.95 г.).
70. Закон РФ «О сертификации продукции и услуг» (в редакции от 10.06.93 г.).
71. Закон РФ «О федеральных органах правительственной связи и информации» (в редакции от 19.02.93 г. № 4524–1).
72. Закон РФ «Об оперативно-розыскной деятельности»//Собрание законодательства Российской Федерации, 1995.– № 33.
73. Защита информации в компьютерных системах. Вып. 2. Элементы криптологии / Под ред. *П.Д. Зегжды*.— СПб., 1993.— 146 с.
74. Защита информации в системах и средствах информатизации и связи: Учебное пособие.— СПб.: ВИКА, 1996.— 113 с.
75. Защита от несанкционированного доступа к информации. Термины и определения. Руководящий документ. Гостехкомиссия России. М., 1992.— 12 с.
76. Защита от шума: Справочник проектировщика / Под ред. *Е.А. Юдина*.— М.: Стройиздат, 1983. — 210 с.
77. *Зегжда Д.П., Ивашко А.М.* Как построить защищенную информационную систему. - 4.1. - СПб: Мир и Семья. -1997.
78. *Зегжда Д.П., Ивашко А.М.* Как построить защищенную информационную систему. - 4.2. Технология создания безопасных систем. - СПб: Мир и Семья. -1998.
79. *Зима В.М., Молдовян А.А.* Многоуровневая защита информационно-программного обеспечения вычислительных систем: Учеб. пособие. - СПб: издательско-полиграфический центр ТЭТУ. -1997.
80. *Зима В.М., Молдовян А.А.* Многоуровневая защита от компьютерных вирусов: Учеб. пособие. - СПб: издательско-полиграфический центр ТЭТУ. -1997. – 170 с.
81. *Зима В.М., Молдовян А.А., Молдовян Н.А.* Защита компьютерных ресурсов от несанкционированных действий пользователей: Учеб. пособие. - СПб: типография Военной Академии Связи. -1997.
82. *Зима В.М., Молдовян А.А., Молдовян Н.А.* Компьютерные сети и защита передаваемой информации. - СПб: издательство СПбГУ. -1998.
83. *Зима В.М., Молдовян А.А., Молдовян Н.А.* Основы резервирования информации и архивация файловых данных в вычислительных системах: Учеб. пособие. - СПб: издательство СПбГУ. -1998.

84. *Зима В.М., Молдовян А.А., Молдовян Н.А.* Резервирование системных данных компьютера и безопасная инсталляция программ: Учеб. пособие. - СПб: издательство СПбГУ. -1998.
85. *Зима В.М., Молдовян А.А.* Схемы защиты информации на основе системы «Кобра»: Учеб. пособие. - СПб: издательско-полиграфический центр ТЭТУ. -1997.
86. *Зима В.М., Молдовян А.А.* Технология практического обеспечения информационной безопасности: Учеб. пособие. - СПб: издательско-полиграфический центр ТЭТУ. -1997. – 117 с.
87. *Зотов-Кондратов Э. С.* «Альфа-4»: комплект аппаратуры беспроводного видеонаблюдения. //Системы безопасности.– № 6 (12), ноябрь – декабрь. 1996, с. 82–83.
88. *Зубак А.Д.* Извещатели оптронно-пожарной сигнализации: Учебное пособие.— Воронеж: Воронежская высшая школа МВД РФ, 1995. — 120 с.
89. *Иоффе В. К., Корольков В. Г., Сапожков М. А*. Справочник по акустике/под ред. М. А. Сапожкова.– М.: Связь, 1979.– 312 с.
90. *Калинин А. И., Черенкова Е. Л*. Распространение радиоволн и работа радиолиний.– М.: Связь, 1972.– 439 с.
91. Каталог 1994 //Smirab Electronics Ltd.,.– 90 p.
92. Каталог 1995// НПО «Защита информации».– 1995.– 56 с.
93. Каталог 1996–1997//НПО «Защита информации»,– 1997.– 32 с.
94. Каталог наименований сыскной и охранной спецтехники. НПО «Защита информации», 1994.
95. Каталог продукции и услуг 2000. СПб: Агентство технической безопасности «НИМРОД», 2000.-100с.
96. *Кейт Х. Мелтон*. Шпионские фотокамеры//Безопасность.– № 5, 1998, с. 28–31.
97. *Киселев А. Е.* и др. Коммерческая безопасность/ Под ред. В. М. Чаплыгина – М.: ИнфоАрт, 1993.– 128 с.
98. *Ковалев А. Н*. Защита информации: правила и механизм лицензирования//Системы безопасности.– 1995.– № 5, с. 8–10.
99. Кодекс РСФСР об административных правонарушениях.– М.: Теис, 1996.– 190 с.
100. Комплексные системы защиты информации//Каталог фирмы Дивекон 1995.– 72 с.
101. Конструкции СВЧ устройств и экранов: Учебное пособие для вузов / Под ред. *А.М. Чернушенко*.— М.: Радио и связь, 1983. — 400 с.
102. Контроль людей и их ручной клади на наличие диверсионно-террористических средств//Специальная техника. № 3, 1998, с. 41–49.

103. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Руководящий документ. Гостехкомиссия России. М., 1992.— 12с.
104. *Куренков Е. В., Лысов А. В., Остапенко А. Н.* Рекомендации по оценке защищенности конфиденциальной информации от ее утечки за счет ПЭМИ//Конфидент.– № 4, 1998.– С. 48–50.
105. *Кутин Г.И., Кузнецов АС.* Охраняемые сведения и демаскирующие признаки при противодействии техническим разведкам.— Л.: МО, 1989. — 55 с.
106. *Лебедев И.В,* Техника и приборы СВЧ / Под ред. *Н.Д. Девяткова*.— М.: Высшая школа, 1970.— 440 с.
107. *Леонтьев Б.* Хакеры, взломщики и другие информационные убийцы. - М.: Познавательная книга. - 1999.
108. *Лихарев С. Б., Фомин Г. А.* Обзор средств криптографической защиты информации в персональных компьютерах//Технологии электронных коммуникаций, т. 45, 1993, с. 5–48.
109. *Лопатин В. В.* Правовые аспекты информационной безопасности//Системы безопасности связи и телекоммуникаций.– № 21, 1998, с. 8–10.
110. *Люцарев В.С., Ермаков К.В., Рудный Е.Б., Ермаков И.В.* Безопасность компьютерных сетей на основе Windows NT. - М.: «Русская редакция». - 1998.
111. *Макаров В.* Суперкодированная связь//Красная звезда, 1992.
112. *Макаров Г.И.* Оборудование для автоматических систем контроля доступа.— М.: Формула безопасности, 1997.— 24 с.
113. *Максимов Ю. Н.* и др. Защита информации в системах и средствах информатизации и связи. – СПб.: ВИКА, 1996.–113 с.
114. *Максимов Ю.Н., Еремеев М.Л.* Построение криптосистем на основе свойств эллиптических кривых//Безопасность информационных технологий. №2. 1995. С. 52—55.
115. *Мафтик С.* Механизмы защиты в сетях ЭВМ / Пер. с англ. — М.: Мир, 1993.— 216с.
116. *Медведовский И.Д., Семьянов П.В., Платонов В.В.* Атака через Internet/ под редакцией П.Д. Зегжды. - СПб.: «Мир и семья». -1997.
117. *Мельников В. В*. Защита информации в компьютерных системах.– М: Финансы и статистика; Электронинформ, 1997.– 368 с.
118. *Месси Дж. Л.* Введение *в* современную криптологию // ТИИЭР. 1988. т. 76.№ 5. С.51—74.
119. Микрофоны и телефоны /Справочник.– М.: Радио и связь, 1998.– 236 с.

120. Миниатюрные УКВ ЧМ передатчики серии «Штифт»/Фирма «Анна», 1995.
121. *Мироничев С. Н.* Коммерческая разведка и контрразведка или промышленный шпионаж в России и методы борьбы с ним.– М.: Дружок, 1995.– 223 с.
122. *Михайлов АС.* Измерение параметров ЭМС, РЭС. — М.: Связь, 1980. — 200 с.
123. *Молдовян А.А., Молдовян Н.А., Советов Б.Я.* Криптография. – «Учебники для вузов. Специальная литература». - СПб.: Издательство «Лань», 2000. –224 с.
124. *Молдовян А.А., Молдовян Н.А., Советов Б.Я.* Скоростные программные шифры и средства защиты информации в компьютерных системах. - СПб.: типография Военной Академии Связи. -1997.
125. *Молдовян Н.А.* Проблематика и методы криптографии. - СПб.: издательство СПбГУ. -1998.
126. *Надеждин В. С.* Технические средства защиты от диктофонов и подслушивающих устройств//Защита информации, 1995.– №3, с. 72–76.
127. *Некрасов М. Ю.* Прибор защиты информации OSC-5000//Конфидент.– № 2. 1998, с. 99–101.
128. Нелинейный радиолокатор «NR-900M»: Техническое описание. Инструкция по эксплуатации.
129. *Николаев Ю.И.* Проектирование защищенных информационных технологий. Часть первая. Введение в проблему проектирования распределенных вычислительных систем. - СПб.: издательство СПбГТУ. -1997.
130. Организационно-технические методы контроля защиты информации в объектах ЭВТ: Учебное пособие.— СПб.: ВИКА, 1994.— 77 с.
131. *Орлов, В. А., Петров В. И.* Приборы наблюдения ночью и при ограниченной видимости. М.: Воениздат, 1989, 254 с.
132. Оружие шпионажа /Под ред. М. В. Данилова.– М.: Империал, 1994.– 240 с.
133. *Отт Г.* Методы подавления шумов и помех в электронных системах. М.: «Мир», 1979, 320 с.
134. Основы обеспечения безопасности данных в компьютерных системах и сетях/ *Большаков А.А., Петряев А.Б.* и др. - СПб.: ВИККА им. А.Ф. Можайского. -1995.
135. *Паркер Тимоти.* TCP/IP. Освой самостоятельно. - М.: «БИНОМ». -1997.
136. *Петраков А. В.* Защита и охрана личности, собственности, информации, Справочное пособие, М.: «Радио и связь», 1997, 320 с.
137. *Петраков А. В., Лагутин В. С.* Телеохрана. М.: Энергоатомиздат, 1998, 376 с.

138. Прайс лист //АОЗТ «Анна-спецтехника», 17 октября 1995 г.
139. Предпринимательство и безопасность.– М.: Универсум. 1991, с. 215–216.
140. Положение о государственном лицензировании деятельности в области защиты информации.
141. Положение о сертификации средств защиты информации. Введено постановлением Правительства РФ №608. М., 1995.
142. Положение по аттестации объектов информатики по требованиям безопасности информации. ГТК. М., 1994.
143. *Полонский И. Б.* Конструирование электромагнитных экранов для радиоэлектронной аппаратуры. — М.: Сов. радио, 1979. — 216 с.
144. *Попугаев Ю.* Телефонные переговоры: способы защиты//Частный сыск и охрана.– 1995.– № 3, с. 78–84.
145. *Прытко С. М., Топоровский Л. Н.* Нелинейная радиолокация: принцип действия, область применения, приборы и системы //Системы безопасности связи и телекоммуникаций.– № 6, 1995, с. 52–55.
146. Радиоэлектронные средства и мощные электромагнитные помехи / Под ред. *В. И. Кравченко*.— М.: Радио и связь, 1987. — 256 с.
147. Разъяснение о порядке предоставления сведений ограниченного распространения по запросам сторонних организаций.– Инструктивное письмо Государственной налоговой службы Российской Федерации от 11.05.95 г. № ЮБ-6-18/261.
148. *Рикетс Л.У., Бриджес Дж.Э., Майлетта Дж.* Электромагнитный импульс и методы защиты / Пер. с англ., под ред. *Н.А. Ухина*.— М.: Атомиздат, 1979. —328с.
149. *Римский-Корсаков А. В*. Электроакустика.– М.: Связь, 1973.– 373 с.
150. *Роб Тидроу.* Управление реестром Windows'95.– СПб.: BHV, 1996.– 280 с.
151. *Ронге М*. Разведка и контрразведка.– Киев: Синто, 1993.– 239 с.
152. *Сазонов Д. М.* Антенны и устройства СВЧ.– М.: Высш. школа, 1988.– 432 с.
153. *Сапожков М. А.* Речевой сигнал в кибернетике и связи. М.: Государственное издательство литературы по вопросам связи и радио, 1963, 452 с.
154. *Синилов В. Г., Ковалев М. С.* Телевизионные камеры для использования в целях безопасности //Системы безопасности связи и телекоммуникаций.– № 21, 1998, с. 24.
155. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. ГОСТ 28147—89.
156. *Сребнев В. И.* Поисковый радиомониторинг: проблемы, методики, аппаратура// Системы безопасности. – № 24, январь – февраль, 1999, с. 58–63.
157. Слагаемые безопасности: Каталог средств и систем. М.: 1995.— 186 с.

158. *Спесивцев А.В., Вегнер А, Кругляков А.Ю.* Защита информации в персональных ЭВМ. — М.: Радио и связь, МП «Веста», 1992. — 192 с.
159. Специальная техника для контроля и защиты информации//компания ГРОТЕК, 1994.– 89 с.
160. Специальная техника. Системы безопасности и защиты.– М: Knowledge Express Inc., 1994.– 30 с.
161. Специальная техника защиты и контроля информации//Каталог фирмы Маском.– 1995.
162. Специальная техника//Каталог фирмы Нелк.– 1995.
163. Специальная электроника//АОЗТ «Бэтмэн», 1995.–10 с.
164. Справочник по акустике/*Иоффе В. К., Корольков В. Г., Сапожков М. А.*/Под ред. М. А. Сапожкова.– М.: Связь, 1979.– 312 с.
165. Справочник по радиоизмерительным приборам/Под ред. *В. С. Насонова*.– М.: Сов. радио, 1979.– т. 3.– 424 с.
166. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Руководящий документ. Гостехкомиссия России. М., 1992.— 24 с.
167. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Руководящий документ. Гостехкомиссия России. - М. - 1997.
168. Средства защиты информации//Каталог фирмы «Конфидент», 1993.
169. Средства защиты конфиденциальной речевой информации от утечки по линиям радио- и проводной связи «Рокада».– НПО «Заря», 1994.
170. Средства защиты в машиностроении. Расчет и проектирование. Справочник. М.: «Машиностроение», 1989, 368 с.
171. Старый знакомый OSCOR//Системы безопасности.– № 24, январь – февраль, 1999, с. 55.
172. *Стенг Д., Мун С.* Секреты безопасности сетей. - Киев: «Диалектика». - 1995.
173. *Сырков Б. Ю.* Перехват паролей при помощи программных закладок, внедряемых в операционные системы//Системы безопасности связи и телекоммуникаций.– № 23, 1998, с. 18–21.
174. Теория и практика обеспечения информационной безопасности/ под редакцией *П.Д. Зегжды.* - М.: издательство агентства «Яхтсмен». -1996.
175. Техническая защита//Каталог продукции и услуг. «Конфидент», 1995.– 42 с.
176. Технические средства безопасности//Информационно-коммерческий центр-1.– 1995.

177. Технические средства защиты информации ’99.– М.: ЗАО «АННА», 1999.– 112 с.
178. Технические средства разведки/Под ред. В.И. Мухина.– М.: РВСН, 1992.– 394 с.
179. Технические средства охраны, безопасности и сигнализации //Справочник. Вып. 4.– М.: ВИМИ, 1994.– 28 с.
180. Технический шпионаж и борьба с ним.– Минск, 1993.– 25 с.
181. *Тимофеев Ю.А.* Анализ работ в области международной стандартизации методов и средств криптографической защиты данных для вычислительных систем и сетей // Вопросы специальной радиоэлектроники, серия ЭВТ. — 1990, вып. 3. С.23—30.
182. *Топоровский Л.* Средства нелинейной радиолокации: реальный взгляд //Системы безопасности связи и телекоммуникаций.– № 23 , 1998, с. 94–96.
183. *Уайз Д.* Охота на кротов.– М.: Международные отношения, 1994, с. 87.
184. Указ Президента РФ № 334 от 3.04.95 г. «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставлении услуг в области шифрования информации»//КомпюТерра.– № 16, 24.4.95 г.
185. Указ Президента РФ № 188 от 6.03.97 г. «Перечень сведений конфиденциального характера».
186. Указ Президента РФ № 633 от 23.06.95 г. «О первоочередных мерах по реализации Федерального закона “Об органах федеральной службы безопасности”».
187. Указ Президента РФ № 212 от 19.02.99 г. «Положение о Государственной технической комиссии при Президенте Российской Федерации».
188. Указ Президента РФ № 21 от 9.01.96 г. «О мерах по упорядочению разработки, производства, реализации приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы, а также использованию специальных технических средств, предназначенных для негласного получения информации».
189. Указ Президента РФ № 484 от 15.05.97 года «О представлении лицами, замещающими государственные должности Российской Федерации, и лицами, замещающими государственные должности государственной службы и должности в органах местного самоуправления, сведений о доходах и имуществе».
190. *Ухлинов Л.М.* Анализ безопасности протоколов управления ключами в сетях ЭВМ //Автоматика и вычислительная техника. 1990. №1. с.11—16.
191. *Феденко Б.А., Макаров И.В.* Безопасность сетевых ОС. - М.: ЭКО-ТРЕНДЗ. -1999.

192. *Фролов Г. В.* Тайны тайнописи.–М.: Инфосервис Экспресс, 1992–124 с.
193. *Халяпин Д. Б., Ярочкин В. И.* Основы защиты промышленной и коммерческой информации.– М.:ИПКИР, 1994.–70 с.
194. Хорев А. А. Малогабаритные панорамные приемники //Специальная техника № 3, 1998, с. 23–27.
195. *Цветков В. В., Демин В. П., Куприянов А. И.* Радиоэлектронная борьба: радиоразведка и радиопротиводействие. Учебное пособие. М.: Изд-во МАИ, 1998, 248 с.
196. *Шапиро Д.Н.* Основы теории электромагнитного экранирования. — Л.: Энергия, 1975. —109с. '
197. *Шелков В. А*. Кит Мэлтон и его музей «шпионской» техники//Специальная техника.– № 4–5, 1998, с. 54–64.
198. *Шиверский А. А*. Защита информации: проблемы теории и практики.– М.: Юрист, 1996.– 112 с.
199. *Шумилов А. Ю*. Новый оперативно-розыскной закон.– М.: Фирма АВС, 1997.– 47 с.
200. *Эдварде Марк Джозеф.* Безопасность в Интернете на основе Windows NT: пер. с англ. - М.: «Русская редакция». -1999.
201. *Ярочкин В. И.* Безопасность информационных систем. М.: "Ось-89", 1996.
202. *Ярочкин В. И*. Предприниматель и безопасность. Часть II.– М.: Экспертное бюро, 1994.– 64 с.
203. *Ярочкин В. И.* Служба безопасности коммерческого предприятия.– М.: «Ось-89», 1995.–144 с.
204. *Ярочкин В. И., Халяпин Д. Б*. Основы защиты информации. Служба безопасности предприятия – М.: ,1993.– 42 с.

Литература на иностранных языках.

205. *Abrams M., Jeny A.* Network security; Protocol reference models and me trusted computer system evaluation criteria-IEEE network magazine. April 1987, v. 1, p. 24—33.
206. Audio Intelligence Devices // Product Catalog, 1992.–399 p.
207. Audio Intelligence Devices// Catalog.– Florida USA, 1995.
208. Anics firm // Catalog 1994 г. 99. Communication Control System jf New York, LTD //Product Catalog, 1992.– 46 p.
209. AM/FM Stereo Radio. Model ANS-55W. Operation Instruction // DAE-WOO.– 5 p.
210. Anics firm // Catalog 1994 г.– 68 p.
211. AR-3000A //Technical Specifications. 1993.– 26 p.
212. Armada International.– 1990.– V. 14.– № 2.– P. 91.
213. Armada International.– 1990.– V. 14.– № 3.– P. 14–54.
214. *Bucnmann J., Williams H. A* Key-Excnange System Based on Imaginary Quadratic Fieid // J. Of Cryptology, v. 1, p. 107—118.
215. *Cabidulin E. endKjelsen O.* Randomizing tne public key for improving perfomances pf public — key cryptosystems. — In Proc. Sixth joint Swedish — Russian Int. Workshop on Inf. Theory, Ang., 1993, pp. 293—300.
216. Communication Control System jf New York, LTD //Product Catalog, 1992.– 46 p.
217. Combicontrol 8000 Spesial. Owner’s Manual /PAN International.– P. 5.
218. Communication Recever // Icom Inc., 1994.– 12 p.
219. *Coppersmith D.* Fast evaluation of logarithms in fields of characteristic two // IEEE Trans. Inform. Theory, IT 30,1984, pp. 587—594.
220. *Cordon D.* Diskete Logaritms in GF (p) Using the Number Sieve. — CTAM J. Disc. Math., v.6, N 1, 1993, p. 124—138.
221. Covert Audio Intercept //Surviellance Tecnology Group.– London, 1993.– 32 p.
222. Data encryption Standart. FIPS publication 46. Washington. DS: National Bureau of Standards, 1977.
223. *Diffie W.* and *Hellman H.* New directions of cryptograpny. — IEEE Trans Inform. Theory. VIT — 22, Nov. 1976. pp. 644—654.
224. Electronic Welt’93//Conrad Electronic.– P. 346–358, 385–392
225. *Fumy W., Ries H.P.* Kryptographie — Entwurfund Analyse Symmetrischer Krypto-syseme. Oldenbourd, Munchen, 1989.— p. 327.
226. Government Suplier of Surveillance Technology //PK Electronic.– Hamburg, 1994.– 268 p.
227. International Defense Review.– 1987.– № 1 – P. 21.
228. International Logistics System./Catalog, 1993.– P. 56.

229. Jane’s Defence Weekly.– 1985.– V. 4, № 2.– P. 236.
230. *Koblitz N. A* Course in Number Theore and Cryptography. — Springer Veriag, N.Y., 1987,281p.
231. *Krouk E.* Tne New publictey cryptosystem In Proc. Sixtn Joint Swedich-Russian Int. Workshop jn Iht. Theory, Ang., 1993. —pp. 268—271.
232. LEA//Product Catalog.– 1992.–84 p.
233. *Lenstra H.* Factoring integers with elliptic curves // Ann. of Math., N126, 1987, pp. 649—673.
234. Me Elice R/ A public-key cryptosystem based on algebraic coding theory // DEN Progress Rep. 4244, JPZ, pp. 114—116.
235. Mebgerate Mebsysteme. Rohde & Schwarz.– Munich, 1992.– 204.
236. *Miller S.* Uses of elliptic curves in cryptography // Lecture Notes in Comput. Sci. Advances in Cryptology — CRYPTO'85. 1986. Vol. 21, pp. 419—426.
237. Miniport recever EB 100 (20 to 1000 MHz)//Rohde & Schwarz. Munich. FRD. 1990.– P. 1–2.
238. Neuhiten 91\94 186. Rohde & Schwarz.– Munich, 1992.– 56 p.
239. News Week.– 1985.– V. 106.– № 7.– P. 38–39.
240. *Niederraiter H.* Knapsacktupe Cryptosystem and Algebraic Coding Theory // Probl. of Contr. and Inf. Th., 1986, v.15. pp. 123—127.
241. Olimpus. Pearlcorder.– Germany, 1992.
242. PK Anti-riot Equipment.– Hamburg, 1993.– 100 p.
243. PK Electronic international //Professional general export catalogue.– Hamburg, London, Paris, New York, № 1.– 268 p.
244. *Pollard J.* Monte Carlo Methods for Index Computation (mod p) // Math. Сотр., Vol. 32, N143, p. 918—924.
245. PRO-46//Owners Manual.– 46 p.
246. *Rivest R., Samir A., Adleman LA.* Method for obtaining digital signatures and publik for obtaining digital signatures and public key cryptosystems. Comm. of ACM. 1978, v.21, N2, pp.120—126.
247. *Shannon C.* Communication theory of Secrecy systems, Bell Syst. Tech. J.v.28. Ost. 1949. pp.656—715.
248. Spectrum.– 1985.– V. 22. – № 7.– P. 30–38.
249. Spy Head Quoter//Product Catalog, 1992.– 56p.
250. Stereo Radio Cassete Recorder. Model RQ-A160/170. Operation Instruction// Matsushita Electric Industrial Co.– 79 p.
251. Telecommunication Monitoring //PK Electronic.– 1993.– 18 p.

Периодические издания.

252. «Системы безопасности связи и телекоммуникаций» – издатель компания «Гротек», Москва.
253. «Защита информации. Конфидент» – издатель ООО «Конфидент», С.-Петербург.
254. «Специальная техника» – учредитель ОАО ХК «Электрозавод», Москва.
255. «Иностранная печать о техническом оснащении полиции зарубежных государств» – ежемесячный информационный бюллетень ВИНИТИ, Москва.
256. «Бизнес и безопасность» – издатель ООО «Шанс», Киев.
257. «Жизнь и безопасность» – ежеквартальный журнал, С.-Петербург.
258. «БДИ» (Безопасность, Достоверность, Информация), С.-Петербург.
259. «Оперативное прикрытие» – издатель ООО «Оперативное прикрытие», С.-Петербург.

Ресурсы Интернет.

- Наиболее полный каталог ресурсов российской части Интернета. Это «Рамблер» (или Rambler). Войдя в раздел «Безопасность» тематической части каталога (hyperlink http://counter-windows-1251.rambler.ru/ top100/security/), можно подробно изучить более 200 ссылок на разные адреса. Следует иметь в виду то, что часть ссылок отправит вас на различные разделы одних и тех же сайтов.
- В течение 1998 года появилось несколько специализированных каталогов ресурсов российского Интернета, посвященных теме безопасности. Наиболее «вместительным» из таких каталогов оказалась коллекция ссылок, собранная г-ном Свирским (hyperlink http://www. corbina.net/~ksi/). Все ссылки организованы в тематические разделы. Есть также ссылки на некоторые зарубежные ресурсы.
- Другой специализированный каталог ресурсов можно найти на сайте Санкт-Петербургской компании «Регионэксперт» (hyperlink http://www. regionexpert.ru/). Здесь также можно искать информацию о ресурсах по тематическим разделам. Многие ссылки снабжены краткими комментариями.
- Приведем некоторые, наиболее интересные адреса, где можно найти информацию, относящуюся к проблемам защиты информации и противодействию промышленному шпионажу.
- Украинский сервер, поддерживаемый Киевским журналом «Бизнес и Безопасность» (hyperlink http://www.bsm.com.ua/). В его разделах «Белые

страницы» и «Желтые страницы» представлено большое количество украинских фирм, относящихся к заявленной тематике.

- Первый российский сервер, посвященный специально этой теме. Это Spy Market Pro (http:/www.spymarket.com/), принадлежащий Санкт-Петербургской компании «СмерШ Технике» и созданный (при некотором участии Лаборатории ППШ) еще в начале 1997 года. На сервере немного собственно информации. Один из разделов содержит небольшое количество ссылок на российские компании (раздел платный — этим и объясняется малое количество ссылок). Есть две библиотеки: «старая» и «новая». Одним из наиболее интересных и посещаемых разделов сервера является его дискуссионная зона. Это одно из очень немногих мест русскоязычного Интернета, где «встречаются» специалисты и потребители товаров и услуг в области противодействия промышленному шпионажу.
- «Территория взлома» — так называется сервер (hyperlink http://www. hackzone.ru/), содержащий несколько разделов, каждый из которых достоин отдельного повествования. Здесь можно найти статьи, периодические обзоры и вообще много интересной и полезной информации.
- Следующий сервер зарегистрирован в Германии, но создан и поддерживается выходцами из России. Называется он «Werwolf» (hyperlink http://www.werwolf.de/). Здесь тоже много интересной и полезной информации по компьютерной безопасности (и не только). Большую часть материалов можно читать на русском языке.
- «Частная жизнь в Интернете» (hyperlink http://www.tamos.com/ privacy/ru/). Этот сайт полезен всем, кого интересуют вопросы обеспечения собственной анонимности при работе в сети. Интересно и доступно изложены понятия о криптографии и стеганографии, о возможностях поиска людей по адресу и т. д. Множество полезных ссылок, которыми изобилуют тексты.
- Различные документы по компьютерной безопасности выложены на личных страничках Казеннова Владимира Николаевича (hyperlink http://www.win. wplus.net/~kvn/compsec.htm)).
- На сервере Питерского интернет-провайдера Web Plus есть интересный раздел (hyperlink http://wwwwin.support.wplus.net/security/index.htm), где изложены практические рекомендации по обеспечению сохранности паролей пользователей и безопасной конфигурации пользовательских компьютеров от посягательств злоумышленников. Полезен всем, кто обеспокоен проблемой создания надежной защиты своих кошельков от любителей пользоваться Интернетом за чужой счет.
- Не только компьютерная безопасность, но также и другие проблемы безопасности освещены в проекте «БИБ: Библиотека Информационной Безо-

пасности» (hyperlink http://www.pps.ru/bib/index.html). Этот проект — наследник «старой» библиотеки на Spy Market Pro. К сожалению, работы по созданию БИБ'а затянулись.

- «Радиошпион» (hyperlink http://www.chat.ru/~radiospy/) — это специализированный интернет-журнал, содержащий много материалов, относящихся к техническим каналам утечки информации. Правда, не совсем ясно, в каком направлении будет развиваться этот сайт. Пока же здесь, к сожалению, больше материалов, посвященных несанкционированному получению информации. Рекомендуется тем, кто хочет убедиться в ее доступности и незащищенности от посягательств злоумышленников.
- «Конфидент. Защита информации» (hyperlink http://www.confident.ru/ magazine/Page1/Pagel.htm) — Интернет-вариант достаточно известного журнала. Рассматриваются в основном вопросы, посвященные компьютерной безопасности и противодействию промышленному шпионажу.
- «БДИ» (Безопасность, Достоверность, Информация) — еще один журнал, где освещаются различные аспекты безопасности. Адрес: hyperlink http:// www.bdi.spb.ru.
- Московское издательство Groteck (http://www.groteck.msk.ru/) известно своими журналами и каталогами на темы безопасности, телекоммуникаций и др. На сайте издательства нет «Интернет-дубликатов» печатных версий. Но здесь есть еженедельные выпуски новостей, и это, видимо, единственное место в Интернете, где периодически публикуются новости по тематике «безопасность».
- «Все о радиомониторинге» (hyperlink http://radiomon.8m.com/). Это совместный проект Госсвязьнадзора и московской фирмы НЕЛК. Пока рано говорить, насколько будет удачен этот проект, но планы неплохие.
- Фирма «АНКАД» (hyperlink http://www.microdin.ru/~ancud/index.html) предлагает криптоплаты, ПО к ним, смарт-карточные технологии и скремб-леры для защиты телефонных разговоров.
- «Центр информационной безопасности Маском» (hyperlink http://www. mascom.ru) — так называется одна из наиболее известных компаний в области технической безопасности. Особая специализация — телефонные каналы связи. Своя продукция: скремблеры серии SCR. Поставляют также различную продукцию российских и зарубежных производителей. Предлагают услуги по аттестации объектов, обучение.
- «НПЦ Фирма НЕЛК» (hyperlink http://www.aha.ru/~nelk/) — еще одна известная компания. Специализируется на разработках программного обеспечения и программно-аппаратных комплексов радиомониторинга. По-

ставляют оборудование других производителей, оказывают услуги. Наиболее известные торговые марки собственных продуктов: Sedif, «Крона».

- «Радиосервис» (hyperlink http://www.aha.ru/~rserv/) тоже специализируется на разработках программного обеспечения и программно-аппаратных комплексов для радиомониторинга. Узкая специализация позволяет сконцентрировать внимание специалистов-разработчиков на одной конкретной теме. Продукты серии RS достаточно хорошо известны в России и ближнем зарубежье.
- «Радиус ТСБ» (hyperlink http://www.aha.ru/~radius/) — одна из очень немногих торговых компаний, представленных в Интернете (конечно, на рынке безопасности). К сожалению, сервер «неживой»: обновления бывают крайне редко, нет возможности оформить заказ через Интернет и т. д. Для торговой компании это, как представляется, не очень правильный способ представить себя в Интернете. Красивая витрина.
- Фирма «РелТех» (hyperlmk http://www.reltech.ru/) занимается разработкой и производством специальной аппаратуры для контроля за пейджинговыми сообщениями, переговорами в аналоговых стандартах сотовой связи и др. Вся спецтехника предназначена для субъектов ОРД, деятельность фирмы лицензирована ФСБ.
- Фирма «Безопасность Бизнеса» (hyperlink http://www.secur.spb.ru/ index.htm) предлагает разнообразную технику. Собственные разработки и производство: изделия марки «Барьер» для защиты телефонных линий. В соответствии с лицензиями ФСБ компания предлагает спецтехнику для субъектов ОРД. Интересный раздел сайта: «Страницы безопасности».
- Фирма «Бэтмэн» на своем сайте (hyperlink http://www.batman.ru/) предлагает своеобразную выставку технических средств безопасности от различных производителей. Не рекомендуется смотреть этот сайт с помощью браузера от фирмы Netscape Communications.
- ЗАО «Лаборатория ППШ» (hyperlink http://www.pps.ru/) — еще одна ведущая питерская фирма. Из наиболее известных собственных разработок нужно назвать так называемые «подавители диктофонов». На сайте много информации о различных приборами средствах как поиска, так и защиты технических каналов утечки информации. Услуги: аттестация объектов, сертификация средств защиты, обследование помещений, консультации и обучение. Особняком стоит сервер, целиком посвященный одному прибору — ST031 «Пиранья» (http://www.piranha.ru/), разработанному компанией ДОБРО ПОЖАЛОВАТЬ НА НАШ WEBSITE: http://www.pps.ru
- Сервер компании «СмерШ Технике» (hyperlink http://www.spymarket. com/smerch). Компания занимается разработкой и производством собст-

венных средств защиты информации. Сервер небольшой, но продукты интересные. К сожалению, не все они представлены на сайте. Поскольку «СмерШ Технике» предпочитает реализовывать свою продукцию через дилеров, рекомендуем посмотреть их список. В ряде случаев у дилеров можно получить более подробную и развернутую информацию о продуктах этой компании.

- Компания «Центр Речевых Технологий» (hyperlink http://www.stc. rus.net/). Это ведущая российская компания в области шумоочистки сигналов, как в реальном времени, так и записанных на какие-либо носители.
- В Архангельске — компания «КОНДОР-Техно» (hyperlink http://www.arh.ru/~condortn/)/.
- Екатеринбург — компания «Центавр» (hyperlink http://www.skyman.ru/~centavr/)/.
- Липецк — компания «Айра» (hyperlink http://aira.lipetsk.ru/)/.
- Новосибирск — «Центр Информационной Безопасности» (hyperlink http://www.nsk.su/~security/)/.
- Саратов — фирма «Коронэль» (hyperlink http://www.sarexpo.ru/koronel/).
- Хабаровск — «Лотос Системы» (hyperlink http://lotos.khv.ru/).

В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена программа его развития на 2009–2018 годы. В 2011 году Университет получил наименование «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

КАФЕДРА БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Кафедра «Безопасные информационные технологии» (БИТ) осуществляет подготовку специалистов по специальности 090103 «Организация и технология защиты информации», бакалавров и магистров по направлению 090900 «Информационная безопасность». Широкий профиль подготовки, знание методов обеспечения информационной безопасности и средств защиты информации, практические навыки работы с современными техническими, программными и программно-аппаратными средствами защиты информации - все это позволяет выпускникам кафедры найти работу на производственных предприятиях, в подразделениях информационной безопасности, научно-исследовательских и инновационных организациях, а также в коммерческих структурах. Выпускники кафедры последних лет работают в Федеральной службе технического и экспортного контроля (ФСТЭК), Лаборатории Касперского, компаниях Dr.Web, специализированных предприятиях в сфере разработки и применения комплексных систем защиты информации «Эврика», ГазИнформСервис, и т.д. Партнерами кафедры являются ОАО «Воентелеком», Санкт-Петербургский институт информатики и автоматизации РАН, Военная академия Генерального штаба ВС РФ, Военно-космическая академия им. А.Ф. Можайского, Бостонский университет (США), Комитет по управлению городским имуществом администрации Санкт-Петербурга и другие научные организации и вузы.

Каторин Юрий Федорович.
Разумовский Андрей Владимирович
Спивак Антон Игоревич

Защита информации техническими средствами

Учебное пособие

В авторской редакции
Редакционно-издательский отдел НИУ ИТМО
Зав. РИО Н.Ф. Гусарова
Лицензия ИД № 00408 от 05.11.99
Подписано к печати
Заказ №
Тираж
Отпечатано на ризографе

Редакционно-издательский отдел
Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики
197101, Санкт-Петербург, Кронверкский пр., 49