Федеральное агентство по образованию
Государственное образовательное учреждение высшего профессионального образования
Санкт-Петербургский государственный политехнический университет
(«СПбГПУ»)

Ю.С. Сидорин

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Учебное пособие

САНКТ-ПЕТЕРБУРГ

Издательство Политехнического университета

2005

УДК 004.056(075.8)

ББК 32.973-018.2я73

С 347

Сидорин Ю.С. **Технические средства защиты информации:**

Учеб. пособие. СПб.: Изд-во Политехн. ун-та, 2005. 141 с.

Пособие соответствует государственному образовательному стандарту дисциплины ОПД.Ф.14 «Технические средства защиты информации» по специальности

090104- «Комплексная защита объектов информатизации» направления подготовки специалистов 090000 «Информационная безопасность».

Рассматриваются понятие коммерческая тайна и основные источники её разглашения; кратко даются концептуальные положения по защите информации. Основное внимание уделено техническим каналам утечки информации как совокупности объектов, устройств несанкционированного сбора информации и физических каналов различных типов, по которым информация передаётся агенту. Рассматриваются пути съёма информации, деконспирационные признаки работы устройств, системы защиты от съёма информации по каждому каналу. Приводится обобщённая методика по обнаружению каналов утечки информации.

Автор ставит цель не только ознакомить студентов с проблемами защиты информации, но и научить их уметь самостоятельно анализировать и разрабатывать основные устройства. В пособии делается попытка в ограниченном объёме изложить достаточно обширный материал. Для понимания материала читателю необходимы основные сведения из электроники в объёме курсов образовательного стандарта.

Предназначено для студентов четвёртого курса факультета технической кибернетики, изучающих дисциплину «Технические средства защиты информации».

Табл. 11, Ил. 72, Библиогр.: 21 назв. Печатается по решению редакционно-издательского совета Санкт-Петербургского политехнического университета.

© Сидорин Ю.С., 2005
© Санкт-Петербургский государственный политехнический университет, 2005

ISBN

ВВЕДЕНИЕ

Распад бывшего Советского Союза, образование на его базе новых государств, отсутствие четких границ, кризис в экономике, ослабления всех видов ответственности и несовершенство законодательства привело к резкому увеличению преступных групп. Наличие у преступников значительных денежных средств позволяет им создавать технически хорошо оснащенные мобильные группы. Применение новой техники и подкупа сотрудников фирмы (или внедрение своих людей в состав фирмы) позволяет преступникам успешно проводить свои операции. Объектами их деятельности являются частные фирмы, заводы, базы и склады, нефте и газоперерабатывающие станции, музеи, ценное художественное имущество государства и граждан и т.д. Деятельность преступных групп приводит к резкому снижению доходов предприятия, а в некоторых случаях и к его краху. Существует государственный и коммерческий сектора экономики.

Государственная собственность порождает государственные секреты, которые охраняются мощными спецслужбами, в которых архитектура системы защиты базируется на директивных отработанных формах управления. Не государственные коммерческие предприятия могут вести работы по заказам Правительства и по заказам других фирм. Если работы ведутся по заказам Правительства, то правила защиты информации номинируются Государственными спецслужбами. Если работы ведутся по заказам других коммерческих структур, то правила защиты информации

номинируются руководством фирмы в соответствие с составленными и утверждёнными коллективом “Перечнем сведений, составляющим коммерческую тайну предприятия”.

В дальнейшем будут рассмотрены только проблемы связанные с защитой фирменных секретов.

Экономическая сущность воровства коммерческой тайны ясна – не тратить средства на проведение разработок и получение новой продукции (на это требуются, как правило огромные суммы), а законным или незаконным путем получить требуемую информацию у конкурента и таким образом получить большую прибыль.

Пример 1: Одна из фирм корпорации “Дженерал Моторс” в течении значительного времени моделировала новые формы автомобиля. Когда работа подошла к концу, над двориком студии, где стоял макет, появился вертолет и за несколько секунд (пока закрывали макет чехлами) сфотографировал объект. Т.е. труд большого числа людей (вложенные в разработку деньги) был приватизирован за несколько секунд [1].

Пример 2: Бывший вице-президент “Дженерал Моторс” Джон де Лори писал в своей книге: “Руководство концерна было настолько озабочено планами своего конкурента – корпорации “Форд”, что не утверждало свои производственные программы до тех пор, пока не получало свежие разведанные о противнике”. Данные получались от агентов работавших у Форда [1].

Из опыта зарубежных фирм следует, что попытка переложить всю ответственность за сохранность объектов и информации на специальные государственные службы является удобным способом, но не эффективным. Обеспечение безопасности фирм - это сложная и дорогостоящая работа, которая состоит в правильном сочетании:

- действий милицейской службы;
- частных служб охранных предприятий;
- технических средств зашиты территорий и помещений;
- технических средств зашиты информации;
- правильной кадровой политики руководства фирм.

Правила и методы действия милицейских и частных служб охраны, рекомендации по кадровой политике для руководства предприятий изложены в соответствующих нормативных документах. В данной книге будут рассмотрены в основном вопросы технической утечки информации, а так же технические средства зашиты информации. В связи с тем, что главный источник утечки информации - человек, очень кратко придется осветить кадровую политику руководства по защите информации (не смотря на значительный объем рекомендаций по данному вопросу). Что же надо защищать? Безусловно, защищать надо то, что приносит фирме большую прибыль, причем стоимость методов и средств зашиты должна быть меньше прибыли.

1. КОММЕРЧЕСКАЯ ТАЙНА

Коммерческая тайна (КТ) - это информация, которая позволяет получать предприятию большую прибыль по сравнению с конкурентом.

Работа по определению сведений которые следует отнести к коммерческой тайне [1] выполняется в несколько этапов, а именно:

1 этап. Составление ориентировочного перечня сведений “Коммерческая тайна”. В состав перечня могут входить: планы предприятий; документы по управлению предприятием; финансовой деятельности; производственной деятельности; рынок сбыта; протоколы переговоров и совещаний; цены на продукцию и услуги; списки компаньонов, посредников, поставщиков, конкурентов; исследования по созданию новых технологий и их использованию; организация службы безопасности.

2 этап. Сокращение списка “Перечня” за счет:

а) исключения сведений, охраняемых государственными спецслужбами;

б) исключения сведений, являющихся общедоступными на законных основаниях.

Состав общеуступных сведений уточнен Постановлением Правительства РСФСР от 5.12.91г. №35 “О перечне сведений, которые не могут составлять коммерческую тайну”. К ним относятся: учредительные документы; регистрационные удостоверения, лицензии; финансовая отчетность для наложения налогов; документы о размерах имущества; численный состав работающих.

Общедоступными являются так же научно-технические сведения после их публикации в открытой печати.

3 этап. Оценка ущерба, если сведения из перечня будут известны конкуренту; определение времени, необходимого конкуренту для реализации добытой информации.

4 этап. Определение источников и каналов утечки информации.

5 этап. Определение возможностей от утечки информации.

6 этап. Определение стоимости мероприятий по защите информации.

На основании результатов, полученных при рассмотрении всех этих этапов, проводится сопоставление потерь от возможной утечки информации со стоимостью мероприятий по защите информации; далее исходя из критерия "эффективность - стоимость" принимается решение об отнесении сведений к КТ. В качестве заключительного документа составляется "Перечень сведений, относящихся к коммерческой тайне предприятия". Утверждение этого документа коллективом и руководством предприятия придает ему соответствующую юридическую силу.

Конкретные наказания за разглашение КТ обычно оговариваются в пункте "Обеспечение охраны труда" Коллективного договора между администрацией и трудовым коллективом. Например:

- за разглашение определенных пунктов (номера пунктов “Перечня”) лишать вознаграждений (полностью или частично) за выслугу лет и (или) за общие результаты работы за год;
- за разглашение пунктов (номера пунктов “Перечня”) не выдвигать на любые виды морального поощрения по подразделению и.т.д.

В соответствии с коллективным договором при поступлении на работу служащий пишет "Обязательство", в котором он подтверждает свою ответственность за разглашение КТ и личное согласие о виде наказания [1].

2. ИСТОЧНИКИ РАЗГЛАШЕНИЯ КОММЕРЧЕСКОЙ ТАЙНЫ

Источники разглашения КТ:

- люди;
- документы, публикации, отходы производства;
- технические каналы и т. д.

Разглашение информации людьми

Одним из наиболее важных источников, образующий возможный канал утечки информации, является "человек". По данным итальянского специалиста в области промышленной безопасности, персонал любой компании состоит:

- 25% честных людей, которые остаются таковыми при любых обстоятельствах;
- 25% люди, ожидающие удобного случая поживиться за счет интересов фирмы;
- 50% лиц, которые могут оказаться честными или не останутся честными в зависимости от обстоятельств.

Для получения информации используются (рис 2.1 [1]):

- сознательные действия сотрудников, обусловленные инициативным сотрудничеством с другой фирмой; продажей информации за взятку, под угрозой шантажа, в виде мести; переход на другую фирму на более высокую оплату (кража мозгов);
- обман (например, за счет создания ложной фирмы, в которую заманивают специалиста на собеседование, беседуют, выуживают сведения и затем отказывают; доверчивый человек же считает, что он упустил шанс);
- особенности характера сотрудника, например, его болтливость, желание показать себя более компетентным;
- слабое знание и невыполнение требований по защите информации;
- и т. д.

Поэтому одним из условий сохранения КТ является правильная кадровая политика, создание нормального психологического климата в коллективе.

Получение информации за счет обработки документов, публикаций, отходов производства и других факторов

Документы и публикации являются одним из важных возможных каналов утечки информации. КТ может содержаться в различной документации – проектной, конструкторской, отчетной, программной и других видах технической документации.

Документ имеет определенные этапы жизни: составление, оформление, размножение, пересылка, использование, хранение и уничтожение. На любом этапе возможна утечка информации. Для уменьшения возможности утечки информации руководство предприятия устанавливает:

- перечень документов с грифом КТ.
- список лиц, допускаемых к работе с документами.
- организацию учета входящих, исходящих документов и правил работы с ними.

- правила хранения (инвентарный учет, номенклатура дел, наличие сейфов и т. д.) документов.
- правила уничтожения документов.

Французский исследователь методов промышленного шпионажа Морис Денюзер отмечает: “Современная научная, промышленная и экономическая информация большей частью легко доступна. 95% интересующих Вас данных можно получить из специализированных журналов и научных трудов, отчетов компаний, внутренних изданий предприятия, брошюр и проспектов, раздаваемых на ярмарках и выставках. Сами по себе эти данные не секретные, взятые отдельно выглядят невыразительно. Но стоит их сопоставить друг с другом и они становиться красноречивыми”. Цель шпиона раздобыть остальные 5% информации [1]. Из отходов производства фирмы (например, испорченные накладные, чертежи, бракованные заготовки деталей, кожухов и т.д.) заинтересованное лицо может получить достаточно большую информацию. Один из советов начинающему шпиону [1] формулируется так: “Не гнушайся выступить в роли мусорщика. Осмотр мусорных корзин может принести Вам богатый улов”.

Этот канал сбора информации позволяет при малых затратах получить значительный объем нужных данных.

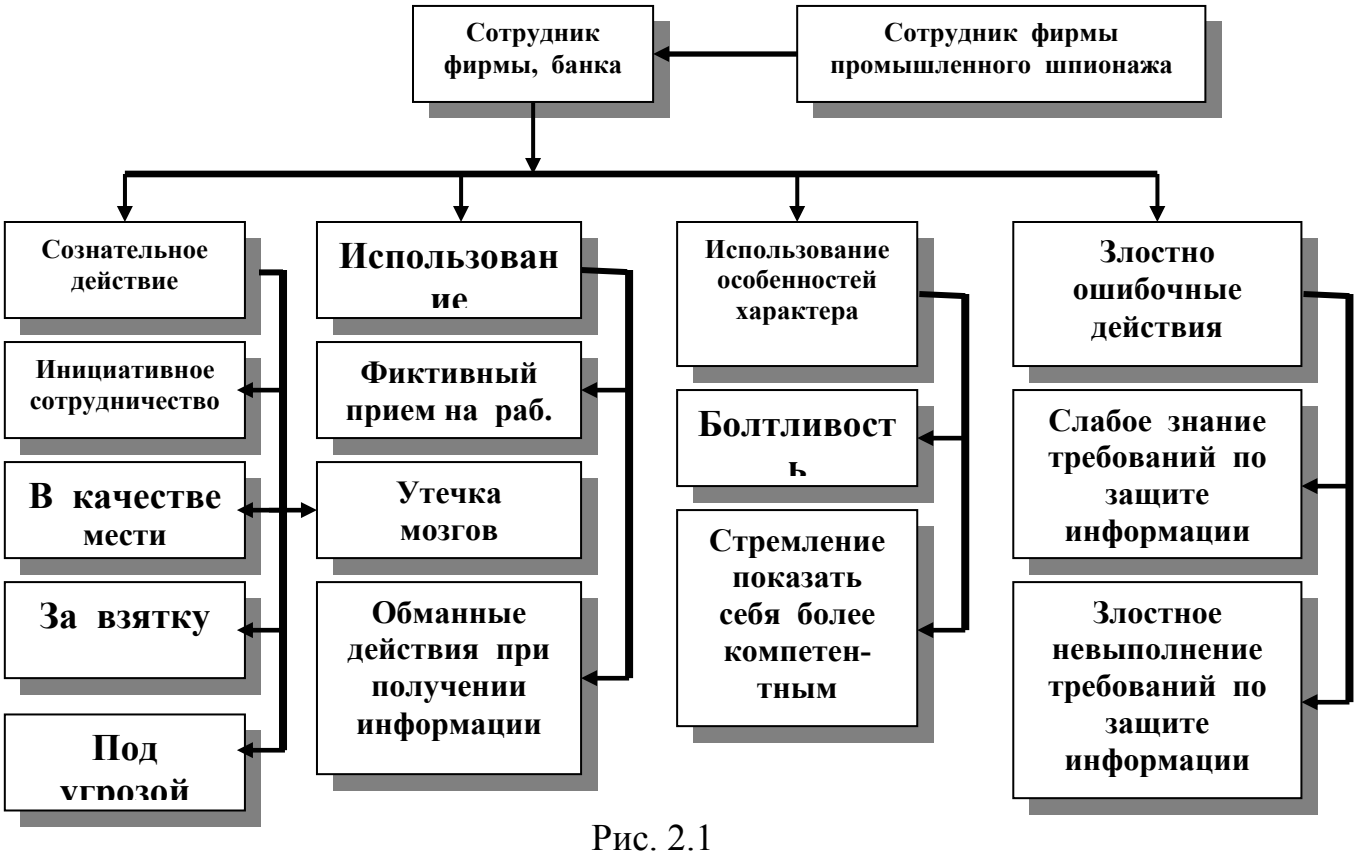


Рис. 2.1

Технические каналы утечки информации

Для обеспечения технической деятельности фирмы широко используются телефоны, радиотелефоны, компьютеры, принтеры, дисплеи, клавиатура, обычный речевой обмен информацией и т.д. Потеря информации возможна по акусто - преобразовательным, электромагнитным, визуальным и др. каналам (подробно см. гл. 5 – 11).

Рассмотрим концепцию защиты информации, виды технических каналов утечки информации и методы борьбы с технической утечкой информации.

3. КОНЦЕПТУАЛЬНЫЕ ПОЛОЖЕНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Система защиты информации (СЗИ) – организационная совокупность специальных органов, средств, методов и мероприятий, обеспечивающих защиту информацию от несанкционированного доступа к ней [1].

Способы защиты информации

- правовые;
- организационные;
- инженерно-технические.

Правовая защита обеспечивается:
наличием патентов, авторских свидетельств, товарных знаков; наличием документов, определяющих понятие “коммерческая тайна”, обязательств служащих о неразглашении коммерческой тайны, подписки при увольнении о сохранении коммерческой тайны.

Организационная защита обеспечивается совокупностью положений о Службе безопасности и планами работы этой службы. Планы мероприятий службы безопасности охватывают широкий круг вопросов, в частности:
а) На ранней стадии при проектировании помещений и строительстве
Служба безопасности рассматривает следующие вопросы:
выделение помещений для совещаний и переговоров (в таком помещении делается специальные перекрытия и каналы воздушной вентиляции, отдельные комнаты экранируют и т. д.);
удобство контроля помещений, людей, транспорта;
создание производственных зон по типу конфиденциальности работ с самостоятельным дополнительным допуском;
б) Служба безопасности участвует в подборе персонала с проверкой их качеств на основании личных бесед (изучение трудовой книжки, получения информации с других мест работы; затем принимаемый на работу ознакомляется с правилами работы с конфиденциальной информацией и порядком ответственности);
в) Служба безопасности готовит положения и осуществляет:
организацию пропускного режима;
организацию охраны помещений и территорий;
организацию хранения и использования документов, порядок учета, хранения, уничтожения документов, плановые проверки.

Инженерно-техническая защита включает в себя:
аппаратные средства защиты;
программные средства защиты – это использование специальных программ в системах, средствах и сетях обработки данных;
математические способы защиты – применение математических и криптографических методов в целях защиты конфиденциальной информации (без знания ключа невозможно узнать и дешифрировать украденную информацию).

Программные и математические методы защиты информации рассматриваются в специальных курсах; в объеме данного пособия будут рассмотрены аппаратные средства защиты.

С позиций системного подхода, защита информации должна быть:

1. Непрерывной (если на какой-то момент защита снимается, то злоумышленник воспользуется этим);
2. Плановой, централизованной (каждая служба разрабатывает свои планы, которые должны быть взаимосвязаны);
3. Целенаправленной и конкретной (защищается не все подряд, а только самое необходимое, учитываются самые опасные каналы утечки и в них конкретизируются самые опасные зоны);
4. Надежной, универсальной и комплексной (каналы утечки перекрываются различными способами, например техническими плюс получением данных от информаторов).

Правильное сочетание услуг сотрудников правоохранительных органов, негосударственных агентов, внутренней службы безопасности и технических средств защиты являются эффективным условием защиты объектов (информации).

4. ОБЩИЕ ПОЛОЖЕНИЯ О ТЕХНИЧЕСКИХ КАНАЛАХ УТЕЧКИ ИНФОРМАЦИИ

Технический канал утечки информации это совокупность объекта информации, технических средств съема информации и физического канала, по которому информация передается агенту [2]. Объектом информации чаще всего являются люди, ведущие переговоры на объекте, и аппаратура, по которой передаётся (хранится) информация.

Для нелегального съёма информации используются различные технические средства, которые будут рассматриваться в следующих главах. Информация с объекта поступает агенту по следующим физическим каналам:

- акустическим каналам;
- дополнительным проводным каналам и с помощью диктофонов;
- вибрационному каналу колебаний конструкций здания;
- электромагнитным каналам;

- телефонным каналам;
- электросетевым каналам;
- визуальным каналам.

В табл. 4.1 приведены основные каналы утечки информации и процент их использования агентами. Процент использования получен на основании обработки данных [3] по использованию подслушивающих устройств в 1996 г.

На основании данных приведенных в табл. 4.1 можно сделать вывод, что для снятия информации чаще всего используется электромагнитный канал (61%) с внедрением на объект "жучков", затем телефонный канал (15%) и далее проводные каналы и диктофоны (13%). Использование акустического канала с применением направленных микрофонов, вибрационного канала и электросетевого канала редко. Данных по использованию визуального канала нет.

Таблица 4.1

П/п	***Вид канала утечки информации***	***%***	***%***
1	Акустические каналы а) непосредственное прослушивание звуковой информации человеческим ухом б) прослушивание информации от структурной волны в) прослушивание информации направленными микрофонами	 2 2	4
2	Дополнительные проводные каналы: а) ненаправленные микрофоны б) диктофоны	 6 5	11
3	Вибрационный канал колебаний конструкций (акустомеханические каналы): а) прослушивание информации стетоскопами	 6	7

	б) прослушивание информации лазерными устройствами в) гидроакустические преобразователи	1	
4	Электромагнитные каналы: а) прослушивание информации по радиоканалам б) прослушивание информации от работающей аппаратуры в) прослушивание информации: • от внедренных радио закладок (радио микрофонов, жучков) • от пассивных устройств	 6 1 53 1	61
5	Телефонный канал: а) прослушивание информации при прямом и не прямом подключении к телефонной линии б) использование микрофона при положенной трубке в) использование ретрансляторов	 12 3	15
6	Электросетевой канал		
7	Визуальный канал		

100%

5. АКУСТИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

Акустическое поле несет информацию. Это поле может создаваться воздушной или структурной волной.

5.1. Непосредственное подслушивание звуковой информации

Человек, радиоприемники, пишущие и копировальные машины и т.д. излучают звук. Диапазон звуковых волн от 16 Гц до 20 кГц. Основная энергия речевого сигнала сосредоточена в диапазоне частот от 70 Гц
до 7 кГц, причем 95% смысловой информации лежит в более узком диапазоне 200 Гц – 5 кГц [4]. Акустическая информация выше и ниже этих частот несет информацию об эмоциях и личности говорящего (устный почерк) и несколько повышает разборчивость речи в условиях повышенных шумов. Громкость разговора оценивается в децибелах.

В табл. 5.1 приведены данные по силе звука некоторых источников

Таблица 5.1

П/п	***Источник сигнала***	***Сила звука, дБ***
1.	Предел чувствительности человеческого уха	0
2.	Шорох листьев. Слабый шепот на расстоянии 1 м.	10
3.	Тихий сад	20
4.	Негромкая музыка. Шум в жилом помещении	40
5.	Слабая работа громкоговорителя. Шум в учреждениях с открытыми окнами	50

6.	Громкий радиоприемник. Шум в магазинах. Средний уровень разговорной речи на расстоянии 1 м.	60
7.	Шум мотора грузового автомобиля. Шум внутри трамвая	70
8.	Шумная улица. Машинописное бюро	80
9.	Автомобильный гудок	90
10.	Автомобильная сирена. Отбойный молоток	100
11.	Сильные удары грома. Реактивный двигатель	120
12.	Болевой предел. Звук уже не слышен	130

Сложный доверительный разговор ведется обычно с уровнем 55дБ [4], сила звука при выступлении в зале составляет 75 дБ. Акустические колебания распространяются в помещении. Если на пути звука нет препятствий, воздушная волна распространяется равномерно во все стороны и может быть зафиксирована агентом-сотрудником фирмы промышленного шпионажа.

В ближней зоне от источника акустических колебаний (примерно 0.5-0.8 м для комнаты 30 м^2) уровень сигнала уменьшается пропорционально расстоянию, далее сигнал во всех точках в помещениях с реверберацией остается примерно постоянным и равным -(60-70) дБ от сигнала излучения [3].

Исходя из этого, качество съема речевых сигналов в небольших помещениях за пределами ближней зоны не зависит от места размещения приемника акустических сигналов и микрофоны можно помещать в любом месте открытом для звука [3].

5.2. Прослушивание информации от структурной волны

Звуковые волны оказывают переменное давление на предметы, расположенные на их пути, вызывая механические колебания в твердом теле со звуковой частотой. В отдельных конструкциях эти колебания могут передаваться на значительные расстояния, почти не затухая, и вновь излучаться в воздух, как слышимый воздушный звук. Особенно хорошо излучают звук легкие строительные конструкции с большой площадью поверхности. Передаваемый звук носит название "структурный звук".

Пример возникновения канала утечки за счет сформированного структурного звука в стенах и перекрытиях здания приведен на рис. 5.1

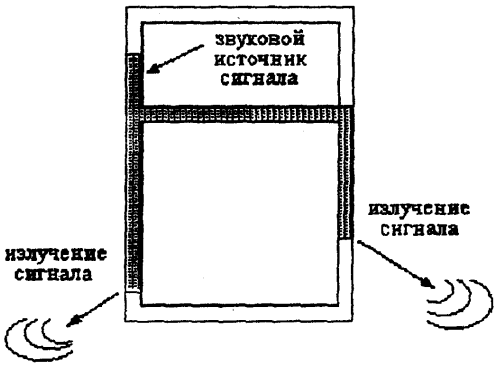


Рис. 5.1

Наиболее возможные каналы передачи структурного звука - стены, трубопроводы, каналы воздушной вентиляции помещений и т.д.

Таким образом, "заинтересованный человек", находясь даже на значительном расстоянии, может получить желаемую звуковую информацию. В табл. 5.2 приведены данные по затуханию звукового сигнала в воздуховоде в зависимости от материала воздуховода и его изгибов [3].

Таблица 5.2

Материал воздуховода	Затухание звукового сигнала дБ/один погонный метр
Кирпич	0.2-0.4
Асбестовая труба	0.1-0.2
Изгибы воздуховода	3-10

Используя данные таблицы получим, что затухание в асбестовой трубе на расстоянии 600 м составляют (60-120) дБ. В то же время, затухание звука в комнате, обладающей эффектом реверберации на расстояние более 0.8м составляет ≈(60-70) дБ [3]. Таким образом, структурный звук передается на расстояние почти в 600 раз больше, чем обычный звук. Пример носит, безусловно, частный характер, так как структура помещений разная.

5.3. Прослушивание информации направленными микрофонами

Направленные микрофоны (т.е. микрофоны беспроводной системы) обеспечивают прослушивание переговоров на больших расстояниях за счет узкой направленности приемных устройств. Наиболее часто используются направленные микрофоны с интерференционным элементом и с параболическим рефлектором.

5.3.1. Схема направленного микрофона *с интерференционным элементом приведена на рис. 5.2 (диаграмма направленности примерно 20° [3, 5, 6].*

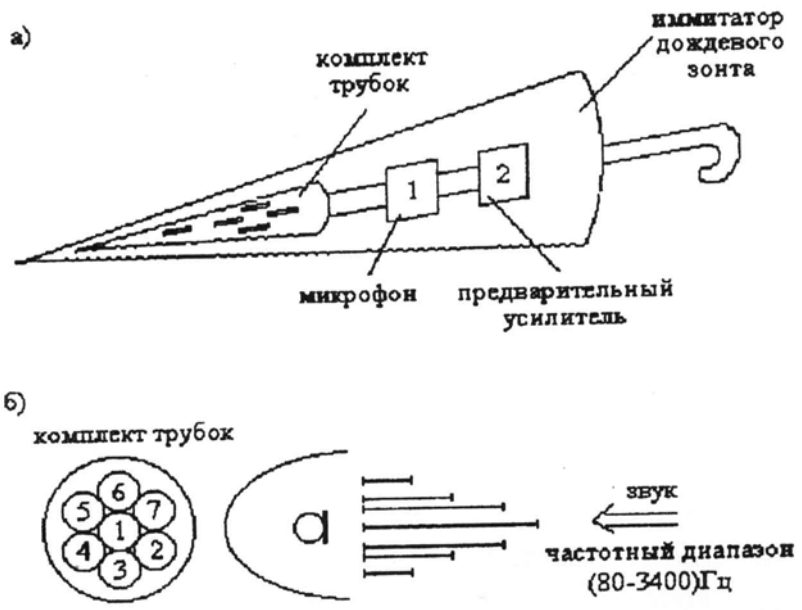


Рис. 5.2

Трубки - это направленные системы, длина каждой трубки определяется рассчитываемой частотой. Каждую трубку можно рассматривать как узконаправленную антенну, настроенную на определенную резонансную частоту; за счет этого трубкой воспринимается только сигнал расчетной частоты, приходящей по оси трубки, и не воспринимаются сигналы с других направлений. Сквозные пазы трубки закрыты тканью с соответствующим акустическим сопротивлением. Сигналы после трубок поступают на отражатель и далее на микрофон, где они суммируются. В настоящее время на отечественном рынке имеется упрощенный вариант устройства, в котором использовано ограниченное число трубок (3 шт).

В качестве примера можно привести устройство ЛСТ-НМ-101, позволяющее прослушивать разговоры до 6О м.

5.3.2. Параболический рефлектор *(рис 5.3) формирует игольчатую диаграмму направленности [3, 5].*

Угловая избирательность по приёму обеспечивается тем, что звуковые волны с осевого направления, отражаясь от параболического зеркала, суммируются в фазе в фокальной точке; если направление прихода звука не осевое, то не все слагаемые будут в фазе. Ослабление тем сильнее, чем больше угол прихода звука по отношению к оси [5].

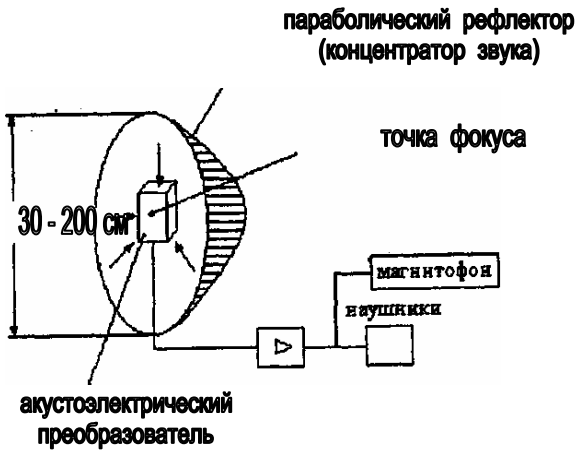


Рис. 5.3

Звук с рефлектора подаётся на акустический преобразователь и далее после отражателя на наушники и микрофон. По данным, приведенным в работе [5], одна из разновидностей подобного микрофона РК375 имеет следующие параметры: габариты 600 х 300 мм, вес 1,2 кг; работа обеспечивается в течении 75 часов при питании от источника 5 В.
Дальность приема подобных устройств на открытых площадках (при жесткой установке прибора) составляет 1000-1500 м, в условиях города –100 м; стоимость 1000 $. Параболические микрофоны выпускаются фирмами
HEL LING, COMMUNICATION CONTROL SYSTEM и др. [3].

5.3.3. Недостатки направленных микрофонов

Недостатками направленных микрофонов являются [3]:

1. Большие габариты, особенно параболических микрофонов; поэтому человек с этим прибором сразу привлекает к себе внимание.
2. Узкая направленность микрофонов - его достоинства и одновременно его недостатки. При очень узкой направленности получается высокое отношение сигнал/шум, так как шумы вне диаграммы направленности не попадают на вход устройства. Однако узкая направленность создает громадные трудности по удержанию луча приёма на нужную точку. Передвижение человека сбивает прицел, порывы ветра изменяют положения отражателя. Поэтому попытка удержать прицел на уровне рта человека равносильна попытке удержать "солнечный зайчик" на одном месте при расстоянии 100 м.
3. Переотражённые волны от стен, колонн и т.д. снижают разборчивость речи.

В связи с вышеизложенным, реальное расстояние использования направленных микрофонов составляет 100 м, а по мнению других специалистов- 5- 6 м.

5.4. Деконспирационные признаки

Прослушивание информации от воздушной волны и структурной волны не имеет деконспиративных признаков.

Деконспиративным признаком направленных микрофонов является наличие на территории новых людей, направляющих на разговаривающих какие-то устройства; технически этот вид подслушивания определить невозможно.

5.5. Система защиты от утечки по акустическому каналу

Активных методов защиты (кроме защиты от утечки информации через воздуховоды) не существует [3]. Некоторые фирмы предлагают использовать активные звуковые генераторы шума, включаемые во время переговоров. Однако уровень сигналов от них должен превышать сигнал разговоров (35 – 50 дБ) и шум в помещении (до 50 дБ); то есть суммарное значение составит 90 дБ, что вызовет болевые ощущение у находящихся в помещении людей [3]. Поэтому зашумление помещения, где находятся люди, практически невозможно.

Для защиты от утечки информации по акустическому каналу применяют методы пассивной защиты:

1. Переговоры проводят при плотно закрытых окнах и дверях в помещениях с двойными оконными рамами и дополнительными тамбурами.
2. Для переговоров используют комнаты, обшивка которых выполнена из звукоизолирующих материалов (пористая штукатурка, ворсистые ковры, пенобетон и т.д.). В этих материалах много поверхностей раздела между воздухом и твердым телом, поэтому звук, проходя через каждую из этих поверхностей, многократно отражается и поглощается (например, слой пенопласта толщиной 5см эквивалентен по звукоизоляции бетонной плите толщиной 50 см [7]).

Для предотвращения утечки информации через воздуховоды их необходимо выполнить по специальной конструкции (например, много колен перегиба и т.д.

[1]), а так же в них можно устанавливать динамики от генераторов акустического шума.

Для защиты информации от утечки через направленные микрофоны необходимо плотно закрывать помещения, а при переговорах на открытой местности - проводить организационные мероприятия по выявлению новых лиц, направляющих какие-либо устройства в сторону беседующих.

6. ПРОВОДНОЙ КАНАЛ УТЕЧКИ ИНФОРМАЦИИ И ПРИМЕНЕНИЕ ДИКТОФОНОВ

Акустоэлектрический преобразователь - это устройство, преобразующее акустическую энергию в электромагнитную, например- микрофон. Акустический сигнал на объекте с помощью установленного микрофона преобразуется в электрический сигнал. Этот сигнал специально проложенными двумя проводами передаётся в соседнее помещение (где находится агент) и телефоном преобразуется в прослушиваемый акустический сигнал.

Акустический сигнал можно и просто записывать на оставленный в определенном месте диктофон.

6.1. Упрощенный принцип работы микрофона и телефона

В комнате 1 (рис 6.1), из которой нужно получить информацию, устанавливается микрофон, два провода с которого через стену поступают в комнату 2, где находится агент; здесь же находится источник питания E для микрофона и телефонный наушник. Предположим, что, у нас угольный микрофон. Под влиянием звука чувствительная мембрана микрофона приходит в движение и воздействует на угольный порошок, находящийся в корпусе (порошок сжимается или разжимается), его сопротивление R1 меняется,
в результате изменяется ток в первичной обмотке трансформатора Тр1

$$I_{Tp1} = \frac{E}{R1 + R2} \quad ,$$

где R2 – эквивалентное сопротивление первичной обмотки Тр1.

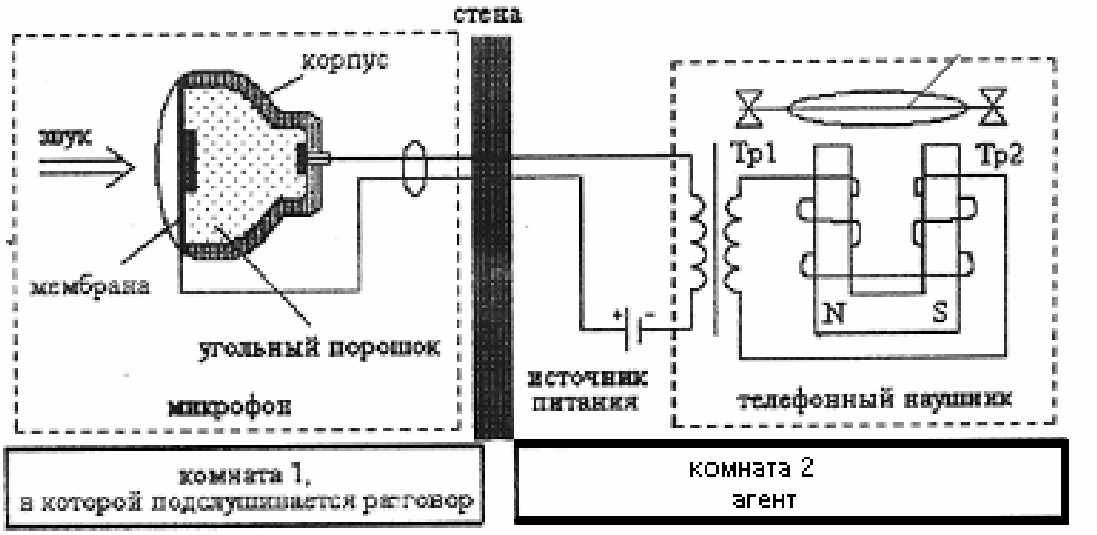


Рис. 6.1

Изменяющийся ток $I_{Тр}1$ трансформируется во вторичную обмотку трансформатора Tpl, что приводит к изменению тока Тр2, обмотка которого намотана на магните. Изменение тока Тр2 приводит к изменению магнитного потока, в результате чего мембрана Тр2 приводится в механическое движение, т.е. происходит колебание воздуха и в комнате 2 воспроизводится речь. В качестве проводов используются тончайшие (не толще волоса) провода, которые можно плести в ковровое покрытие и т.д.

В настоящее время в средствах акустической разведки наиболее широко применяются динамические, конденсаторные и пьезомикрофоны. В работе [8] дается краткое описание их принципа работы, которое приводится ниже. Автор данного пособия дополнил текст упрощенными рисунками, поясняющими принцип работы микрофонов.

Принцип действия *динамического микрофона* (рис 6.2) заключается в том, что катушка находящаяся в радиальном магнитном поле и жестко соединенная с диафрагмой, колеблется под действием звукового давления, пересекая силовые линии. В следствии этого в ней индуцируется электродвижущая сила, возникает напряжение пропорциональное звуку.

Для создания магнитного поля обычно используют кольцевой магнит; диафрагму изготовляют из легких, но прочных материалов.

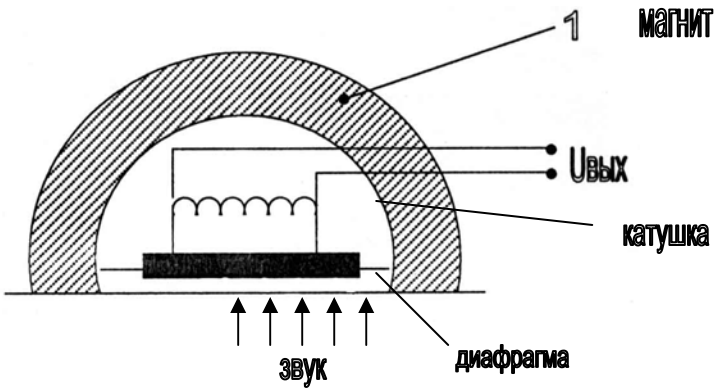


Рис. 6.2

Конденсаторный микрофон (рис 6.3) представляет собой конденсатор, один из элементов которого- массивный магнит 1,
а второй – тонкая натянутая мембрана 2.

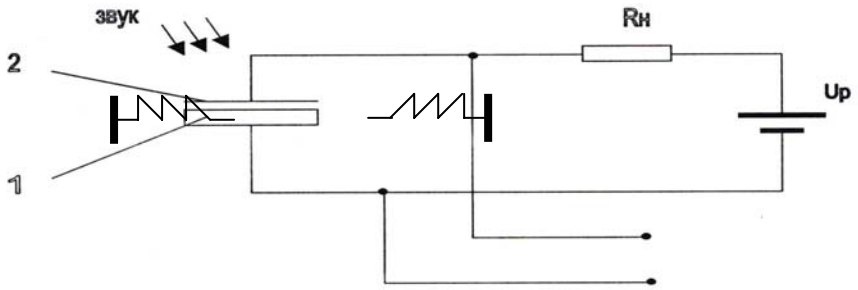


Рис. 6.3

На конденсатор подается поляризующее напряжение U_p через высокоомное сопротивление R_H. Источник поляризующего напряжения не расходует энергии, так как постоянной составляющей тока нет. При колебаниях мембраны емкость конденсатора С изменяется,

$$C=F(\textit{звукового давления})$$

а так как заряд q остаётся постоянным (конденсатор не успевает перезаряжаться из-за большой постоянной времени $t=R_H C_O$), то изменяется напряжение на нем.

$$U_{вых} \approx \frac{q}{C} = F\ (\textit{звукового давления})$$

В *электретном микрофоне,* (рис 6.3) в отличие от конденсаторного, поляризующее напряжение образовано предварительной электризацией электрода 1, изготовляемого из полимеров или керамических поляризующихся материалов.

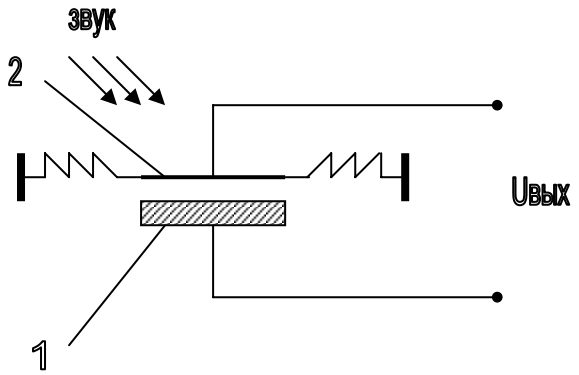


Рис. 6.4

Такой электрод имеет металлическое покрытие, которое по существу и является электродом конденсатора, а электрет служит лишь источником поляризующего напряжения. Поляризация электрета постепенно уменьшается и через несколько лет требуется или его замена, или повторная поляризация.

В этом недостаток электретного микрофона по сравнению с конденсаторным, но и достоинство, так как для него не требуется источника напряжения. По механическим, акустическим характеристикам, а также по конструкции электретный микрофон ничем не отличается от конденсаторного.

В *пьезомикрофонах* (рис 6.5) используется явление пьезоэффекта.

Звук воздействует на мембрану 2, которая давит на пластину 1. Пластина 1 изготавливается из кварца или пьезокерамики. Под влиянием давления на пластине 1 формируется заряд. Величина заряда q=F(звукового давления). Далее это изменение заряда преобразуется в выходное напряжение.

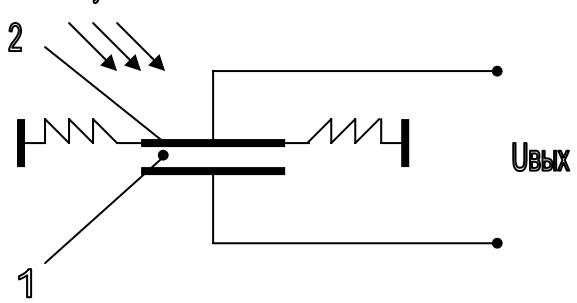


Рис. 6.5

Микрофоны динамического, конденсаторного или электретного типов имеют чувствительность 6…10мВ/Па и способны регистрировать голос человека нормальной громкости на расстоянии до 10..15 м, а некоторые образцы - на расстоянии до 20 м. При этом частотный диапазон составляет в основном от 100...300 Гц до 5...7 кГц. Однако в некоторых случаях используются микрофоны с частотным диапазоном от 50 Гц до 15...18 кГц [8]; диаметр микрофонов различный, в сверхминиатюрном исполнении выпускаются микрофоны с диаметром менее 2.5мм.”

6.2. Проводной микрофон с повышенным отношением сигнал/шум

Для улучшения отношения сигнал/шум [9] сигнал с микрофона МК (рис. 6.6) предварительно усиливается каскадами, выполненными на транзисторах VT1 и VT2.

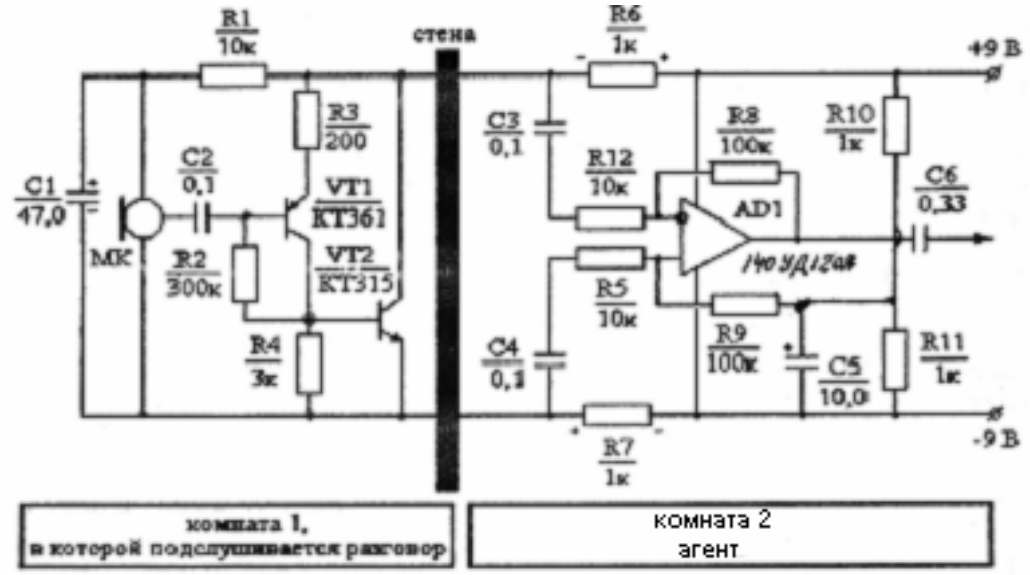


Рис. 6.6

На основе VT2 собран парафазный усилитель с коллекторной нагрузкой R6 и эмиттерной нагрузкой R7, с которых сигнал подаётся на дифференциальный усилитель AD1. За счет того, что полезный сигнал на входы AD1 поступает в противофазе, а помеха, создаваемая на соединительных проводах – в фазе, сигнал усиливается, а помеха подавляется. Усиление сигнала и существенное подавление помехи позволяет обеспечить уверенный съем информации на расстоянии до 100 м [9].

6.3. Использование коммуникаций в качестве соединительных проводов

Проводное подключение внедрённого микрофона позволяет службам охраны по проводу обнаружить пункт прослушивания со всеми вытекающими последствиями.

В связи с этим агенты предпочитают использовать в качестве проводов имеющиеся коммуникации, например провода пожарной и охранной сигнализации, трубы системы отопления и водоснабжения [7]. На рис 6.7 а) приведён пример подключения системы ЛСТ-ВО-2 для передачи информации по трубам водоснабжения (Трубы в исходном состоянии изолированы друг от друга). На рис 6.7 б) приведен пример использования системы ЛСТ-ОС-1, микрофон которой размещен в извещателе охранной сигнализации, установленном на объекте. При сопротивлении МК значительно больше R микрофон не оказывает влияние на охранную сигнализацию. Охранные службы по контрольной панели не видят нарушения режима работы охранной сигнализации, а агент получает нужную информацию.

Кабель, соединяющий телевизор с антенной, также может успешно выполнять роль соединительных проводов. Например, в 1987 году в жилом доме советских дипломатов в Вашингтоне по просьбе жильцов американским техником была установлена телевизионная антенна коллективного пользования. В результате этой "работы" были обеспечены не только нормальный телевизионный прием, но и подслушивание разговоров во всех квартирах, где находились телевизоры [8].

6.4. Негласная запись информации на диктофоны

Диктофон (магнитофон) представляет собой совокупность устройства преобразования акустического сигнала в электрический (т.е. микрофон с полосовым усилителем) и устройство записи. Диктофоны подразделяются на:

- кинематические;
- бескинематические.

а)

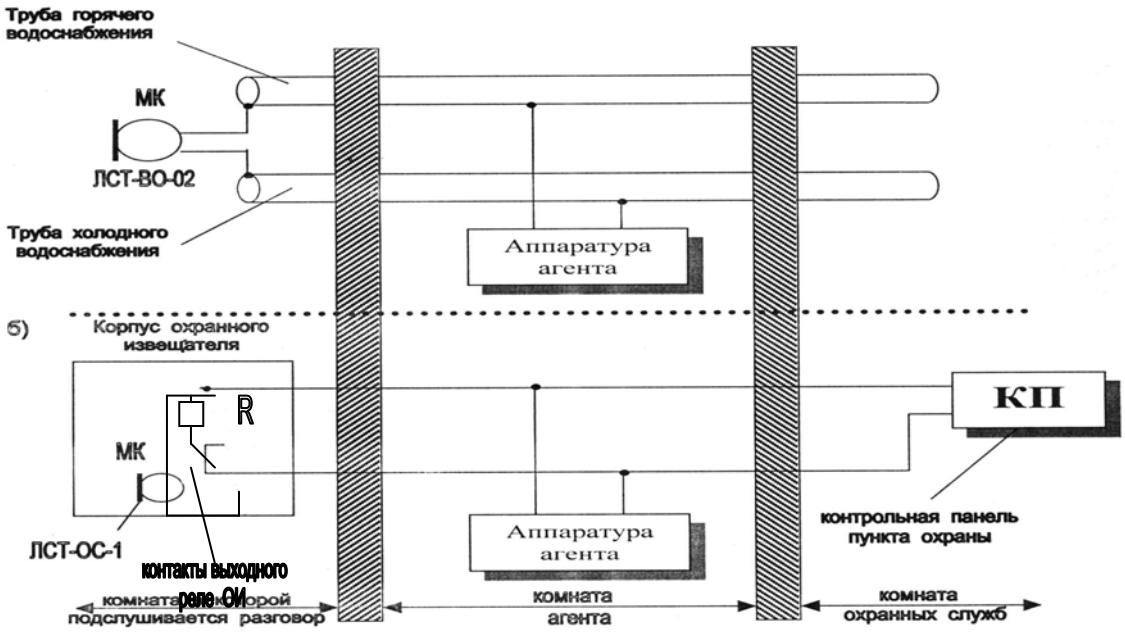


Рис. 6.7

В *кинематических* диктофонах запись производится на ленту, проволоку. Обычно длительность записи (1 - 3) часа; часть магнитофонов активизируется (т.е. включается с целью

экономии ленты) голосом. Примером таких диктофонов является AIWA TP-X900, AIWA TP-L950, OLYMPUS L-400, SONY-950 [3]. Для обеспечения высококачественной записи используются профессиональные магнитофоны MARANIZ PMD-201, PMD-221 с длительностью записи 3 - 6 часов.

В *безкинематических* (цифровых) диктофонах лентопротяжный механизм не используется; в качестве памяти используются сменные миникарты с ПЗУ 2 - 4 Мб, длительность записи 0.5 - 2 часа; магнитофоны обычно активизируются голосом [3]. Имеются сведения о цифровых магнитофонах (например PK-1950-SS) со временем непрерывной записи 16 часов [8]. Миниатюрные цифровые диктофоны имеют весьма малые размеры. Например, минидиктофон Machina EC-CC900 со временем записи до 115 минут имеет размер кредитной карточки, а минидиктофон Machina EC-PC60 выполнен в виде авторучки. Достоинством цифрового диктофона является то, что его невозможно обнаружить с помощью обычных детекторов диктофонов [8].

Диктофоны обычно заносятся на объект в камуфлированном исполнении и изымаются по определенной легенде. Передача информации с диктофона по радиоканалу будет рассмотрена в разделе радиомикрофоны.

6.5. Деконспирационные признаки

Вариант установки проводных микрофонов - заходовый, необходимо проникнуть в комнату 1 для установки микрофона с соединительными проводами; кроме того, агент должен находится вблизи комнаты 1, так как длина L соединительных проводов ограничена в связи с ухудшением отношения $U_{сигнал}/U_{шум}$ при увеличения L. Для установки и изъятия диктофона так же необходимо посещение объекта.

Деконспирационного технического признака работы проводного микрофона не существует, так как он является пассивным устройством. Деконспирационного технического признака работы цифрового диктофона нет. Их обнаружение возможно только при визуальном осмотре места. Деконспирационным признаком лентопротяжного диктофона является создаваемое им электромагнитное поле.

6.6. Системы защиты от диктофонов

Особенностью диктофона с правовой стороны заключается в том, что он не является спецсредством и не надо получать разрешение на его применение. Как указывалось ранее цифровые диктофоны не имеют деконспирационных признаков, ленточные микрофоны создают электромагнитное поле, по которому их можно обнаружить [10].

Ленточные диктофоны имеет следующие недостатки.

1. Электромагнитное паразитное излучение мотора.
2. Наличие акустических шумов, создаваемых в процессе работы движущимися частями.
3. Поле, создаваемое электрическими цепями генератора тока стирания и подмагничивания (ГСП).
   Вышеуказанные недостатки могут быть существенно ослаблены применением металлического корпуса.
4. Достаточно большие габариты, определяемые, в основном, лентопротяжным механизмом (ЛПТ).

Теоретическая дальность обнаружения диктофона, который можно представить в виде диполя с мощностью дипольного момента 10^{-5} Ам^2 – 10^{-4} Ам^2 составляет 2 – 4 м [10]. Практически возможность обнаружения диктофонов ограничена наличием помех. Обычно сигнал от помех в 10^5 раз превышает сигнал от работающего диктофона (Например, промышленная сеть создает помеху 10^{-6} – 10^{-5}А/м, а диктофон на расстоянии 1м создает помеху лишь 10^{-6} – 10^{-5}А/м), поэтому даже при применении сложных устройств можно обнаружить диктофон на расстоянии не более (0,5 – 1,8) м.

Существуют стационарные и портативные детекторы диктофонов. Портативные детекторы часто дают ложные тревоги, так как при их перемещении происходит пересечение магнитного поля земли и возникает э.д.с., превосходящая сигнал от диктофона.

Стационарные детекторы диктофонов устанавливаются в спинке и подлокотниках кресла установленного в зале переговоров. Сигналы с этих детекторов поступают на компьютеры. Основная задача компьютера определить наличие сигнала от детектора на фоне мощных помех. Для этих целей осуществляется ряд операций.

1. Создаётся электромагнитный шаблон обстановки, т.е. осуществляется спектральный анализ сигналов в помещении до начала заседания.
2. Создаётся шаблон изменения электромагнитной обстановки от проезжающих трамваев, от включения в процессе заседания организационной техники и т.д. Эти частоты исключаются.
3. Используются большое количество детекторов диктофонов (датчиков). От мощных удалённых станций расстояние до всех датчиков будет одинаково и сигнал с датчиков будет одинаков; от ближнего маломощного источника (диктофона) сигналы будут разные, так как расстояние от диктофона до соседних датчиков разные; это позволяет исключить мощные станции и обнаружить маломощный сигнал.

Описанные принципы обнаружения диктофонов применены в офисной системе PTRD 018 (фирма Смерш Техникс), построенной на базе микропроцессора 80C251SB.

Цифровые технологии, реализованные в данной модели, позволяют охватить до 16 посадочных мест, что в 8 раз превышает возможности аналоговых моделей. Применение рассмотренных методов обработки сигналов обеспечивает нормальную работу прибора даже в помещении с очень неблагоприятной помеховой обстановкой, при этом ложные срабатывания при соблюдении правил эксплуатации крайне маловероятны. Дальность обнаружения при благоприятных условиях достигает 1,5 м для каждого датчика, что на начало 1997 года являлось абсолютным рекордом на рынке определения диктофонов.

Ранее выпускаемые обнаружители диктофонов PTRD 014, PTRD 016 и RM-200 (их радиус действия 0,6 м) по своим характеристикам значительно уступают PTRD 018.

Применение экранов в диктофонах уменьшает примерно в 2 раза дальность их обнаружения.

Недостатком стационарной системы обнаружения диктофонов является их жесткая привязка к креслу [10], вследствии чего данные системы не нашли широкого применения.

Кроме обнаружения работающего диктофона используются специальные методы для их нейтрализации. Нейтрализация производится следующим образом:

1. Воздействием размагничивающим устройством на магнитную плёнку при прохождении посетителя через тамбур с размагничивающей аркой;
2. Воздействием на микрофон в ультразвуковом диапазоне с целью перегрузки усилителя и включением активных акустических помех в речевом диапазоне;

Оба данных вида воздействия не нашли широкого применения из-за необходимости изготовления специальной арки и вредности работы персонала в помещении с высоким уровнем зашумления.

3. Воздействием специальными сигналами небольшой мощности на электронные цепи диктофона с целью вывода усилителей в режим перегрузки.

Практически затраты на обнаружение диктофонов могут позволить себе только очень крупные фирмы. В большинстве случаев используются организационные методы по осмотру помещения с целью обнаружения вновь появляющихся предметов с последующим их осмотром.

7. ВИБРАЦИОННЫЙ КАНАЛ УТЕЧКИ ИНФОРМАЦИИ

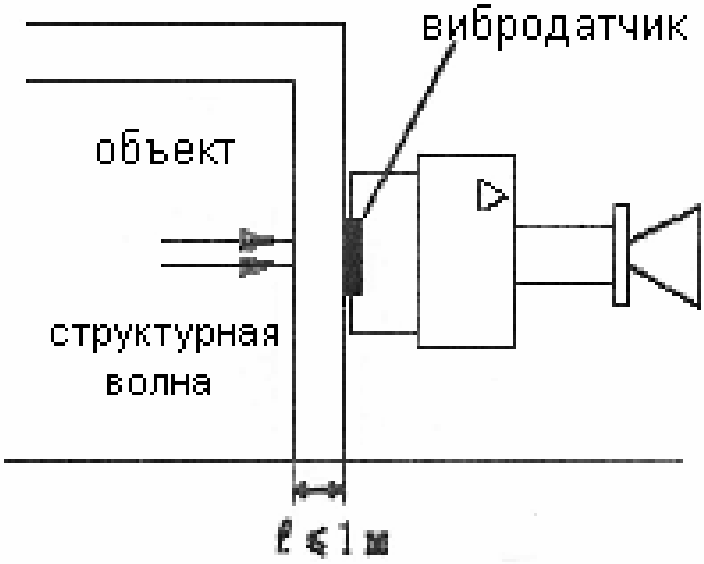
Воздушные волны человеческой речи воздействуют на строительные конструкции и приводят к колебаниям стен, стекол, батарей и т.д. Для съема информации со стен используется электронные стетоскопы, для съема информации со стекла - лазерные системы, для съема информации с воды трубопроводов – гидроакустические преобразователи.

7.1. Электронные стетоскопы

Электронные стетоскопы состоят из вибродатчика, усилителя и динамика или передатчика (рис. 7.1).

Вибродатчик устанавливается на потолке или стене с наружной стороны от объекта прослушивания. Звуковая информация воздействует на стену и вызывает ее механические колебания. Колебательные ускорения поверхности кирпичной стены с толщиной 0,5м от воздействия акустического сигнала 75дБ составляют приблизительно 10^{-5}g, где g=9,8 м/см^2 [11]. Вибродатчик воспринимает эти колебания и преобразует их в электрический сигнал, который затем усиливается и подаётся на динамик или радиопередатчик.

Распознавание речи зависит от материала конструкций, толщины конструкций, от шумов образующихся в конструкции, от движения людей, транспорта, вибрации и т.д. В табл. 7.1



приведены данные дальности различимой передачи механических колебаний в зависимости от материала перекрытий и вида заделки
труб [3].

Рис. 7.1

Основным преимуществом стетоскопа является трудность его обнаружения, так как он устанавливается в соседнем помещении.

По данным, приведенным в работе [9], размер датчика устройства DTI составляет 2,2хО,8 см, диапазон частот 300 – 3000 Гц, вес 126 грамм, - коэффициент усиления 20 тысяч. С помощью подобного устройства можно прослушивать разговоры через стены толщиной до 50 – 100 см.
В настоящее время широкое применение нашли стетоскопы с передачей информации по радиоканалу, например, SIPE PS, SIPE OPTO 2000.

Таблица 7.1

№	Материалы конструкций	***Дальность передачи***	Примечание
1	Железобетон	60 см	
2	Кирпич	50 см	
3	Гипсовые стены	30 см	
4	Стекло без воздушной прослойки		Толщина стекла не влияет на затухания сигнала
	Стекло при двух рамах и расстоянии между ними менее или равное 15см		Затухание сигнала в 3-5 раз
5	Тепло и водопроводные трубы	Несколько этажей	При нежесткой заделке труб в стене
		В пределах помещения	При жесткой заделке труб в стене

7.2. Лазерные системы подслушивания

Лазерные системы подслушивания (рис 7.2) состоят из лазерного передатчика, фотоприемника, усилителя.

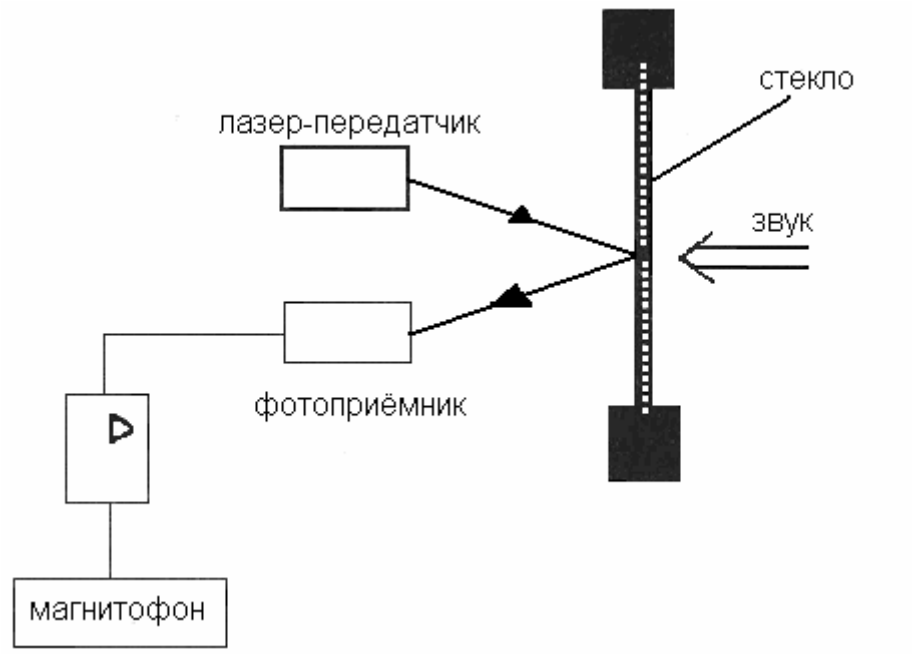


Рис. 7.2

Под воздействием звука оконное стекло колеблется подобно мембране микрофона. Оператор направляет луч лазера на окно помещения, информацию из которого необходимо получить. Колебание окна модулирует луч. Отраженный промодулированный луч лазера (отражается под углом, равным углу падения) принимается фотоприемником, сигнал демодулируется и записывается на магнитофон или прослушивается.

Например: фирма Hewlett-Packard (США) выпускает прибор HP-150, имеющий размер кейса; прибор работает на длине волны λ=0,63 мкм, обеспечивает съем информации на расстоянии до 1000 м, его стоимость ≥ 10тыс. $. В России выпускается прибор ЛСТ-ЛА2, обеспечивающий съем информации до 100 м, его стоимость значительно ниже.

Данные по лазерным системам YKG GD-7800, STG-5410, PK-1035SS приведены в работе [8].

Недостатки лазерных систем:

1. Трудность установки системы. Необходимо найти такое место, чтобы падающий и отражённый луч попадали на устройство. Сложность заключается в том, что стекло имеет кривизну и отраженный луч может не попасть в лазерную систему.
2. Трудность получения информации при приоткрывании окна. Опытный сотрудник фирмы обычно в процессе разговора приоткрывает и призакрывает окно, сводя на нет усилия по лазерному прослушиванию.

7.3. Гидроакустические преобразователи

Гидроакустические преобразователи снимают информацию с воды, протекающей по водопроводу (рис. 7.3).

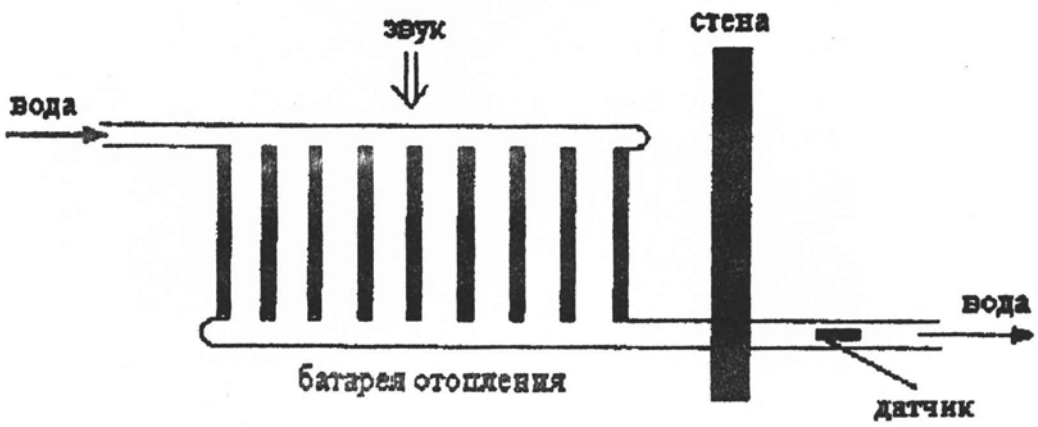


Рис. 7.3

Звук воздействует на трубопровод и соответственно на воду. Вода протекает по отопительным системам и информация передается на большие расстояния, так как звуковые волны распространяются в воде с малым затуханием. Преобразовав изменение давления воды в звук, можем получить информацию. Дальность прослушивания сильно зависит от шумов водопровода.
Гидроакустические датчики широко используются в военно-морском флоте для обнаружения подводных лодок (прослушивается шепот в подводной лодке, находящейся на глубине несколько десятков метров), сведений о применении их в коммерческой разведке не имеется.

7.4. Десконспирационные признаки

Основными достоинствами электронных стетоскопов, лазерных систем и гидроакустических преобразователей являются:

- беззаходовый вариант, то есть эти устройства не надо устанавливать на объекте;
- отсутствие деконспирационных признаков.

7.5. Система защиты информации от утечки по вибрационному каналу

Данный канал утечки не имеет деконспирационных признаков, и, следовательно, нет возможности технически определить происходит ли утечка информации по этому каналу. Оценка возможности утечки информации осуществляется специалистами на основании изучения архитектурно-строительной документации на определенную часть объекта с последующей проверкой выводов с помощью стетоскопов.

Если оказывается, что такой канал утечки возможен, то встаёт задача закрытия этого канала. Для закрытия канала целесообразно применять искусственные источники помех – системы виброакустического зашумления (СВЗ). Структурная схема СВЗ приведена на рис 7.4.

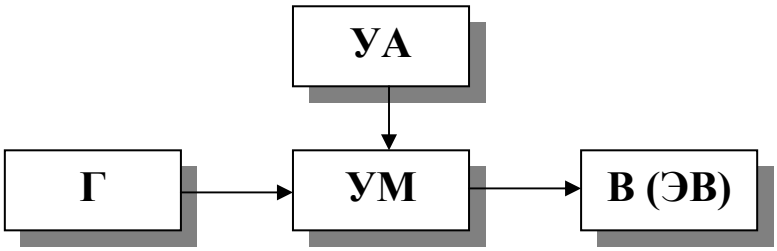


Рис. 7.4

Она состоит из генератора шума Г, формирующего помеху в диапазоне частот 0,2 – 5 кГц; усилителя мощности УМ, включаемого устройством управления УА (УА включается голосом или вручную) и вибратора В (электромеханического преобразователя), обеспечивающего преобразование электрического сигнала в механические колебания конструкции. Вибратор жестко крепится к конструкции с помощью винта.

Генератор создает шум (лучше всего в виде речевого хора), который подается на УМ. Сигналом с УА включается УМ, и сигнал с него поступает на вибратор. Вибратор начинает работать и появляются колебания стены, которые зашумляют колебания стены от акустического сигнала. Радиус действия одного вибратора обычно от 0,8 м до 3 метров.

Основными критериями эффективности системы являются [4, 11]:

- превышения уровня создаваемых СВЗ помех над уровнем, созданным акустическим сигналом, содержащим защищаемую информацию;
- равномерность создаваемых СВЗ помех в заданном частотном диапазоне для конструкций из разных материалов;
- структура помех создаваемых СВЗ;
- уровень паразитных акустических шумов (создаваемых СВЗ в помещении), которые снижают комфортность работы людей в этом помещении.

7.5.1. Уровень создаваемых СВЗ помех в строительных конструкциях

а) “Минимальная степень защиты речевой информации осуществляется, когда при многократном прослушивании фонограммы невозможно восстановить смысл сообщения. Это называется нулевой смысловой разборчивостью [4]” . Это происходит при отношении сигнал/помеха равном минус 10дБ, то есть, когда помеха в 3 раза превышает сигнал.

б) “Максимальная степень защиты соответствует ситуации, когда невозможно установить сам факт проведения беседы”. Это происходит при отношении сигнал/помеха равным минус 20дБ, то есть, когда помеха в 10раз превышает сигнал.

Спектральные характеристики ряда систем приведены на рис 7.5. Вибраторы были установлены на кирпичной стене толщиной 0,5 м;

в большинстве случаев расстояние от вибратора до точки контроля бралось 3м [4]. Кривая 1 является АЧХ системы “Шорох”; кривая 2 характеризует систему “Порог-2М” при расстоянии до вибраторов 0,8 м; кривая 3 описывает АЧХ системы VNG-006DM; кривая 4 показывает какие колебательные ускорения получает стена при воздействии на нее акустического сигнала 75 дБ. Как видно из рисунка, система “Шорох” создает от своих вибраторов в 100 раз большие колебательные ускорения поверхности стены, чем акустический сигнал, содержащий защищаемую информацию; системы “Порог-2М” и “VNG-006DM” обеспечивают десятикратное превышение помехи над акустическим сигналом. Все три рассмотренные системы обеспечивают максимальную степень защиты $U_{сигнал}/U_{помеха} \geq$ -20дБ. Для зашумления различных строительных конструкций необходима регулировка напряжения подводимого к вибратору.

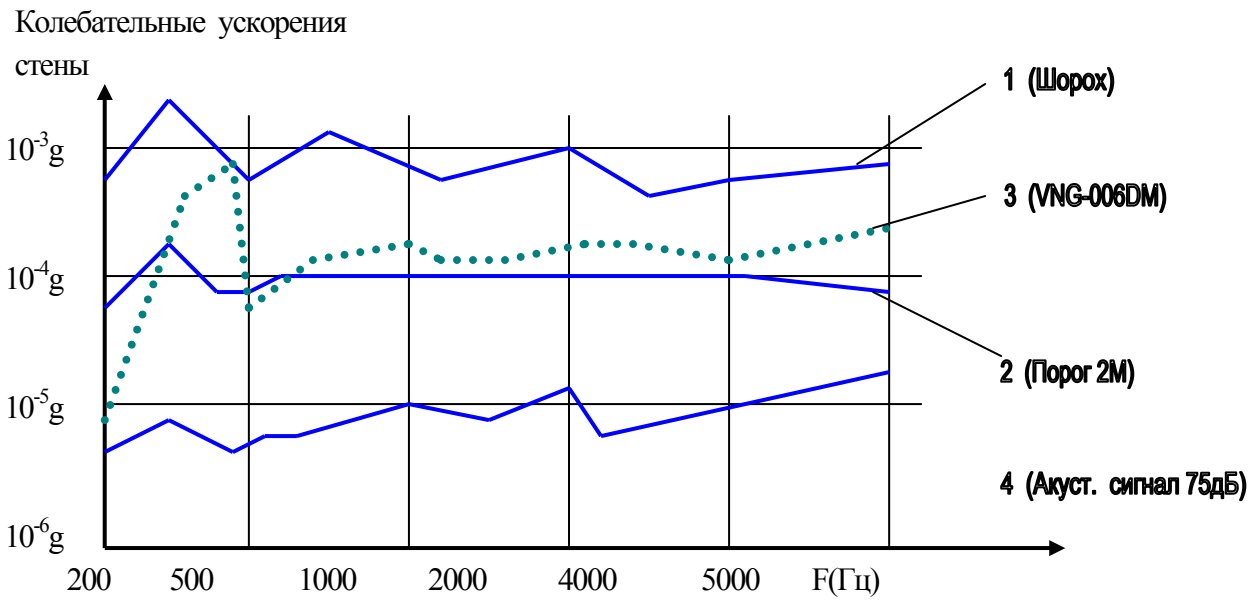


Рис. 7.5

Так например, при одинаковых напряжениях на вибраторе уровень создаваемых вибрационных ускорений на стекле примерно на 20дБ выше, чем на кирпичной стене. В системах “Шорох” и “Порог 2М” такая регулировка существует, во многих же системах ее нет.

7.5.2. Частотные характеристики систем (равномерность создаваемых СВЗ помех)

95 % смысловой речевой информации лежит в диапазоне 200 Гц – 5 кГц. Уличные шумы, шаги, хлопки дверей, работа бытовой аппаратуры создают структурные шумы в конструкциях. Частотный диапазон их близок к спектрам вибрации от речевых сигналов. Агент со стетоскопа снимает полезный сигнал в совокупности с шумами. СВЗ должна создать помеху, подавляющую этот суммарный сигнал во всем частотном диапазоне, то есть в диапазоне 200 Гц – 5 кГц. В связи с тем, что спектральная плотность сигнала в рассматриваемом диапазоне примерно постоянна ((рис 7.5), (кривая 4), то и помеха создаваемая СВЗ должна быть одинакова в этом диапазоне частот. Превышение создаваемой помехи над нормой желательно не больше 2 – 10 дБ [4].

Маскирующая помеха обладает асимметричностью [4]. Асимметричность проявляется в том, что помеха оказывает небольшое влияние на токи маскируемого сигнала ниже ее собственной частоты, но сильно затрудняет восприятия более высоких частот. Поэтому желательно, чтобы в области низких частот созданная помеха немного превышала норму, а в области высоких частот они может быть несколько меньше нормы [4].

Разные строительные конструкции имеют разные АЧХ и поэтому затруднительно создавать одинаковые колебательные ускорения поверхности во всем частотном диапазоне. Только часть СВЗ удовлетворяет этим требованиям, например: “Шорох”, “Порог 2М”, VNG-006DM [11] ; ANG-2000, “Гонг”, Барон и ряд других систем. АЧХ части этих систем приведена на рис. 7.5.

В большинстве этих систем необходимое превышение уровня помехи над уровнем речевого сигнала обеспечивается эквалайзером – системой настройки спектра помехи.

7.5.3. Структура помех создаваемых СВЗ

В первых простейших СВЗ зашумления проводилось сильной помехой на одной или нескольких частотах; однако вскоре агент стал определять эти частоты и устанавливать заграждающие фильтры на эти частоты, что свело на нет зашумляющее действие.

С помехой в виде белого шума так же научились быстро справляться за счет использования методов шумочистки. Цифровая обработка сигнала позволяет получить разборчивую речь при отношении $U_c/U_{помеха}$=-20дБ [11].

Сейчас для эффективного подавления сигнала применяют два метода:

1) Первый метод заключается в зашумлении стены помехой, вид которой определяется по результатам предварительных измерений. Стабильным фиксированным сигналом воздействуют на стену, измеряют спектр и уровень вибраций. Изменяют вид зашумления так, чтобы получить равномерную частотную характеристику и нужный уровень шума. Указанный метод применяется, например, в системах “Порог-2М” и “Шорох”. В системе “Порог-2М” эта операция производится автоматически с автоматической оценкой результатов и выдачей заключения о выполнении или невыполнении поставленной задачи.

В системе “Шорох” настройка производится оператором, который вначале грубо устанавливает вид шума (белый, розовый, ниспадающий) и затем приводит эквалайзером тонкую регулировку спектра.

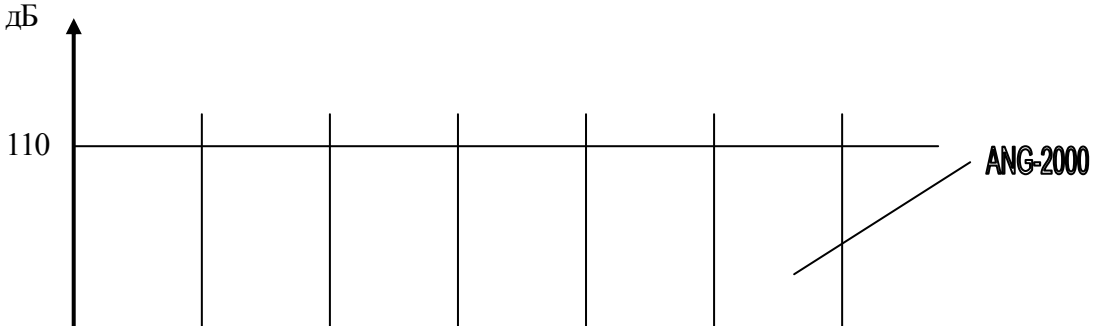
2) Второй метод заключается в создании не фиксированной помехи с речеподобной структурой. Так как помеха не фиксированная (используется не одно и то же речевое выступление), то очистить запись от такой помехи становится очень трудно. Для создания такой помехи можно использовать магнитофон с большим набором предварительно записанных речей. Другой вариант создания такой помехи – это смешивание сигналов нескольких вещательных станций (соответственно нужно несколько приёмников) с сигналом шумогенератора. Этот вариант применяется в СВЗ “Барон” фирмы НЕЛК [11].

В настоящее время большинство СВЗ создают помеху в виде белого шума и только небольшое количество СВЗ (Шорох, VNG-006DM и др.) создают более перспективную речевую помеху.

7.5.4. Уровень паразитных акустических шумов, создаваемы СВЗ в помещении

При включении СВЗ в помещении создается акустический шум из-за работы вибратора. Этот шум воздействует на обслуживающий персонал.

На рис. 7.6 приведены спектры акустических шумов, создаваемые фоном и работой систем “Порог 2М”, VNG-006DM, ANG-2000, измеренные на расстояние 1 м от вибратора [11].



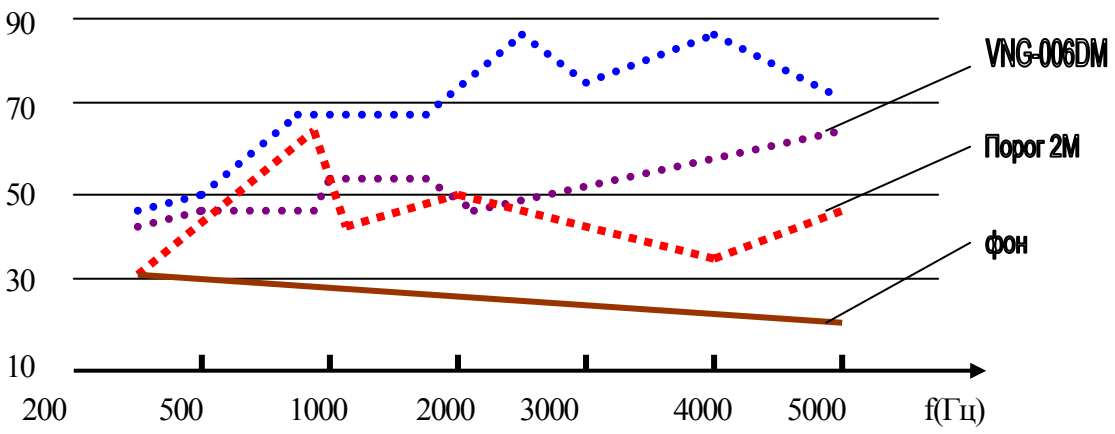


Рис. 7.6

Как видно из рисунка СВЗ создают значительные шумы (напомним, что уровень спокойного разговора 55 дБ SL, разговор по телефону 75 дБ, SL). С целью уменьшения этих шумов рекомендуется вибратор устанавливать в нише стены с последующей заделкой этой ниши.

По данным работы [4] меньший уровень акустических шумов создаёт пьезокерамический вибратор; кроме того, он имеет высокий механический импеданс подвижной системы и поэтому легче согласуется с конструкциями, имеющими высокое акустическое сопротивление (кирпичные и бетонные перекрытия). Поэтому электромагнитные преобразователи (используются в системах “Порог-2М”, ANG-2000) перспективно заменить на пьезокерамические (используются в системе VNG-006DM). Скорей всего и хорошая система “Порог-2М” от этой модернизации улучшит свои параметры.

7.5.5. Простейший метод определения качества работы СВЗ

В помещении создается акустический сигнал с уровнем 75 дБ со спектром речевого хора. В местах возможного перехвата информации устанавливается стетоскоп и измеряется снимаемый с него сигнал A_1. Затем включается СВЗ и со стетоскопа измеряется сигнал A_2. Если $A_1/A_2 \approx$-10дБ, то выполняются минимальные условия защиты. Если $A_1/A_2 \approx$ -20дБ, то можно считать, что обеспечена максимальная степень защиты.

7.5.6. Защита от съема информации со стекла

Защита обеспечивается установкой вибратора на стекло или за счёт периодического приоткрывания и призакрывания окна. При выполнении этой операции меняется угол отражения лазерного луча, в результате чего отражённый луч не попадает на приемное устройство агента.

8. ЭЛЕКТРОМАГНИТНЫЙ КАНАЛ УТЕЧКИ ИНФОРМАЦИИ

Электромагнитный канал утечки информации занимает лидирующее место среди других каналов утечки информации. Источниками утечки информации являются:

- действующая аппаратура (ПЭВМ, дисплеи, факсы, телетайпы, радиотелефоны и т.д.), необходимая для функционирования фирмы;
- вспомогательная аппаратура; кабели, находящиеся и проходящие через помещение фирмы;
- речь в помещении.

8.1. Прослушивание информации от радиотелефонов

При передаче информации по мобильному телефону происходит излучение радиоволн, которые соответственно могут быть приняты заинтересованным лицом. Перехват информации возможен не только на частоте передаче, но и на побочных частотах (гармониках, паразитных и комбинированных частотах). Наиболее прост перехват информации при разговоре по незащищённому радиотелефону:

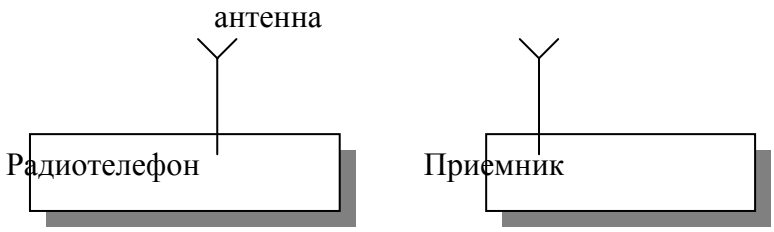


Рис. 8.1

Настроив приемник (рис. 8.1.) на соответствующую частоту радиотелефона можно без хлопот получить информацию.

8.2. Прослушивание информации от работающей аппаратуры фирмы

8.2.1. Утечка информации от мощной офисной аппаратуры

Работающее электрооборудование (например, дисплеи, накопители и т. п.) несанкционированно излучает в эфир информацию.

Дисплей, как известно, состоит из устройств горизонтальной развёртки, вертикальной развёртки, видео усилителя, блоков питания и устройства вывода визуальной информации. Частота следования пикселей меняется то 0 до (35-85) МГц. Мощные каналы видеоусилителя и отходящие от них соединительные проводники можно рассматривать как передатчик, несанкционированно излучающий информацию. Информация может быть восстановлена с помощью обычного телевизора, но без сигналов синхронизации. Изображение на экране будет перемещаться в вертикальном и горизонтальном направлениях. При использовании дополнительной приставки, перехватывающей мощные сигналы синхронизации кадровой и строчной развертки, изображение будет синхронизировано. В последнее время синхронизацию стали осуществлять от более дешевого собственного генератора, частоту которого меняет оператор до момента появления неподвижного изображения. Используя специальную антенну, фильтр и усилитель можно снять информацию

с расстояния до 150 м. При использовании специализированных приемников осуществляется перехват излучения от мониторов
с металлическим кожухом на расстоянии до 400 м, а для дисплеев
с пластмассовым кожухом до 1200 м [1].

В работе [12] приводится упрощённая методика определения дальности, на которой возможен перехват ПЭМИ (побочных электромагнитных изучений). В качестве тестового сигнала обычно берётся сигнал, который "легко идентифицируется при приёме, и который переводит аппаратуру в состояние, при котором уровень создаваемых ею побочных излучений максимален". Для дисплеев и систем внутреннего телевидения, таким тест- сигналом является создаваемая компьютером картинка, состоящая из чередующихся чёрно-белых полос.

В качестве индикатора дальности L_g берется телевизор с настольной антенной. Включаем ПЭВМ, дисплей и телевизор, расположенный рядом с дисплеем. На экране телевизора будем наблюдать чередующиеся и мелькающие чёрно – белые полосы. Перемещая телевизор, добьёмся пропадания этих полос. Расстояние, измерённое между дисплеем и телевизором, будет являться дальностью излучения дисплея L_g .

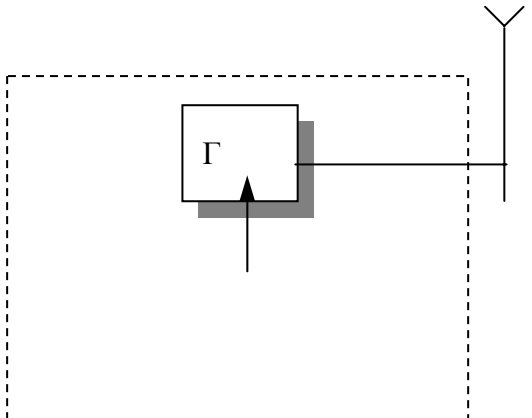
Если отсутствует возможность проведения исследований на границе контролируемой зоны или недостаточна чувствительность телевизора, то "можно воспользоваться расчётно - измерительным способом [12], который заключается в выполнении ряда операций", аименно:

1. Устанавливаем телевизор и измерительную аппаратуру (например, осциллограф) на расстоянии R_0=1 м от дисплея и включаем аппаратуру;
2. Телевизором осуществлён поиск тестового сигнала;
3. Осциллографом измеряем на антенне телевизора значение сигнала в присутствии шумов $И_{с+ш}$;
4. Отключим дисплей и измерим в том же месте шумы $И_ш$;
5. Рассчитываем U_c $$U_{\tilde{N}} = \sqrt{U_{\tilde{N}+\emptyset}^2 - U_{\emptyset}^2}$$
6. Расчетная дальность $L_{рас}$, на которой возможен перехват излучения дисплея находится из формулы:

$$L_{ÐÀÑ} = R_O \cdot \frac{U_{\tilde{N}}}{U_{\emptyset}}$$

Если $L_{рас}$ получается большой, то для того, чтобы уберечься от возможного съёма информации, необходимо брать другой тип дисплея (например, жидкокристальный) или экранировать комнату.

Мощная офисная аппаратура обладает сильным электромагнитным излучением. Если в помещении установлена радиозакладка, то это излучение способно воздействовать на чувствительный усилитель радиозакладки даже помимо микрофона (рис. 8.2). На вход такого усилителя сигнал может подаваться за счёт паразитных связей через паразитные сопротивления, ёмкость или индуктивность; усиленный сигнал модулирует напряжение генератора Г и через антенну передаётся в эфир.



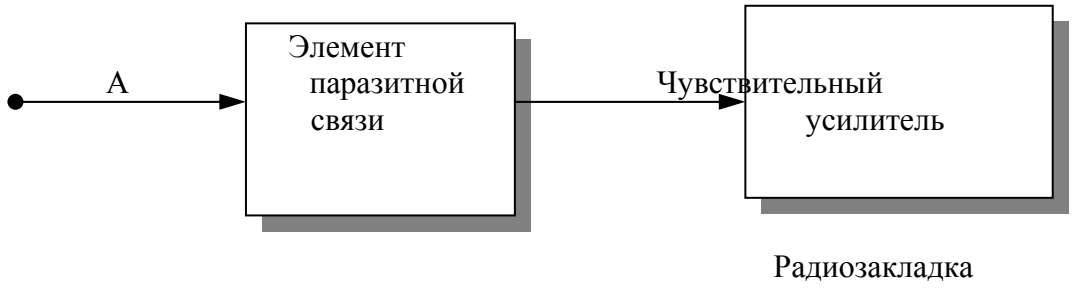


Рис. 8.2

8.2.2. Утечка информации от вспомогательной аппаратуры и кабелей, проходящих через помещение

Часто в одном здании находится достаточно большое количество фирм. Так как здание старое, то в помещениях давно проложено общее питание и жгуты кабелей, не имеющих отношения к работе фирмы.

И общее питание и ненужные кабели могут оказаться причиной утечки информации. Рассмотрим это на конкретных примерах.

Пример 1.

Допустим оборудование запитывается от сети 27 В, проложенное по корпусу здания, и к этой цепи имеет доступ "агент". Если аппаратура на объекте потребляет значительный ток I (рис. 8.3.), то этот ток на сопротивлении проходящих проводов (пусть эквивалентное сопротивление одного участка равно r) создает падение напряжения $U = I \cdot r$. Так как ток потребления в зависимости от величины сигнала меняется, то с чувствительного усилителя, подключенного к одному из проводов цепи питания можно снять информацию.

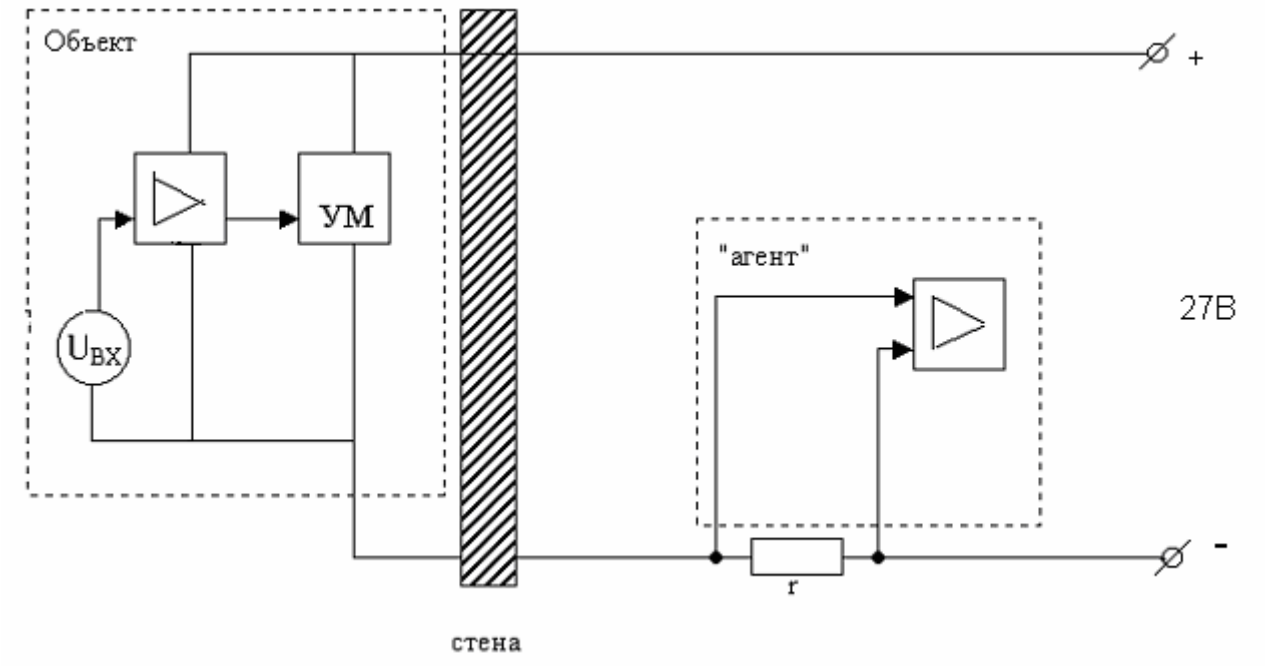


Рис. 8.3

Пример 2.

Пусть источник информации (А) находится в экранированном помещении и через это помещение проходит провод, не имеющий никакого отношения к фирме (рис. 8.4).

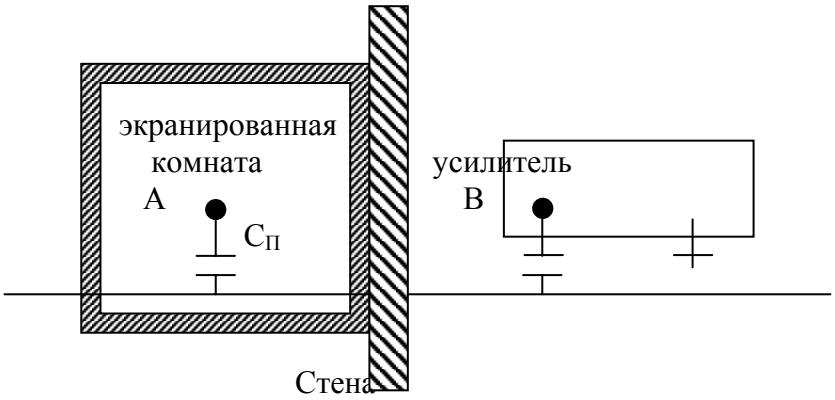


Рис. 8.4

Сигнал из точки (А) через паразитную емкость $C_П$ и конденсатор, подключенный к этому проводу (вне помещения фирмы) поступает на усилитель "агента". Таким образом, даже экранирование комнаты не привело к защите информации.

Возможен так же перехват информации по наводкам, возникающим в совместно проложенных кабелях за счет индуктивной или емкостной связей. Например, пусть по проводам 1, 2 (рис. 8.5.) передается информация с объекта. На проводе 3, лежащем в общем с ним жгуте, за счет индуктивной паразитной связи с проводом 2 наводится сигнал, несущий интересующую информацию.

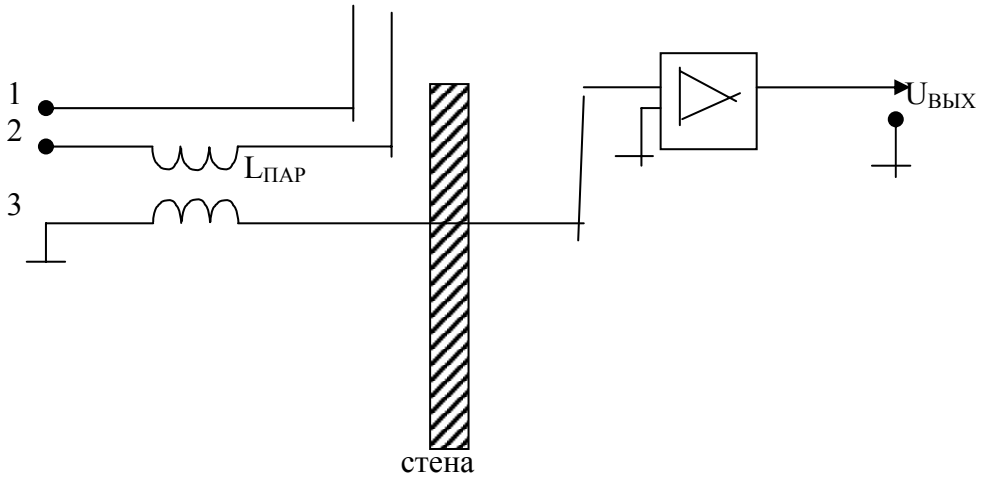


Рис. 8.5

Сигнал снимается с провода 3, усиливается чувствительным усилителем и агент снимает информацию.

8.3. Прослушивание информации от внедрённых радиозакладок

В настоящее время около 61% информации [3], добываемой в бизнесе негласными методами приходится на радиомикрофоны (радиозакладки - РЗ, т. н. «жучки»). Структурная схема несанкционированного съема информации с помощью радиозакладки приводится на рис. 8.6. Радиозакладка состоит из задающего генератора (ЗГ), микрофона (МК), источника питания (ИП), антенны (А).

Акустическая информация, перехваченная с помощью микрофона, преобразуется в электрический сигнал, который модулирует колебания задающего генератора (чаще всего, по амплитуде или частоте) и через передающую антенну излучается в эфир (также возможна передача в телефонную сеть или силовую сеть 220 В). Агент настраивает приемник на частоту передатчика и получает информацию.

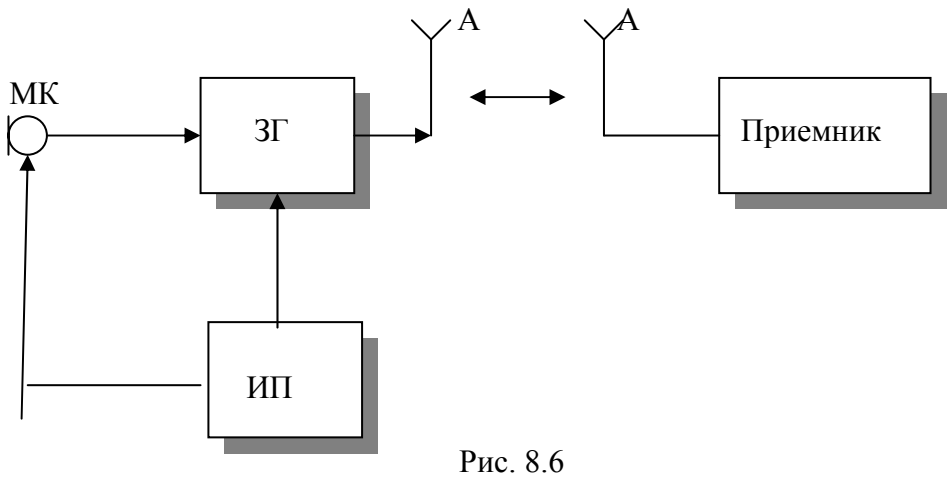


Рис. 8.6

Достоинством радиозакладок является быстрота их установки и малые габариты. Кроме того, беспроводная связь позволяет "агенту" находиться вне здания, что так же повышает вероятность безопасного съема информации.

Для обеспечения скрытности и долговечности работы, радиозакладки должны иметь минимальные габариты и вес, обладать минимальным потреблением энергии, работать в диапазоне частот не прослушиваемом обычным приемником. Обобщенные данные по радиозакладкам, применяемым в России [13] в настоящее время следующие:

Диапазон частот 27 –1300 МГц;
Мощность 0,2 – 500 мВт;
Ток потребления 0,5 – 100 мА;
Вид модуляции (в основном)- широкополосная частотная модуляция
Дальность действия 10 – 1500 м (в основном, 10 –100 м)
Вид стабилизации частоты:с кварцевой стабилизацией, без кварцевой стабилизации;
Период активного существования 4 часа – 20 лет.

Далее в тексте лекций будут рассмотрены некоторые разновидности радиозакладок.

8.3.1. Основные характеристики радиозакладок

Основными характеристиками радиозакладок являются:

- габариты и вес;
- срок службы;
- скрытность работы;
- акустическая чувствительность и дальность передачи;

Габариты и вес

Для государственных служб выпускаются радиозакладки очень малых размеров, но стоимость их баснословно велика. Приведем пример: имеется краткое сообщение о радиомикрофоне с размерами 1,5х1,5 мм и питанием от изотопного элемента. Радиомикрофон способен в течении года передавать информацию на расстояние до 1,5 км

из помещения, где разговор ведется шёпотом. Приведем еще пример: по данным [1] радиозакладка была установлена в пломбу зуба главного бухгалтера фирмы "Нагол-Виннер", что позволило заинтересованной организации осуществлять перехват информации о финансовом состоянии фирмы. В здании посольства США в Москве элементы радиозакладок были рассредоточены по бетонным блокам, представляя собой кремниевые вкрапления. Арматура использовалась в качестве проводников, а пустоты – в качестве резонаторов и антенн.

Радиозакладки обычно малогабаритны и камуфлируются под микро булавки, часы, калькуляторы, авторучки, пачки сигарет и т.д. Благодаря малым размерам радиозакладка может быть быстро и надежно спрятана. Существуют сведения о радиозакладке SIPE-PS, устанавливаемой прицельным выстрелом в форточку на расстоянии 25 м. Данная закладка обеспечивает дальность передачи 50 м [1]. Радиозакладки в виде часов, авторучки и т. п. могут быть внедрены в виде подарка доверчивому служащему фирмы. Коммерческие радиозакладки имеют большие габариты и вес, но соответственно меньшую стоимость. По мере развития техники их размеры уменьшаются. В настоящее время средние параметры коммерческих закладок [7] составляют: объем – (1 см^3- 8дм^3),
вес – (5 – 350) г.

Срок службы

Срок службы радиозакладки в основном определяется применяемым источником питания. Рассмотрим основные виды источников питания:

1. Автономное питание;
2. Питание от устройств, в которых замаскирована радиозакладка;
3. Питание от электросети;
4. Питание от телефонной сети.

1) *При автономном питании* радиозакладку не надо никуда подключать,
то есть время установки и риск её установки минимален. При необходимости большого срока действия, естественно, возникает необходимость смены источника питания, что, соответственно, вызывает существенные трудности и повышает риск обнаружения. Поэтому при первой же установке обычно пытаются поставить батарею максимальной емкости, установив её, естественно, совместно с закладкой, в емкие предметы. Например, в макеты кораблей, цветочные горшки и т.д. Характерным представителем таких РЗ являются устройства производства России ЛСТ-1, ЛСТ-2.

Для увеличения срока службы закладки в качестве автономного источника питания используют солнечные батареи, камуфлируемые вместе с закладкой под питьевые стаканы и т.д. Этот принцип питания используется в устройстве SIPE MT, где элементы солнечной батареи расположены на дне стакана в виде оригинального орнамента. Дальность действия передатчика
в диапазоне 130 -150 МГц составляет 100 м [13]. Пока подобные устройства не нашли широкого применения из-за невозможности работы в условиях слабой освещённости.

Сэкономить ресурс батареи и повысить скрытность передачи позволяет использование дистанционного включения. Например, устройство TRM-1530
с питанием от 3-х литиевых батареек работает в диапазоне 100 – 150 МГц, имеет

время непрерывной работы 300 часов, а с учетом периодического включения до 1 года [13]. Габариты устройства 87х54х70мм, дальность действия 150 м.
Экономия ресурса батареи возможна и при автоматическом включении закладки при наличии звука и соответственном её выключении через несколько секунд после его исчезновения. На принципе включения закладки от звука работает устройство STG-4001, имеющее следующие параметры: габариты 20х38х12 мм^3, вес с батареей 18 грамм, несущая частота 130 – 150 МГц, дальность связи 500 метров [13].

Следующей возможностью экономии ресурса батареи является уменьшение мощности передатчика, что одновременно повышает скрытность его работы. При уменьшении мощности передатчика соответственно уменьшается дальность его работы. Для обеспечения приёма устанавливается дополнительный ретранслятор вне объекта в соседней комнате, автомобиле и т.д. Габариты и питание ретранслятора не лимитированы, и он обеспечивает дальнейшую передачу на требуемое расстояние. Примером закладки работающей на ретранслятор может служить устройство ЛСТ-2-РБ с питанием от изотопного элемента со сроком работы более 10 (габариты устройства – размер батареи «Крона» [7].
2) Питание радиозакладок от устройств, внутрь которых они вмонтированы значительно увеличивает срок их действия. Примером такого устройства является ЛСТ-3, встроенный в калькулятор. Размеры самой закладки 12х6х3 мм, чувствительность микрофона 10 м, дальность передачи 150 метров в диапазоне частот 112-135 МГц. При старении батареи само устройство (например, калькулятор) перестает работать, и в нём неподозревающие сотрудники сами меняют батарейку.

3) Питание РЗ от сети 220 В делает практически не ограниченным их срок действия. В качестве примера можно привести РЗ типа CAL-201, CAL-205. Закладка ЛСТ-4 устанавливается в электророзетках, настольных лампах и других электроприборах, закладка HR 560 LIGHT WULD устанавливается в цоколь лампы накаливания, имеет дальность передачи 250 м. Недостатком такого вида закладок является необходимость проведения определенного вида работ на объекте. Например, для установки закладки, вмонтированной в розетку, агенту ЦРУ потребовалось два месяца, с учетом внедрения агента (ночного стража) и точной подгонки розетки по цвету, трещинам и т.д. на соответствие ранее имевшейся [7, 13].

4) Питание РЗ от телефонной сети также обеспечивает неограниченный срок их службы. Примерами таких закладок являются изделия ЛСТ-3Т5, ЛСТ-54, AD-453. Закладка AD-453 имеет дальность действия 150 м, размеры 22х16х22мм^3, вес 210 грамм. Как и в варианте с сетью 220 В возникают трудности с их установкой.

Скрытность работы

Скрытность работы обеспечивается:

а) выбором частотного диапазона;
б) накоплением информации с последующей ее передачей в режиме быстродействия;
в) малой выходной мощностью передатчика.

Частотный диапазон: Простейшие РЗ работают на частотах FM - вещания, они составляют 30% всего парка РЗ. Более профессиональные РЗ работают в диапазоне между вещательным FM - диапазоном и 6 – м каналом TV - вещания.

Этот класс РЗ составляет в России 50 %. Загрузка метрового диапазона мобильными радиостанциями вынуждает использовать для РЗ следующий диапазон (дециметровый) между 12 и 21 каналами TV. Этот парк составляет оставшиеся 20% парка РЗ. РЗ указанного диапазона трудно обнаружить, они дороги, их используют профессионалы. Для повышения скрытности работы профессионалы начали использовать инфракрасный канал. РЗ типа TRM - 1830 имеет дальность передач днем-150 м, ночью – 400 м. К недостаткам такого вида передачи следует отнести необходимость прямой видимости между закладкой и приёмником,
а также сильное влияние фоновой засветки.

Накопление информации с последующей ее передачей в режиме быстродействия позволяет повысить скрытность работы передатчика, так как выход в эфир становится кратковременным.

Малая выходная мощность РЗ усложняет ее обнаружение из-за малого уровня сигнала от РЗ на фоне мощных помех от работающих радиостанций, от включения и выключения промышленных установок, помех от проезжающих трамваев и т. п.

Акустическая чувствительность и дальность передачи

РЗ характеризуются акустической чувствительностью – способностью воспринимать звук с разных расстояний. Хорошей чувствительностью считается способность воспринимать звук на расстоянии 5-12 м в тихом помещении при прямом поступлении звука. Установка РЗ в шкафы, столы и т.д. уменьшает акустическую чувствительность.

Дальность передачи, с точки зрения безопасности наблюдения, требуется как можно больше, а с точки зрения скрытности работы РЗ и ресурса его работы – как можно меньше. Диапазон компромиссных решений составляет – от десятков до сотен метров.

8.3.2. Основные элементы радиозакладки

Радиозакладка состоит из микрофона МК, усилителя низкой частоты УНЧ, генератора, совмещенного с модулятором, и источника питания. Остановимся более подробно на принципах работы генератора и некоторых видах модуляции, так как виды микрофонов рассмотрены
в п. 6.1, а усилители низкой частоты и источники питания изучались в курсе «Электроника и схемотехника».

В РЗ используются автогенераторы, то есть устройства, формирующие сигнал требуемой амплитуды и частоты. Структурная схема автогенератора приведена на рис. 8.7а.

Автогенератор состоит из усилителя У, частотно-зависимого звена ЧЗ и цепи обратной связи с коэффициентом преобразования β. Усилитель и частотнозависимое звено образуют прямую цепь передачи с коэффициентом К. Значение К равно произведению коэффициентов преобразования усилителя и ЧЗ. Частотные характеристики прямой цепи определяются ЧЗ, который чаще всего представляет собой параллельный LC контур с характеристикой, приведенной на рис. 8.7б. На резонансной
частоте выходное напряжение, снимаемое с контура, максимально. На этой

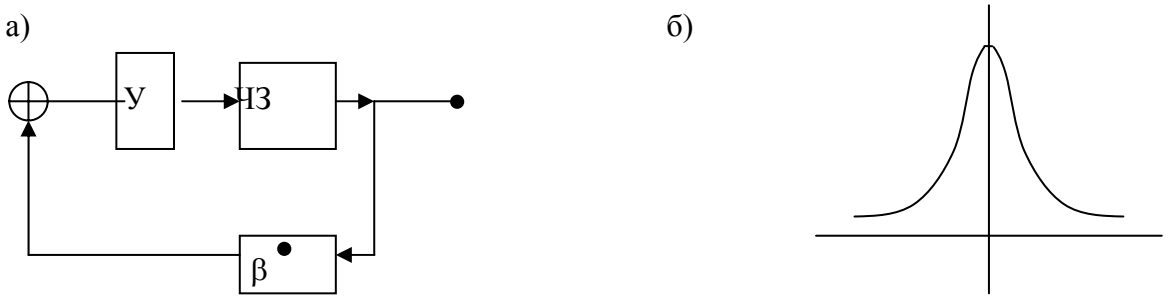


Рис. 8.7

частоте контур имеет максимальное активное эквивалентное сопротивление $R_Э$ и угол фазового сдвига $\varphi_{конт}$ = 0. Добротность Q и эквивалентное сопротивление $R_Э$ контура может быть определено по следующим формулам.

$$Q = \frac{f_0}{\Delta F} = \frac{\omega_0 L}{r} = \frac{1}{\omega_0 c \cdot r}$$

$$R_Э = Q^2 \cdot r = \frac{L/c}{r}$$

где ΔF - полоса пропускания; ω_0 - круговая резонансная частота; L, C, r – индуктивность, емкость и сопротивление потерь контура.

Условия возникновения генерации описываются следующим выражением [14]

$$\begin{cases} K\beta \geq 1 & (1) \\ \varphi + \psi = 2\pi n & (2) \end{cases}, \text{ где}$$

φ - фазовый сдвиг прямой цепи, ψ - фазовый сдвиг обратной цепи,

n – целое число.

Первое условие – условие баланса амплитуд. Для возникновения колебаний петлевое усиление (произведение коэффициента преобразования прямой цепи на коэффициент преобразования цепи обратной связи) должно быть больше или равно единице. При больших Kβ колебания должны быть прямоугольными, но в связи с высокой добротностью контур выделяет только определенную гармонику (на которую он настроен), поэтому снимаемый с контура сигнал будет синусоидальным. Это свойство используется в кварцевых генераторах,

в которых частота кварца берется в n раз меньше частоты контура генератора (более подробно смотри пояснения к рис.8.8). Если Kβ<1, то при включении возможен первоначальный всплеск колебаний с последующим их затуханием по экспоненциальному закону.

Второе уравнение – условие баланса фаз, колебания возникшие в какой-нибудь точке схемы должны возвратиться в эту точку с нулевым фазовым сдвигом. Напомним, что если сигнал подается в базу, а снимается с коллектора, то фазовый сдвиг усилителя $\varphi_{усил}$=180°; если сигнал подается в базу, а снимается с эмиттера то $\varphi_{усил}$=0°; если сигнал подается в эмиттер, а снимается с коллектора, то φ=0°. Фазовый сдвиг прямой цепи на резонансной частоте равен $\varphi = \varphi_{УСИЛ} + \varphi_{ЧЗ} = \varphi_{УСИЛ}$, так как $\varphi_{ЧЗ}$=0,

где $\varphi_{ЧЗ}$ – угол фазового сдвига ЧЗ на резонансной частоте.

Таким образом, можно констатировать, что если устройство охвачено обратной связью и для этого устройства выполняются условия (1) и (2), то такое устройство является автогенератором. Существует большое количество схем автогенераторов.

Наибольшее распространение получили устройства, собранные по схемам “емкостной трёхточки” и “индуктивной трёхточки”. Поясним понятие “трёхточка”. Транзистор имеет три электрода; если все три электрода подключены к емкостям контура, то такая схема называется емкостная трёхточка. Напоминаем, что плюс источника питания по переменному току находится на корпусе устройства. Аналогично емкостной трехточке (рис.8.8а) у схемы с индуктивной трехточкой все три вывода транзистора подключены уже не к емкостям, а к трем выводам индуктивности контура (рис.8.8б).

Докажем, что устройство, собранное по схеме рис. 8.8а, является емкостной трёхточкой. В схеме рис. 8.8а коллектор VT подключен к емкости контура C_3, эмиттер VT подключен к точке соединения C_2 и C_3, база VT через конденсатор C_1 большой ёмкости находится на корпусе по переменному току. Плюс источника питания по переменному току так же находится на корпусе; следовательно, база транзистора по переменному току подключена к верхнему выводу конденсатора C_2.
Таким образом, все три вывода транзистора подключены к емкостям контура, значит устройство собрано по схеме емкостной трёхточки. Докажем, что устройство, собранное по схеме рис. 8.8б является индуктивной трехточкой. Исток транзистора подключён к точке соединения индуктивностей L_1 и L_2 ; затвор подключен к верхнему выводу индуктивности L_1 ; сток по переменному току через источник +E и корпус подключен к нижнему выводу L_2. Таким образом все три вывода подключены к индуктивностям контура, значит устройство собрано по схеме индуктивной трёхточки. Схемы автогенераторов бывают
со стабилизацией частоты и без стабилизации частоты. Схемы без

а) б)

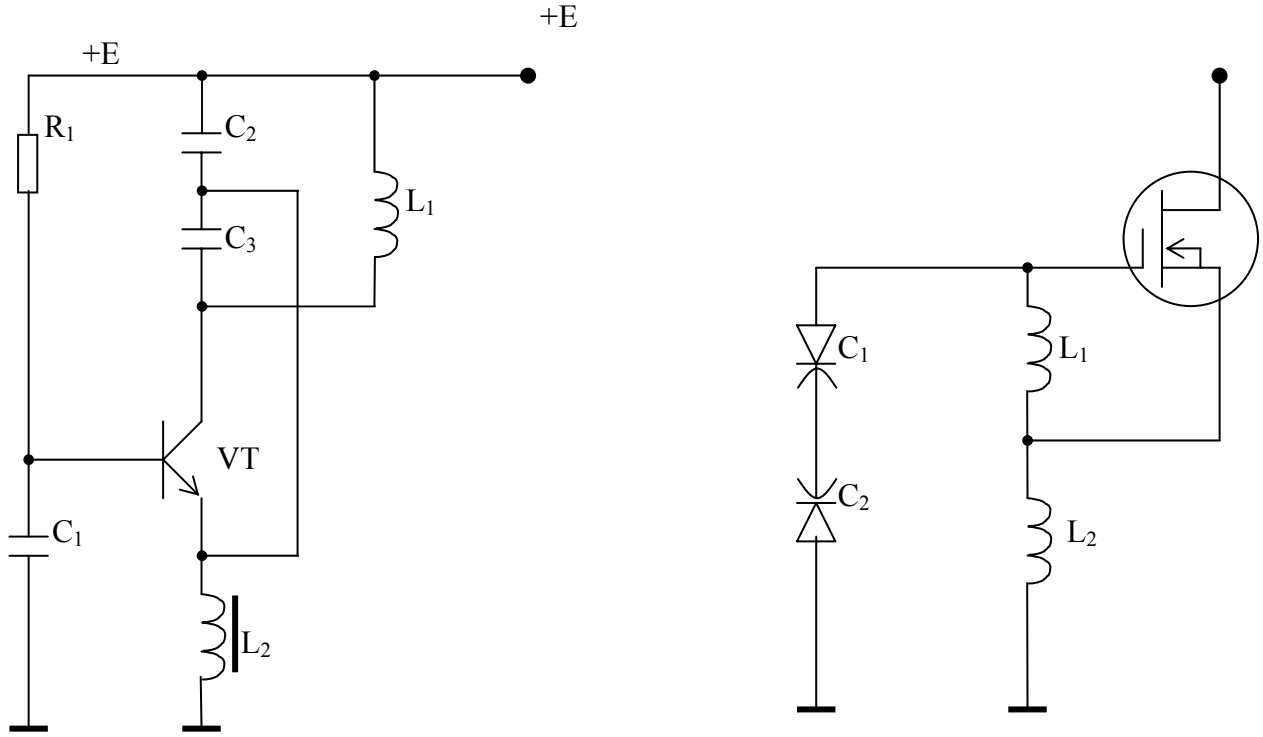


Рис. 8.8

стабилизации частоты (рис. 8.8) более просты и дешевы, но излучаемая частота не стабильна и приходится принять более дорогие приёмники с настройкой частоты.

Причиной изменения частоты может быть: изменение напряжения питания, изменение климатических условий, изменение паразитных емкостей и индуктивностей (например, если передатчик установлен на перемещающемся объекте).

Схемы со стабилизацией частоты (кварцевая стабилизация) несколько дороже, зато их частоты стабильны (рис. 8.9).

Усилитель генератора собран на транзисторе VT, коэффициент усиления К определяется отношением эквивалентного сопротивления контура генератора $R_э$ на частоте ω_0 к значению сопротивления $\left(R_E + \frac{1}{S}\right)$

$$k = \frac{R_Э}{R_E + \frac{1}{S}}$$, где

$S = \frac{I}{26mB}$ - крутизна транзистора, I – ток покоя транзистора.

Резонансная частота кварца f_{KB} берется равной или в n раз меньше резонансной частоты контура ($f_{KB} = f_0$;
f_0 /n). На резонансной частоте и на частоте гармоник эквивалентное сопротивление кварца близко к нулю и сигнал с части контура поступает в эмиттер транзистора, образуя цепь положительной обратной связи. Значение β в данном случае не равно 1, а определяется в основном соотношением емкостей C_1 и C_2.

При $\beta k \geq 1$ в контуре генератора возникают колебания.
Для подстройки частоты кварца в небольшом диапазоне частот используется конденсатор C_3. В связи с высокой добротностью кварца положительная обратная связь возникает только на частотах f_{KB} и nf_{KB}, поэтому частота генератора стабильна.
Для модуляции сигнала генератора используется микрофон.

Электрический сигнал с микрофона модулирует сигнал генератора чаще всего или по частоте или по амплитуде. Рассмотрим принцип частотной модуляции. Если в контур генератора (рис. 8.10а) установить варикапы C_B и подать на них напряжение смещения E_0 и модулирующее напряжение $U_{Нч}(t) = U_C \sin \Omega t$ от микрофона, то емкость варикапов C_B будет меняться (рис. 8.10б) и, соответственно будет меняться частота генератора ω:

$$\omega \approx \frac{1}{\sqrt{L \cdot \frac{C_B}{2}}}$$

т.е. сигнал с микрофона будет модулировать частоту генератора.

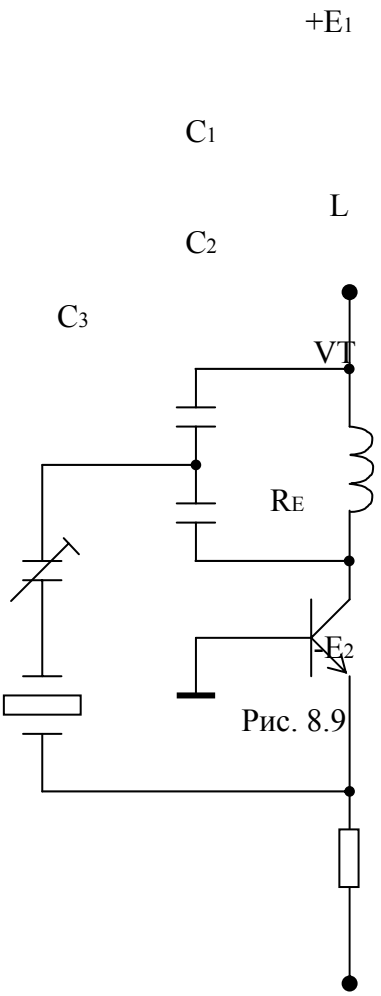


Рис. 8.9

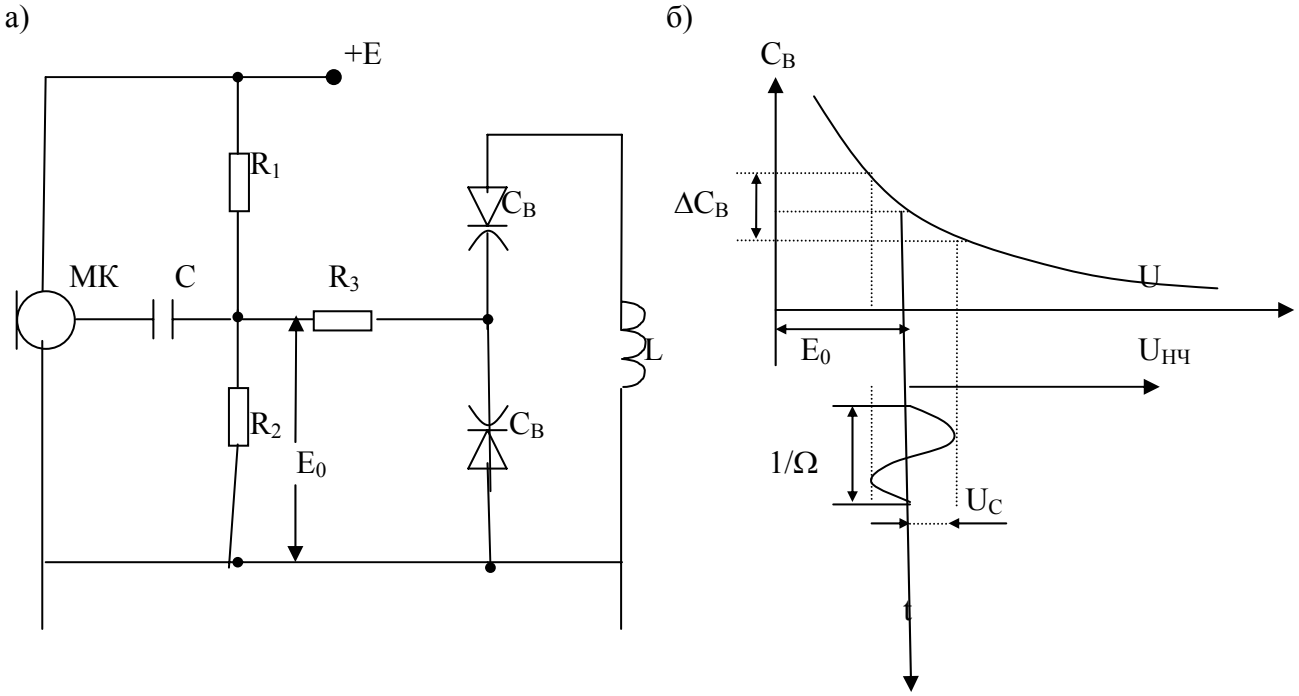


Рис. 8.10

При начальном угле фазового сдвига равном нулю сигнал, снимаемый с контура генератора, определяется выражением [14]:

$$U = U_0 \sin(\omega_0 t + \beta \sin \Omega t),$$

где U_0 – амплитуда высокочастотных колебаний;
ω - круговая резонансная частота генератора при отсутствии модуляции; $\beta = \Delta\omega / \Omega$ - индекс модуляции;
$\Delta\omega$ - изменение частоты генератора.

Данное выражение справедливо также и для фазовой модуляции; отличие заключается в разной зависимости β от модулирующего сигнала. При фазовой модуляции $\beta = kU_C$,

где U_C - амплитуда модулирующего сигнала;

k - коэффициент пропорциональности.

При амплитудной модуляции амплитуда напряжения высокой частоты U_0 меняется по закону модулирующего сигнала. Модулирующий низкочастотный сигнал представляет собой сумму синусоидальных колебаний различных частот.

Рассмотрим для простоты, что низкочастотные колебания представлены колебанием только одной низкой частоты Ω с амплитудой U_C:

$$U_{НЧ}(t) = U_C \sin \Omega t$$

Выражение для амплитудно-модулированного сигнала имеет вид:

$$U(t) = U_0 \sin \omega t + U_C \sin \Omega t \cdot \sin \omega t =$$

$$= (U_0 + U_C \sin \Omega t) \sin \omega t = U_0 \left(1 + \frac{U_C}{U_0} \sin \Omega t \right) \sin \omega t =$$

$$= U_0 (1 + m \cdot \sin \Omega t) \sin \omega t =$$

$$= U_0 \sin\omega_0 t + \frac{1}{2} m U_0 \cos(\omega_0 - \Omega)t - \frac{1}{2} m U_0 \cos(\omega_0 + \Omega)t$$

где $m = \dfrac{U_C}{U_0}$ - коэффициент модуляции.

На рис. 8.11 приведена графическая иллюстрация этой формулы, причем на левой части рисунка изображено немодулированное колебание, а на правой – модулированное. Модулированное колебание, как видно из формулы и рис. 8.11 не является чисто синусоидальным, а содержит комбинацию частот ω_0, $\omega_0 - \Omega$, $\omega_0 + \Omega$; т.е. для получения модулированных сигналов необходимо иметь устройство, которое меняет спектр частот.

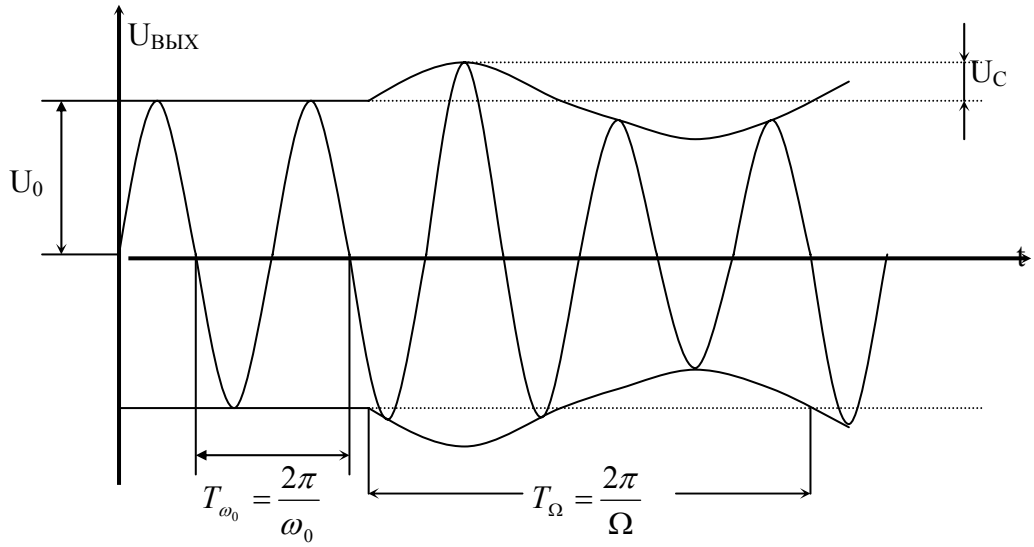


Рис. 8.11

Обеспечение изменения спектра сигнала возможно только при применении нелинейных элементов. В качестве такого нелинейного элемента можно использовать транзистор генератора, например, нелинейность зависимости крутизны S (а, следовательно, коэффициента усиления от амплитуды входных сигналов). Поясним вышесказанное с помощью рис 8.12.

Если сумма сигналов $U_{ВЧ}$ и $U_{НЧ}$ (рис.8.12,а) подается при смещении E_0 на нелинейный элемент с характеристикой рис.8.12,а, то на выходе в точках а, б, в получаем высокочастотный сигнал разной амплитуды, так как низкочастотный сигнал перемещает точку приложения высокочастотного сигнала; а в разных точках крутизна преобразования нелинейного элемента разная. Результирующий сигнал представлен на рис.8.12,в.

В радиозакладках чаще применяют частотную модуляцию, чем амплитудную. Это объясняется тем, что при одинаковых условиях применения отношение сигнал/шум устройств с частотной модуляцией в $\frac{(3 \div 4) \cdot \Delta\omega}{\Omega_{max}}$ раз больше отношения $U_C / U_Ш$ устройств с амплитудной модуляцией [14]. В последнее время применяют также и другие виды модуляции.

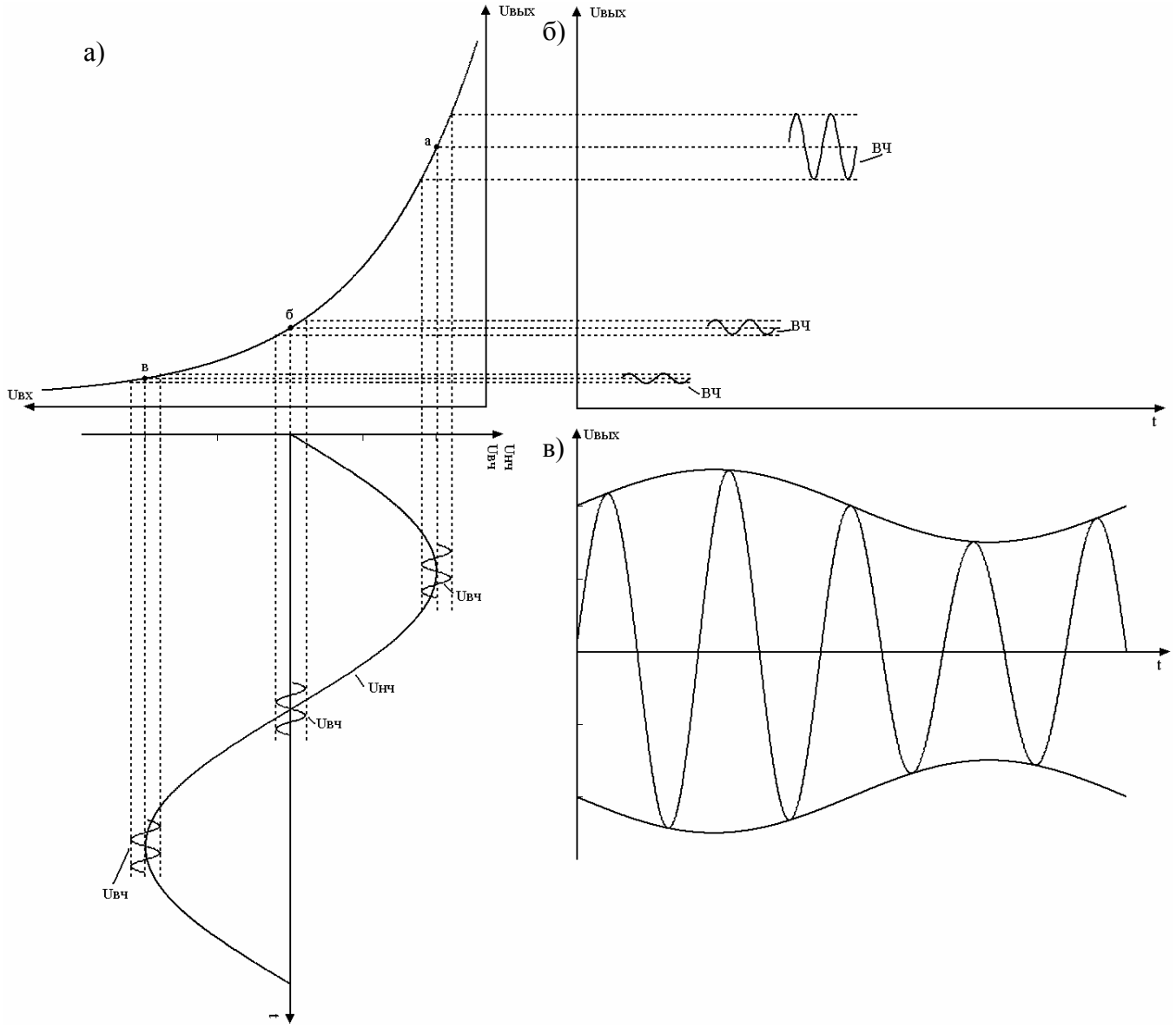


Рис. 8.12

8.3.3. Примеры схем радиозакладок

Схема маломощного передатчика с частотной модуляцией и автономным источником питания представлена на рис. 8.13 [13].

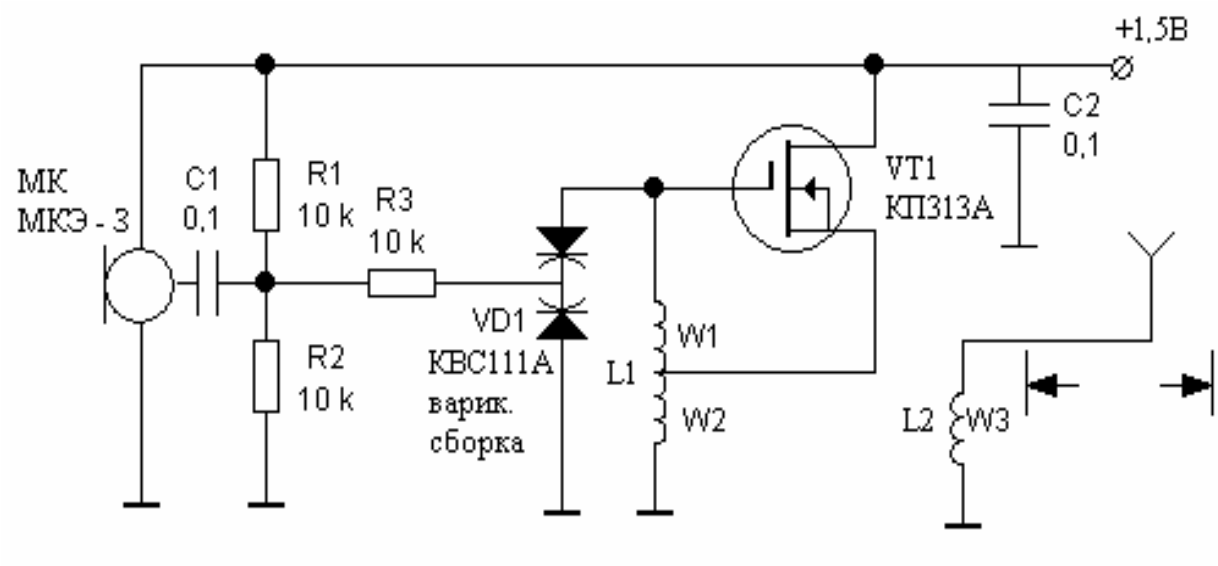


Рис. 8.13

Примечание: Длина антены l = 0.8 м, скручена в спираль.

Питание микрофона МК и генератора высокой частоты, выполненного на транзисторе VT1, осуществляется от батареи 1.5 В. Генератор выполнен по схеме индуктивной трёхточки. Положительная обратная связь обеспечивается за счет автотрансформаторного подключения индуктивности L1 между затвором и истоком транзистора. Так как фазы высокочастотных сигналов в затворе и истоке транзистора VT1 совпадают, и в затвор подается сигнал в $(W_2+W_1)/W_2$ больше, чем напряжение на эмиттере, то $\beta \cdot k \geq 1$; следовательно, устройство на основе транзистора VT1 является генератором. Частота генератора определяется частотозадающим контуром, состоящим из L1 и варикапной сборки КВС111А. Предварительное смещение на варикап задается делителем R1, R2. Электрический сигнал микрофона изменяет емкость варикапа и обеспечивает частотную модуляцию сигнала. Приведем недостающие технические данные: катушка L1 имеет внутренний диаметр 4 мм, W_1=4, W_2=3, W_3=1; катушка L2 выполнена соосно с L1 ближе к земляному выводу; ток транзистора при закороченной L1 $\geq(1\div5)\mu$А.

Передатчик обеспечивает выходную мощность 0.5 мВт, ток потребления $\leq 2\mu$А; частота генератора 80÷100 МГц, дальность передачи
не указывается, вероятно, 10÷20 метров.

Схема мощного передатчика с автономным питанием приведена
на рис 8.14 [13]. Питание передатчика осуществляется от источника +9 В. Для развязки по цепи питания низкочастотной и высокочастотной части передатчика используется конденсатор С6 и RC-фильтр R8, С2. В режиме покоя ток через микрофон МК задается резистором R1.

Сигнал с микрофона через конденсатор С1 поступает на усилитель низкой частоты, выполненный на транзисторах VT1 и VT2. Рабочая точка каскада устанавливается резисторами R4, R5, R6; через резистор R5 обеспечивается отрицательная обратная связь. Конденсатор С3 шунтирует резистор R6, что приводит к увеличению коэффициента усиления каскада на переменном токе, выполненного на транзисторе VT2. Полезный сигнал с коллектора VT2 через RC цепочку R9, С4, R10 поступает на варикап VD1,

изменяя его емкость. Генератор высокой частоты собран по схеме емкостной трёхточки. Положительная обратная связь (ПОС) осуществляется за счет подключения общей точки соединения конденсаторов С8 и С9 к эмиттеру транзистора VT3 и базы VT3 – к корпусу устройства. Дроссель Др1 обеспечивает большое эквивалентное сопротивление на переменном высокочастотном токе, т.е. большую глубину ПОС при условии малого сопротивления на постоянном токе. Режим по постоянному току выставляется резистором R11. Частота генератора определяется задающим контуром, состоящим из индуктивности L1 и конденсаторов С8, С9.

Варикап VD1 через конденсатор С5 подключен параллельно конденсатору С8, так как источник питания +9 В имеет малое сопротивление по переменному току. Следовательно, частота генератора зависит от значения емкости варикапа. Таким образом, сигнал с микрофона после усиления каскадами УНЧ изменяет емкость варикапа, что приводит к частотной модуляции частоты высокочастотного генератора. Сигнал с контура генератора через конденсатор С10 передается на антенну и излучается в эфир. Приведем технические данные: бескаркасная катушка L1 имеет диаметр 8 мм, число витков – 7, намотана проводом ПЭВ с диаметром

0.8 мм. Антенна выполнена в виде катушки диаметром 3 см, диной 50 см, намотанной виток к витку тем же проводом. Дроссель Др1 – типа ДПМ-01 60 мкГн (при отсутствии дросселя можно на сопротивлении 100 кОм 0.25 Вт намотать катушку проводом ПЭВ 0.1 с W=100).

Передатчик имеет выходную мощность 200 мВт, частотный диапазон 65÷108 МГц, дальность действия 100 метров – при использовании в качестве антенны катушки, и 600 метров – при использовании штырьковой антенны длиной 1 м. Срок действия передатчика ограничен емкостью батареи.

8.4. Прослушивание информации от пассивных закладок

Полуактивный радиомикрофон интересен тем, что в нём нет ни источника питания, ни передатчика, ни микрофона. Радиозакладка работает на принципе высокочастотного навязывания [5]. Суть способа заключается в высокочастотном зондировании помещения, в котором происходят переговоры. В результате взаимодействия ВЧ луча с элементами обстановки или специально внедренными устройствами происходит модуляция зондирующих лучей речевыми сигналами. Первый полуактивный микрофон был разработан в 1940 г. Структурная схема устройства приведена на рис. 8.15.

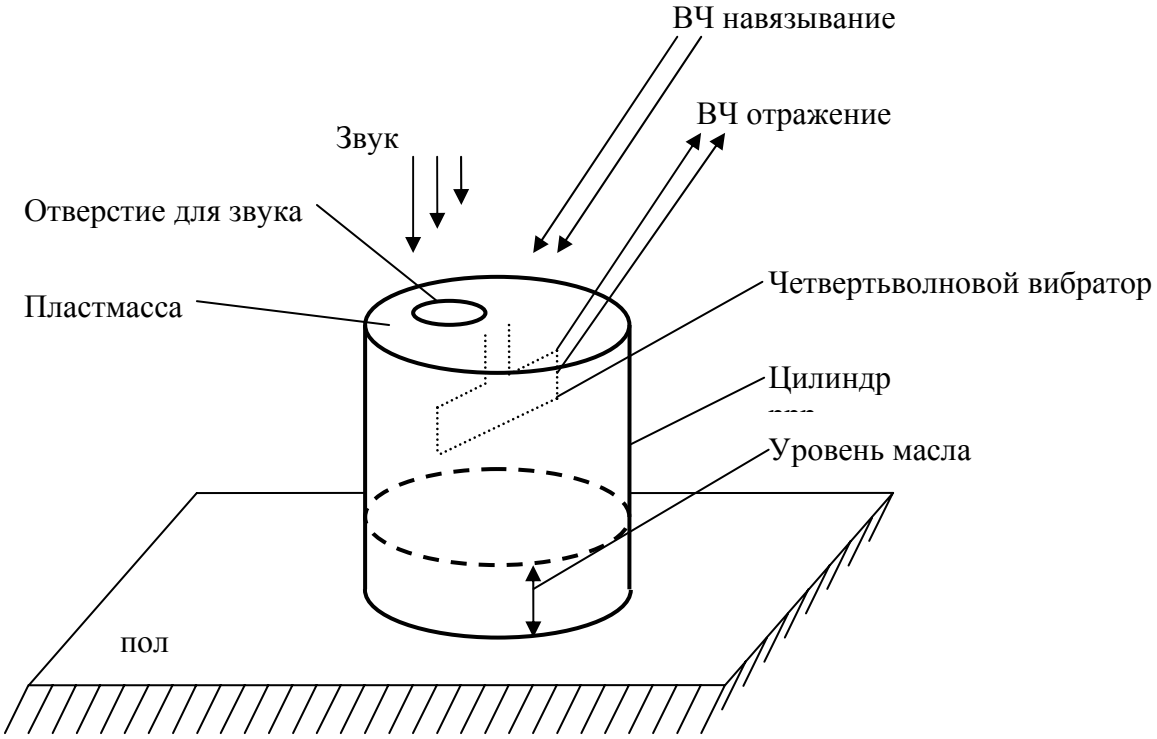


Рис. 8.15

Цилиндр, в который залит определенный уровень масла, благодаря своим размерам и уровню масла, становится резонатором на частоте f=330 МГц. Для приёма и излучения высокочастотных колебаний внутрь цилиндра установлен волновой вибратор с длиной волны $l=\lambda/4$, то есть
с согласованной антенной. ВЧ сигнал поступает и излучается через прозрачную для него пластмассовую крышку. Для поступления звука внутрь резонатора в пластмассовой крышке сделано отверстие.

При проведении разговоров вблизи резонаторов звук через отверстие поступает в цилиндр. На поверхности масла появляются микроколебания, вызывающие изменение добротности и резонансной частоты резонатора (рис 8.16). Например, при отсутствии звука резонатор имеет резонансную частоту $f_{рез}$, а при поступлении $U_{звука}$ его резонансная частота колеблется от $f_{рез}''$ до $f_{рез}'$. При этом происходит модуляция по фазе и амплитуде высокочастотного сигнала переотражённого вибратором. Модуляция несет речевую информацию.

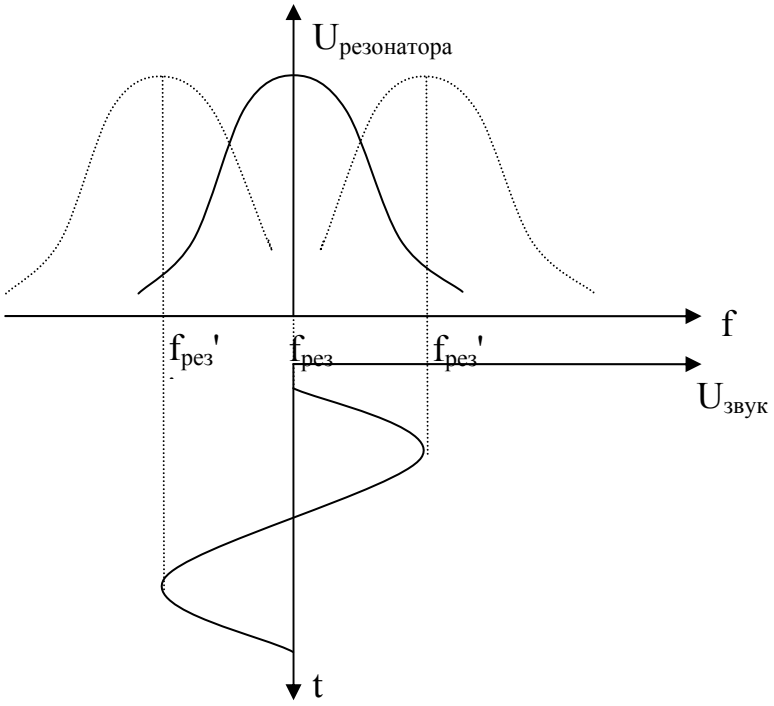


Рис. 8.16

Достоинством полуактивного радиомикрофона является его скрытность, обусловленная тем, что сам он ничего не излучает.
Недостатки – необходимость больших мощностей передатчика (так как КПД отражения мал) и высокая вредность излучения. Использование этих систем весьма вредно как для здоровья тех, кого подслушивают, так и тех, кто подслушивает. Так, например, специалисты ЦРУ вынуждены были надевать специальные фартуки, когда облучали советские учреждения.

Впервые информация об использовании подобной системы были обнародованы представительством ООН в Москве после обнаружения закладки в гербе посольства США в Москве. В последующие годы стали применяться более высокие частоты зондирования, что позволило снизить размеры резонатора до размеров блесны.

Принцип полуактивного радиомикрофона используется в современной системе **SIPE MMI**. Дальность ее действия 100 м, пассивная закладка выполнена в виде специального стержня длиной 30 см
и диаметром 2.5 см. Закладки данного типа применяются только спецслужбами [15].

8.5. Приемники информации с радиозакладок

Для приема информации с радиозакладок используют:

- *обычные приемники и магнитолы.* Их достоинством является низкая стоимость и возможность использования по прямому назначению. Недостаток – низкая

чувствительность и ограниченный частотный диапазон, у отечественных устройств диапазон частот 63÷74 МГц,
у импортных – 88÷108 МГц;

- *обычные приемники и магнитолы с дополнительной перестройкой контуров или применением конверторов.* За счет этих доработок рабочий диапазон частот поднимают до 130 МГц и более;
- *профессиональные приемники.* Радиочастотомеры (например, частотомеры фирмы Optoelectronics, позволяющие практически мгновенно определить частоту сигналов в диапазоне от 1 МГц до 3 ГГц при чувствительности от 0.6 мВ до 60 мВ) и т. д. [8]; сканерные приемники (например, AR-2700, AR-8000 с чувствительностью 1 мкВ при отношении сигнал/шум равном 10; обычно сканерные приемники имеют от 100 до 1000 каналов памяти); анализаторы спектра (например, анализатор спектра 27В4 фирмы “Tektronic” позволяет измерить параметры сигнала в диапазоне частот от 9 кГц до 40 ГГц).

  Более подробные данные о профессиональных приемниках приведены в п 8.7.3;
- *специальные приемные устройства.* Их достоинством является более низкая стоимость, чем широкодиапазонных профессиональных приемников, так как они изготовляются для приема сигналов под определенный диапазон рабочих частот. Примерами специальных приемных устройств могут служить следующие устройства: PK1015-SS; PK830-SS, UXR1, URX3, UXR5, ST6 4401-RX-P2-U[5]. Параметры одного из приемников PK830-SS следующие: габариты 85x54x20мм, вес-275г, помещается в пачке сигарет; диапазон рабочих частот 120-150 МГц; три канала кварцованных частот 139,6 МГц, 139,8 МГц, 140,0 МГц; чувствительность 0,25 мкВ при отношении сигнал/шум на выходе приемника 12дБ; источник питания 9В;
- *специальные комплексы, состоящие из передатчика и приемника,* сделанного именно под данный передатчик. Это изделия нового поколения; радиосигналы передатчика могут быть приняты и декодированы только своим цифровым стереоприемником. На выходе обычного аналогового приемника получится только белый шум без признака информации. Примерами таких комплексов могут служить: SIM-DST-100; SIM-DST-750, SIM-CST-1000/csr-1000 и т.д.

Более сложные и дорогие комплексы передают сигнал от закладки к приемнику под уровнем шумов. Обнаружить подобный сигнал очень сложно. Применяют эти комплексы государственные службы. Примером таких комплексов являются Model SIM-DSS-2000, Model SIM-DSS-5000. Характеристики последнего комплекса приводятся ниже.

Приёмопередатчик SIM-DSS-5000T с псевдослучайной скачкообразной перестройкой несущей частоты (Frequency hopping)
и широкополосными (шумоподобными) сигналами отличается высокой защищенностью информации от перехвата. Он предназначен для использования международными и национальными силами полиции и служб безопасности. Для снижения вероятности перехвата передаваемые сигналы звуковых частот преобразуются в цифровую форму и шифруются ещё до модуляции. Пользователь может в любое время сменить ключ шифра посредством передачи соответствующей команды через блок дистанционного управления. Характеристики передатчика приводятся ниже.

Передатчик

Вид передачи……с псевдослучайной скачкообразной перестройкой несущей частоты

Диапазон частот, МГц…….850-950, 750-850

Количество скачков (изменений)
частоты в 1 с…….500
Ширина полосы скачкообразной
перестройки несущей, МГц…….100
Управление скачкообразной
перестройкой…….случайная
последовательность
импульсов
Выходная мощность, мВт……....300
Регулировка выходной мощности, мВт…..0-3 с шагом 0,3
3-300 с шагом 3
Антенна, Ом ……..входное сопротивление 50,
соединитель SMA
Количество каналов передачи
звуковых частот от микрофонов……..2
Разделение каналов, дБ……..более 70
Динамический диапазон, дБ …….более 70
Ширина полосы звуковых частот ……150 Гц-7 кГц
Полоса звуковых частот голосовой
активации, Гц……..300 - 1200
Скорость передачи команд
дистанционного управления, кбит/с…..…...2,3
Режим передачи команд
дистанционного управления……пакетный
Длительность пакета, мс……..менее 100
Выключение голосовой активацией ……...от 200 мс до 10 с
(регулируется)
Электропитание…….постоянный ток, 6 В
(4,5-6,5 В)
Потребляемый ток, мА……..4-дежурный режим,
100 - 350 – передача
(свыходной мощность 0-99%)
Защита питания ……..от перенапряжений

Проведенные испытания системы показали, что её передачи практически невозможно принимать с помощью обычных радиоприемников. Кроме того, оператор может, пользуясь блоком дистанционного управления, снижать выходную мощность передатчика до минимальной, обеспечивающей требуемую дальность передачи.

Как отмечают авторы работы [5], рассмотренные комплексы надёжно защищены от комплексов контроля радиоизлучений, однако и такие закладки могут быть выявлены при правильном построении системы безопасности предприятия.

8.6. Деконспирационные признаки

Основной вариант установки РЗ - заходовый (только небольшое количество РЗ устанавливается без посещения агентом интересующего его помещения, например, выстрелом из специального ружья).

Радиозакладки имеют свои характерные особенности, позволяющие их идентифицировать как средство несанкционированного съема информации СНСИ:

1. Наличие излучения на частоте отличной от частот официальной карты занятости эфира. Для создания такой карты используются официальные данные по работающим радиостанциям и данные по собственному измерению частот работающих радиостанций на определённом расстоянии от объекта. Расстояние

берется большим дальности действия закладки (обычно около 2 м), что позволяет избежать ситуации, когда мощная закладка будет принята за легальный источник.

2. Наличие маломощного излучения в ограниченной области пространства, причём максимум излучения наблюдается вблизи закладки; уровень излучения уменьшается при удалении от закладки. Уровень излучения от передатчиков официальных служб в пределах помещения и вблизи от него постоянен.
3. Наличие гармоник в излучении. В связи с необходимостью уменьшения габаритов закладок в них отсутствуют качественные фильтры выходного сигнала. В современных закладках ослабление гармоник составляет 40 дБ; наличие гармоник может быть обнаружено приёмником на расстоянии до 10 метров.
4. Наличие модуляции несущей частоты звуками, раздающимися в контролируемом помещении. Модуляция приводит к двум эффектам:

   а) размывание спектра выходного сигнала, то есть кроме несущей частоты будут наблюдаться сочетание несущей частоты с частотой звука в помещении (данный эффект не относится к кодирующему типу модуляции).

   б) к возможности прослушивания на поисковом приемнике шумов помещения (эффект звуковой обратной связи), если закладка работает без маскирования. При маскировании будет прослушиваться «какафония» (для выявления понятной речи можно применять специальные алгоритмы, но обычно обходятся зондированием импульсными акустичестическими сигналами). При использовании в закладке кодирования оператор будет слышать только белый шум, то есть по данному признаку закладка не может быть обнаруженной.
5. Непостоянство излучения радиозакладок, включаемых голосом и дистанционно. В зависимости от режима работы, обычно днём, они частично включаются, а ночью выключены. Сокращение времени выхода в эфир уменьшает возможность обнаружения РЗ; в то же время непостоянство излучения является признаком наличия сложной радиозакладки. Простейшие радиозакладки, работающие по этому признаку, обнаружить невозможно.
6. Наличие нелинейных элементов в РЗ. Радиозакладка может быть обнаружена даже в том случае, если она не работает. Причиной этого является наличие в РЗ нелинейных элементов, которые могут быть обнаружены методом нелинейной радиолокации (см 8.8.2.3).

8.7. Системы защиты от утечки по электромагнитному каналу

Защита от утечки по электромагнитному каналу обеспечивается пассивными и активными методами.

8.7.1. Методы пассивной защиты

К методам пассивной защиты относится комплекс мероприятий по экранированию помещения и сигнальных проводов, осуществление развязки по цепям питания и т.д.

8.7.1.1. Экранирование помещений и сигнальных проводов

Наиболее радикальным способом предотвращения перехвата информации от побочных излучений и установленных радиозакладок является экранирование помещений.

Экранирование с хорошим контактом делается медной сеткой или фольгой по всем стенам, потолку и полу, окна закрывают алюминиевыми жалюзями (рис. 8.17).

Без экрана информация из (·)А от сигнала U_c передавалась в (·)В через паразитную емкость $C_п$, а сигналы от передатчика излучались в пространство. При наличии экрана сигнал с (·)А через $C_п$ замыкается на экран, с передатчика сигнал также замыкается на экран. Эффект излучения за пределы помещений снижается в 10 – 1000 раз.

Таким образом, в место нахождения агента информация не поступает.

Для устранения наводок от информационного сигнала на соседние провода общего жгута необходимо помещать информационные линии в экранирующие короба.

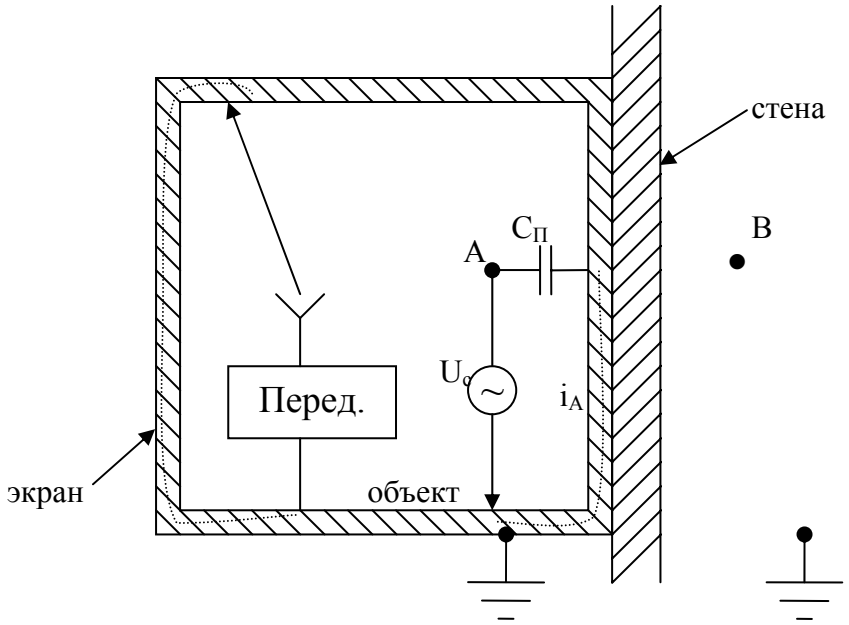


Рис. 8.17

При невозможности использования экранирующих коробов наиболее важные информационные сигналы передаются с использованием экранированных проводов. Положительные свойства экрана можно продемонстрировать с помощью следующего примера.

Пусть имеется провод 1 с информацией (рис 8.18,а), за счёт паразитной емкостной или индуктивной связи сигнал будет передаваться на другой провод 2, находящийся в общем жгуте, с которого агент может снять информацию.

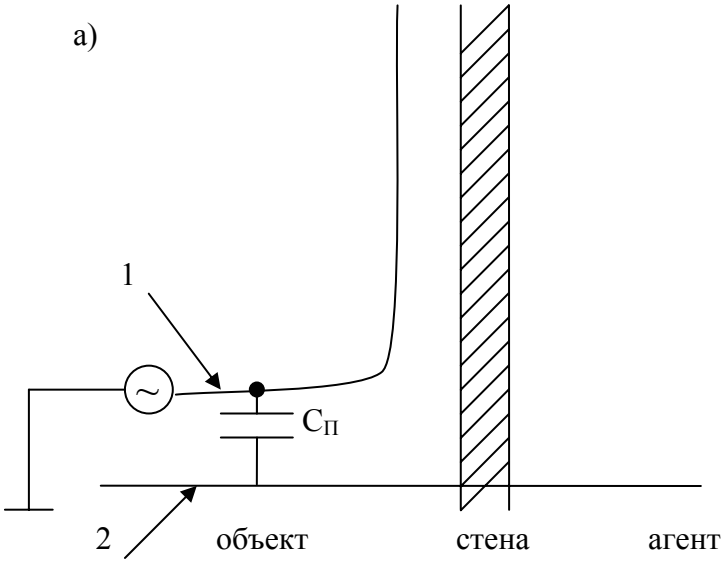


Рис. 8.18,а

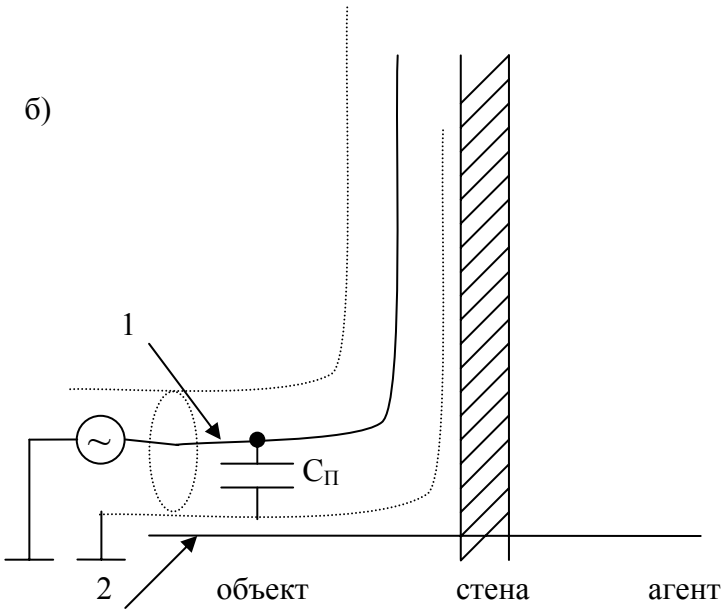


Рис. 8.18,б

При помещении провода в экран (рис 8.18б) информация через $C_п$ и экран замыкается на корпус и не поступает к агенту.

Для исключения утечки информации за счёт создаваемых магнитных полей необходимо скручивать информационные провода (рис 8.19).

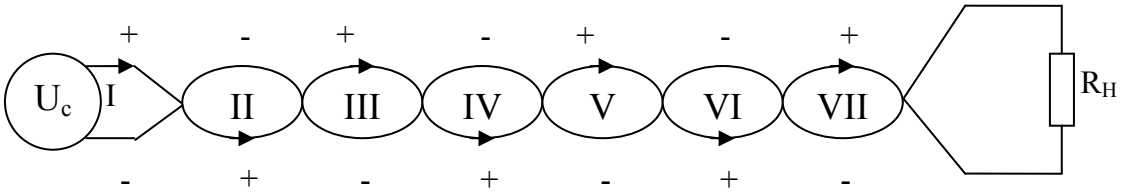


Рис. 8.19

По проводам течет ток, и образуются магнитные потоки. При скрутке образуются контура I, II, III, и т.д. В связи с тем, что магнитные потоки от соседних контуров направлены в разные стороны, суммарный магнитный поток близок к нулю и, следовательно, излучение информации в пространство близко к нулю.

Сочетание скрутки проводов с дополнительным экраном (триаксиальный кабель) позволяет снизить утечку информации и по магнитным, и по электростатическим каналам.

8.7.1.2. Развязки по цепям питания и земле

Мощные устройства вычислительной и копировальной техники потребляют значительный ток (например, по цепи 220 В). Этот ток даже на очень малом сопротивлении проводов цепи питания создаёт падение напряжения. При подключении к какому-нибудь доступному участку этих проводов агент получает информацию. Соответственно, необходимо, чтобы информация не доходила до этого доступного участка, то есть её необходимо замкнуть внутри помещения.

Для этого мощные устройства (рис. 8.20) подключаются в розетку через сетевой фильтр (например, ФСП-3Ф-10А фирма ППШ,
не пропускающий в сеть помехи с f≤150 кГц при I_{max}= 10 А).

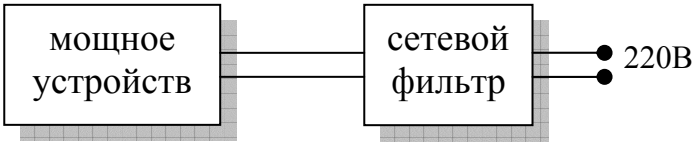


Рис. 8.20.

Для обнаружения утечки информации через сеть 220 В используются различные устройства (например, комплекс АРК-Д1, "Крона") [5].

8.7.2. Технические средства для поиска работающих радиозакладок

Для поиска работающих радиозакладок используются индикаторы (детекторы) поля, специальные приемники, комплексы радиоконтроля и выявления закладных устройств. Обширный материал по видам и параметрам этих устройств приведен в работах [2, 5, 8]; в нашем пособии приводятся данные по небольшому количеству изделий с целью ознакомления с ориентировочными техническими характеристиками.

8.7.2.1. Индикаторы (детекторы) поля [5] – это приемники с низкой чувствительностью. Они могут обнаруживать сигнал на весьма малых расстояниях (10 – 40 см). Важным достоинством детекторов является способность обнаруживать средства несанкционированного съёма информации СНСИ по высокочастотному излучению независимо от вида модуляции. Основной принцип поиска заключается в определении максимума излучения.
Простейшая схема индикатора поля приведена на рис 8.21

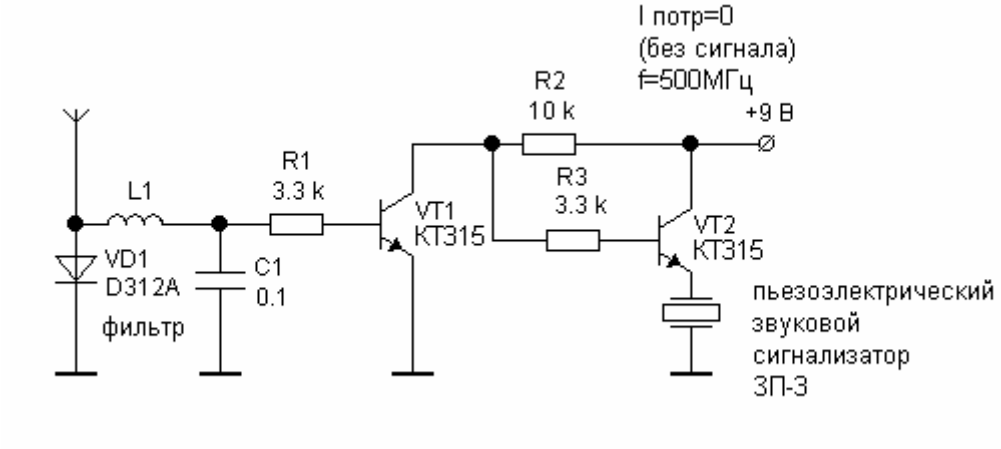


Рис. 8.21

Настройка чувствительности осуществляется изменением длины телескопической антенны. Мощность радиополя вблизи "жучка" (на расстоянии 5-10 см), как правило, значительно превышает фоновые значения, а при удалении на 50-100 см (в условиях больших городов) сигнал "жучка" сливается с фоном. Для детекторов обычно указывают:

- диапазон регистрируемых частот (обычно 50-1000 МГц);
- чувствительность или дальность обнаружения;
- ресурс источника питания.

Практическая проверка детекторов осуществляется на месте эксплуатации с помощью 2-3 радиомикрофонов средней дальности действия (150-200 м), работающих в перечисленных выше диапазонах. Если детектор на удалении от "жучка" на 2-3 м молчит, а на расстоянии 20-30 см даёт сигнал, то настройки проведены правильно. Если детектор даёт сигнал на расстоянии 2-3 м, то кроме "душевного дискомфорта" оператор ничего не получит. В более сложных детекторах используют режимы:

- "ступенчатый аттенюатор" – для загрубления чувствительности;
- "фильтрация помех" – для фильтрации фиксированных государственных и коммерческих радиостанций и телевизионных каналов.

Хорошие индикаторы поля снабжены частотомерами и акустическими динамиками. Отсчёт одной и той же частоты в последовательных измерениях является признаком наличия излучения. Амплитудные детекторы, применяемые в индикаторах для определения уровня излучения, одновременно являются детекторами сигналов с амплитудной модуляцией. Это позволяет детектировать высокочастотный сигнал от закладки, который промодулирован звуком помещения (для закладок с амплитудной модуляцией) и, соответственно, прослушивать в наушниках оператора звук помещения. Звук помещения в наушниках является гарантией того, что работает закладка. Во многих случаях даже для закладок с частотной модуляцией индикаторы позволяют ее обнаружить по прослушиваемому в наушниках звуку в помещении. Это обусловлено тем, что в большинстве закладок существует паразитная амплитудная модуляция.

Для увеличения чувствительности используют детекторы, включенные по дифференциальной схеме (рис. 8.22). Такой детектор состоит из двух устройств, выделяющих высокочастотную составляющую (устройство №1 и №2), дифференциального усилителя ДУ, на выходе которого получается разностный сигнал, и устройства сигнализации, например, динамика.

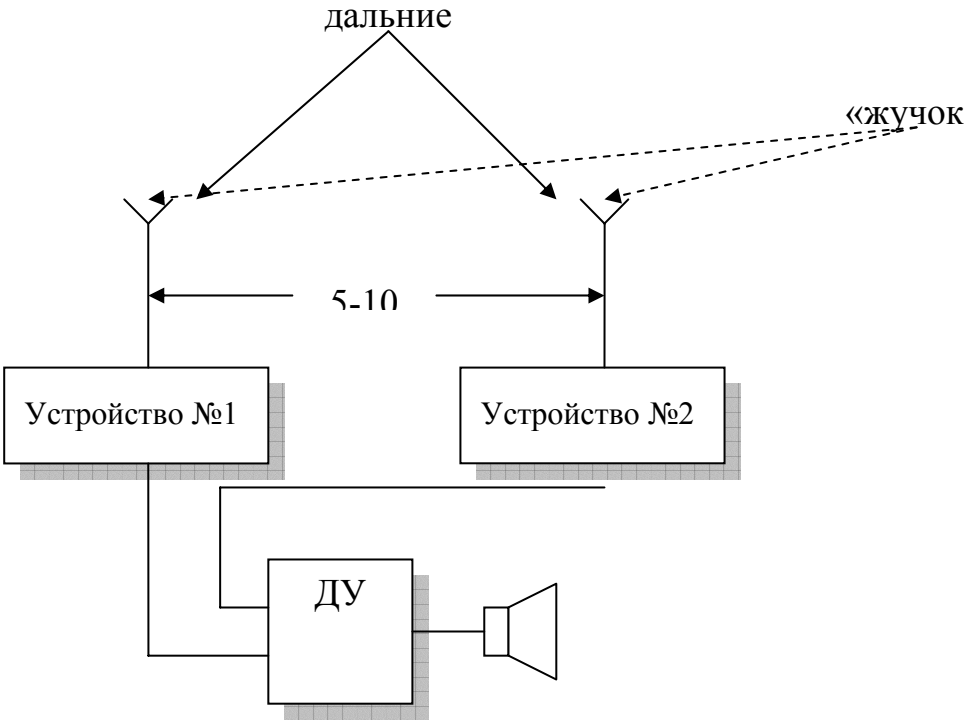


Рис. 8.22

Дальние станции создают одинаковые сигналы в сбалансированных устройствах №1 и №2, поэтому разностный сигнал равен нулю. Если индикатор находится вблизи радиозакладки, то из-за разнесения антенн устройств №1 и №2 сигналы на выходе устройств №1 и №2 будут отличаться, в результате появиться сигнал о наличии "жучка" несмотря на наличие мешающих станций.

Недостатком детекторов является малая чувствительность, которая обычно неравномерна в пределах рабочего диапазона.

Современные индикаторы поля комплектуются устройствами измерения частоты. Если в пределах некоторого промежутка времени фиксируется одна и та же частота, то это указывает на то, что это работает какая-то радиостанция (закладка), а не временная помеха от мощных устройств. Подобные устройства называются частотомерами. Примерами индикаторов могут служить следующие устройства [5]:

СИВ – прибор, предназначенный для измерения частоты радиосигналов и поиска прослушивающих устройств. Он имеет цифровой фильтр, функцию автозахвата, десятичный 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.

ПИТОН – приемник-детектор, предназначенный для обнаружения и демодуляции частотномодулированных сигналов в диапазоне от 30 до 1000 МГц; чувствительность не хуже –48 дБ относительно 1 В; время сканирования не более 2 с; задержка поиска после пропадания сигнала – не более 3 с; питание от 6 элементов по 1.5 В; габариты – 146x70x45 мм.

8.7.2.2. Панорамные приемники (сканеры) – являются более сложными устройствами, чем индикаторы поля. Характерной особенностью панорамных приемников являются:

- чрезвычайно большой диапазон контролируемых частот;
- высокая избирательность;
- перестраиваемый шаг настройки;
- большое количество каналов памяти зафиксированных сигналов;
- возможность прослушивания информации переданной радиозакладкой при различных видах применяемой в закладке модуляции.

Для построения панорамных приемников используется метод последовательного анализа. При последовательном анализе весь диапазон контроля разбивается на несколько поддиапазонов. Реальный коэффициент перекрытия внутри поддиапазона 2 - 2.5; переход с одного поддиапазона на другой осуществляется заменой высокочастотных фильтров. Структурная схема приемников подобного типа приведена на рис. 8.23. С антенны входной сигнал поступает на перестраиваемые фильтры высокой частоты ФВЧ. Гетеродин Г обеспечивает перестройку приемника в заданной полосе. На выходе смесителя СМ получается сигнал с фиксированной промежуточной частотой. Сигнал усиливается усилителем промежуточной частоты УПЧ и далее поступает на анализатор А. При автоматической перестройке приемник как бы прощупывает (сканирует) частотный диапазон; при обнаружении

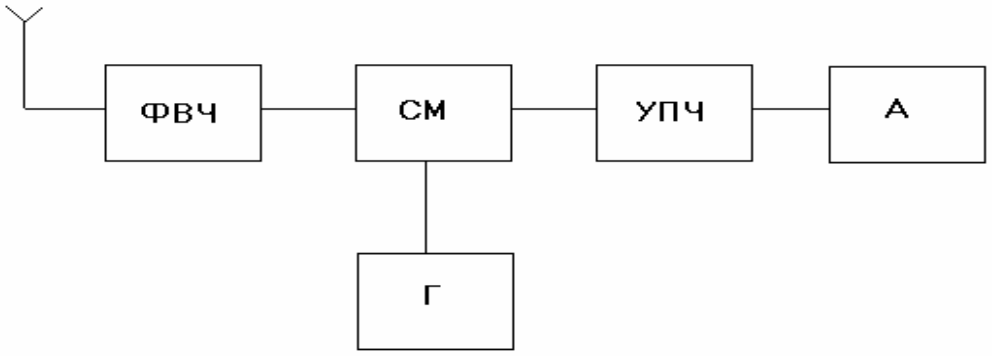


Рис. 8.23

сигнала сканирование прекращается и возобновляется в соответствии с заложенным алгоритмом.

Технические данные некоторых сканеров приведены в табл. 8.1.

Таблица 8.1

Модель	Диапазон МГц	Вид модуляции	Чувст. мкВ (с/ш=1)	Шаг настройки кГц	Кол-во каналов памяти	Габариты мм	Вес кг
IC-R 9000	0.03...1999	AM,FM,CW, FS,SSB,WFM	0.3...6	0.01;0.1;1; 10;12.5;20 ;25;100	1000	424x150x365	20
FSM-8.5	26...1000	AM,FM,WFM	1...10	ручная плавная	-	210x158x52	
IC-R 7100	25...199.9	AM,FM,WFM,SSB	0.2...1.6	от 0.1 до 1000	900	241x94x239	6
IC-R 7000	25...999.9 1025..1999	AM,FM,WFM,SSB	0.3...1	99		286x110x276	8
IC-R 100	0.1...1856	AM,FM	0.2...3.2	1.5;8;9;10	121	150x50x181	1.4
AR-3000A	0.1...2036	AM,FM,WFM,L	0.25...3	от 0.05 до 995 по 0.05	400	200x138x80	1.2
TRM-230	20...1000	AM,FM,WFM	1	-	30	188x71x212	3
TRM-231	20...1000	AM,FM,WFM	0.5	-	100	433x132x465	15
EB-100 Miniport	20...1000	AM,FM,WFM,SSB,FSK, CW	1...9999	-	30	188x71x212	3
STV-401	26...300	AM,FM,WFM	2	ручная плавная	-	360x320x130	7

Аббревиатуры, приведенные в табл. 8.1, следующие:

AM – амплитудная модуляция; FM – частотная модуляция; CW – телеграфные сигналы; WFM – широкополосная частотная модуляция; NFM - узкополосная частотная модуляция; SSB – однополосная амплитудная модуляция (USB – прием

верхней боковой полосы, LSB – прием нижней боковой полосы); FS – фазовая модуляция. “В некоторых 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 контроля. Кроме того, 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 (голоса в помещении), но не среагирует на излучение от включившегося факса или вдруг заискрившейся электророзетки [5]”.

Если заранее неизвестен вид модуляции, применяемой в закладке, то для ее поиска применяется особый вид сканеров – анализаторы спектра. “Анализатор спектра позволяет получить частотный портрет сигнала за счет того, что принятый сигнал как бы последовательно просматривается специальным узкополосным фильтром, выводя данные на экран устройства”[5]. Данные по анализаторам спектра одной из фирм (Hewlett Packard) приведены в табл. 8.2

Таблица 8.2

Наименование характеристик	Индекс (тип)			
	HP 8560 E	HP 8561 E	HP 8563 E	HP 8564 E
Диапазон частот	От 30 Гц до 2,9 ГГц	От 30 Гц до 6,9 ГГц	От 9 кГц до 26,5 ГГц	От 9 кГц до 40 ГГц
Погрешность измерения амплитуды, Дб	1,85		3	
Погрешность измерения частоты, Гц	106		1 кГц	
Ширина полосы разрешения	От 1 Гц до 2 МГц			
Чувствительность, Дб	-145			
Тип детектора	AM/FM			

Большинство панорамных приемников по последовательному интерфейсу RS-232 могут сопрягаться с ПЭВМ. При этом повышается надежность и оперативность поиска РЗ. На Российском рынке наиболее известны следующие программы: Скан Ар, Sedif, Flesn, RS peus, Крот-mini и др.. ПЭВМ при этом решает следующие задачи [5]:

- Хранение информации об официально работающих радиостанциях в контролируемом диапазоне частот;
- Получение программными методами временных и частотных характеристик принимаемых сигналов;
- Тестирование принимаемых сигналов по совокупности признаков на

принадлежность к РЗ.

Стоимость панорамных приемников достаточно высока: например, изделие “Тантал-1000” московской фирмы “Анна” стоит 960 $, японский приемник AR-3000 – 1400 $.

8.7.2.3. Программно-аппаратные комплексы

Дальнейшим шагом на пути совершенствования поисковых устройств является создание программно-аппаратных комплексов. Возможности программно-аппаратных комплексов намного шире, чем у просто совмещенных с ЭВМ сканирующих приемников. Комплексы обеспечивают:

- выявление излучения РЗ;
- пеленгование РЗ в реальном масштабе времени;
- определение дальности до РЗ;
- обработку сигналов с целью определения их принадлежности к излучению радиозакладок;
- контроль силовых, телефонных, радиотрансляционных и других сетей;
- работу в многоканальном режиме, позволяющем контролировать несколько объектов одновременно;
- постановку прицельных помех на частотах излучения РЗ и др.

Наибольшей популярностью среди специально разработанных комплексов пользуются изделия OSC-5000(Oscor), CPM-700(Акула), ST031(Пиранья), АРК.

В работе [5] приводится ряд характеристик этих комплексов, в том числе комплекса АРК.

Комплексы АРК представлены семейством стационарных, мобильных (автомобильных, вертолетных) и портативных приборов.

С точки зрения поиска ЗУ наибольший интерес представляют именно портативные комплексы АРК-Д1 (КРОНА-1), АРК-ПК и многоканальный комплекс контроля помещений учреждения АРК-Д3 (КРОНА-2).

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 следующее:

- возможность обнаружения излучений радиомикрофонов, работающих под прикрытием мощных станций, различение внешних и внутренних источников излучений для контролируемых помещений;
  (Данная функция обеспечивается за счет применения разнесённой 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 закладных устройств в сетях переменного тока в радиотрансляционных, в телефонных и других сетях;
- контроль излучений внедренных портативных телевизионных камер (устройство АРК-КТВ);
- активное и пассивное выявление излучений специальных технических средств негласного съёма 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 95, 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.

Комплексы размещаются 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.

Стоимость комплексов весьма велика, так, например, стоимость изделия OSC-5000 составляет 12000-16000 $ [5].

Какому комплексу отдать предпочтение, зависит прежде всего от решаемых задач и возможностей потребителя.

8.7.3. Поиск радиозакладок нелинейными радиолокатарами

Детекторы, сканеры, частотомеры, анализаторы спектра и многие другие устройства могут обнаружить только работающую закладку, когда она излучает в эфир энергию. Если же закладка установлена в ждущем режиме программно, дистанционно или каким-либо другим способом, то она не излучает энергию и вышеперечисленными средствами обнаружена быть не может.

Для обнаружения как работающих, так и закладок в ждущем режиме используют нелинейные радиолокаторы (НРЛ) [17,18]. Рассмотрим принцип работы НРЛ. Оператор включает НРЛ и последовательно облучает ($f \approx 600 - 900 МГц$) различные точки комнаты. Во всех закладках имеются нелинейные элементы: диоды, транзисторы, микросхемы. Происходит облучение интерьера и элементов закладки. От интерьера комнаты и от закладки в приемное устройство НЛ поступает отраженный сигнал. Причём, частота отражённого сигнала от интерьера, корпуса закладки, ее линейных элементов будет такая же, как частота облучения.

А вот от нелинейных элементов отраженный сигнал кроме первой гармоники будет содержать и боле высокие гармоники. Например, при подаче на диод с вольтамперной

характеристикой (рис 8.24,а) переменного напряжения (рис 8.24,б) через диод потечет ток (рис 8.25,в). Спектр такого периодического сигнала, в общем случае, содержит постоянную составляющую, первую, вторую, третью и т.д. гармоники; причем основная мощность сигнала сосредоточена в первых гармониках
и с повышением номера гармоники эта мощность уменьшается.

Таким образом, если приемное устройство НРЛ получает отклик на второй и третьей гармониках, то значит обнаружен нелинейный элемент, то есть как будто бы РЗ найдена. Но, к сожалению, это может оказаться не РЗ, а естественный нелинейный элемент металл – окисел – металл, иначе МОМ – диод (ржавчина, канцелярские скребки, монеты, арматура стены
и т. п.). Соответственно необходимо различить сигналы от искусственных и естественных нелинейных элементов. В зависимости от вида излучения (непрерывное или импульсное), эта задача решается по разному.

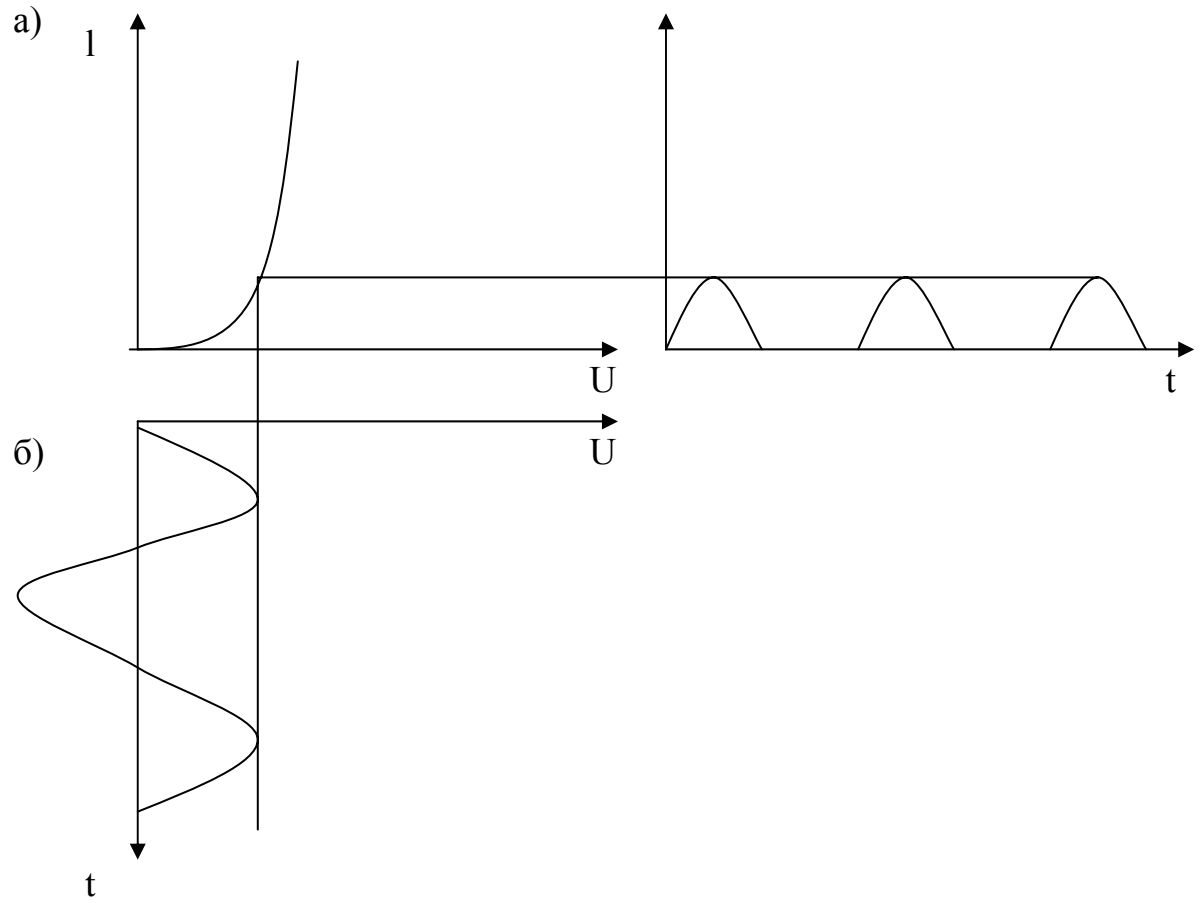


Рис. 8.24

В общих чертах рассмотрим **НРЛ с непрерывным режимом излучения**. Этот вид излучения, в основном, применяется в зарубежных разработках, в Российских разработках используется редко. Примером Российского НРЛ с таким режимом излучения является Родник-23.

В табл. 8.4 приведены характеристики различных Российских устройств НРЛ, в том числе и Родника-23 [17].

Таблица 8.4

Тип локатора	*Режим излучения*	*Мощность передачи ,Вт min/max*	*Коэффициент усиления антенны, дБ*	*Частота излучения, МГц*	*Частота приема, МГц*	*Чувствит. ДБ/Вт*	*Диаграмма направл. глав. лепест., гр.*	*Поляр и-зация*
Онега-3	имп.	/100	3	910	1820	-120	90	Эллипсо

					2730			ид
NR-900M	имп.	40/150	8-9	900	1800	-115	60-70	Кругова я
NR-900E	имп.	40/150	8-9	900	1800 2700	-115	60-70	Кругова я
Родник-23	непрер.	0,03/4	3-8	910	1820 2730	-145	100	Линейна я
Циклон-МІА	имп.	/300	3	680	1360	-110	110	Кругова я

Рассмотрим вначале *принцип обнаружения работающих РЗ.*
Непрерывный режим работы характеризуется малой мощностью передатчика, поэтому к нелинейным элементам РЗ приходит небольшой сигнал. Как показано в работе [18] диоды, транзисторы, микросхемы во включенном состоянии имеют небольшое открывающее смещение и квадратичную характеристику, а естественные нелинейные элементы имеют характеристику близкую к кубичной. Поэтому, если на локатор приходит отклик на второй гармонике больший, чем на третьей – значит обнаружена работающая РЗ; если приходит отклик на третьей гармонике больший, чем на второй – значит в этом месте находятся естественные нелинейные элементы (ржавчина и т.д.). Амплитудные значения отраженных сигналов весьма малы. Открывающее напряжение во включенной РЗ повышает крутизну вольтамперной характеристики искусственного нелинейного элемента и поэтому амплитуда отраженного сигнала от работающей РЗ значительно больше, чем от неработающей, это одна из причин, почему работающие РЗ обнаруживаются проще, чем неработающие.

Принцип обнаружения выключенных радиозакладок

РЗ в обесточенном состоянии имеет “искусственные p-n переходы в точности подобны МОМ- диодам”. Кроме того, автор работы [18] утверждает, что нелинейные элементы, выполненные по КМОП – технологии, имеют так же характеристики подобные МОМ – диодам, и, следовательно, даже действующие закладки на КМОП элементах по предыдущей методике не будут обнаружены. Для обнаружения РЗ в дежурном режиме и РЗ на КМОП элементах можно включить в точках (где есть отклик на гармониках) вибратор. По мнению автора работы [18] вибрация окажет воздействия на естественные p-n переходы (на сигнале отклика будет наблюдаться модуляция с частотой вибрации), а на искусственные p-n переходы вибрация не окажет действия.

Таким образом, если оператор получает сигнал на третьей гармонике с модуляцией, то это МОМ – диод. Если оператор получает сигнал на второй гармонике без модуляции, то это действующая РЗ на биполярных элементах. Если оператор получает сигнал на третьей гармонике без модуляции, то это или РЗ на биполярных элементах в ждущем режиме, или РЗ на КМОП элементах. Необходимо помнить, что мощность облучения мала, и сигнал от РЗ в ждущем режиме очень трудно выделить. Дальность обнаружения (глубина просвечивания интерьера) 10 – 15см [17].

НРЛ с импульсным режимом работы

В НРЛ с импульсным режимом работы вся мощность сосредоточена
в высокочастотной пачке. При больших значениях импульсной мощности дальность обнаружения возрастает и достигает 20 – 25 см. Сделав большую скважность, можно получить небольшую среднюю мощность, то есть, обеспечить кажущуюся безвредную работу персонала с НРЛ. При большой мощности излучения естественные и искусственные нелинейные элементы имеют примерно одинаковый вид вольтамперных характеристик и поэтому отклик от них будет не на разных гармониках а на одинаковых. В связи с этим в аппаратуре можно оставить устройство обнаружения только на одной гармонике [18].

Для того чтобы различить РЗ от МОМ - диода применяют вибрацию конструкции. Если сигнал получается с модуляцией, то это МОМ- диод; если сигнал на локаторе будет без модуляции, то это РЗ. Большая мощность излучения в импульсе позволяет получить достаточно большой сигнал от неработающих закладок и, соответственно, обнаружить их.

Рассмотрим более подробно импульсный режим работы. Формула для определения мощности отклика объекта на №-ой гармонике $P_{Nпр}$ в месте расположения приемной антенны локатора и комментарии к ней взяты из работы [17,18] и приводятся ниже.

$$P_{Nпр.}=P_{изл.}G_{изл.}G_{Nпр.}\,\lambda^2/(4\pi r)^4.\,\lambda^2/N^2.G_{Hопр.}G_{Nизл.}\,\xi_N(\omega,P_{изл.}).K_1(\omega)K_2(\omega_N), \quad (1)$$

где $P_{Nпр.}$ – мощность отклика объекта на N-ой гармонике в месте расположения приемной антенны локатора;

$P_{изл.}$ – мощность излучения локатора;

$G_{изл.}$ – коэффициент усиления излучающей антенны локатора;

$G_{Nпр.}$ – коэффициент усиления приемной антенны локатора на N-ой гармонике;

$\lambda = c/f$ - длина волны излучения локатора (эквивалентна частоте, где с – скорость света, f – частота излучения локатора);

r – расстояние до объекта;

N – номер принимаемой локатором гармоники;

$G_{Hопр.}$ – коэффициент усиления эквивалентной приемной антенны нелинейного объекта;

$K_1(\omega)$ - частотно-зависимый коэффициент затухания зондирующего сигнала локатора в среде распространения;

$K_2(\omega_N)$ - частотно-зависимый коэффициент затухания сигнала N-ой гармоники от объекта в среде распространения;

$\xi_N(\omega, P_{изл.})$ – коэффициент нелинейного преобразования для N-ой гармоники, который (как будет показано ниже), зависит от частоты и мощности излучения локатора.

Анализ выражения (1) показывает, что мощность на гармониках, излучаемая объектом (а значит, и эффективность обнаружения при прочих равных условиях), возрастает при увеличении мощности излучения локатора $P_{изл.}$, снижении частоты его излучения f и номера принимаемой гармоники N. Кроме того, чем ниже частота излучения локатора, тем меньшие значения имеют коэффициенты затухания K_1, K_2, что также ведёт к увеличению мощности сигнала от объекта. Существенным отличием нелинейной локации от классического наблюдения (обнаружения) объектов с активным ответом является прямое преобразование падающей на объект энергии зондирующего сигнала в энергию высших гармоник.

В связи с этим, модель радиолокационного наблюдения (обнаружения) в условиях нелинейной локации можно классифицировать как наблюдение с полуактивным ответом, что связано с отсутствием потребления энергии объектом от специального источника питания. Его особенностями являются очень малое значение коэффициента нелинейного преобразования (ξ_N <<1) и зависимость от частоты и мощности зондирующего сигнала локатора. График зависимости коэффициента нелинейного преобразования для второй гармоники ε_2 от входной мощности непосредственно на входе нелинейного элемента РЗ приведен на рис 8.25,а. Этот график автор работы [17,18] получил путем теоретического моделирования.

Из рис. 8.25,а видно, что на начальном участке ε_2 резко увеличивается с увеличением приходящей на вход нелинейного элемента мощности, в дальнейшем после 1Вт скорость роста ε_2 с повышением $P_{вх\ НЭ}$ уменьшается, то есть увеличивать мощность локатора для повышения ε_2 целесообразно только до определенных значений.

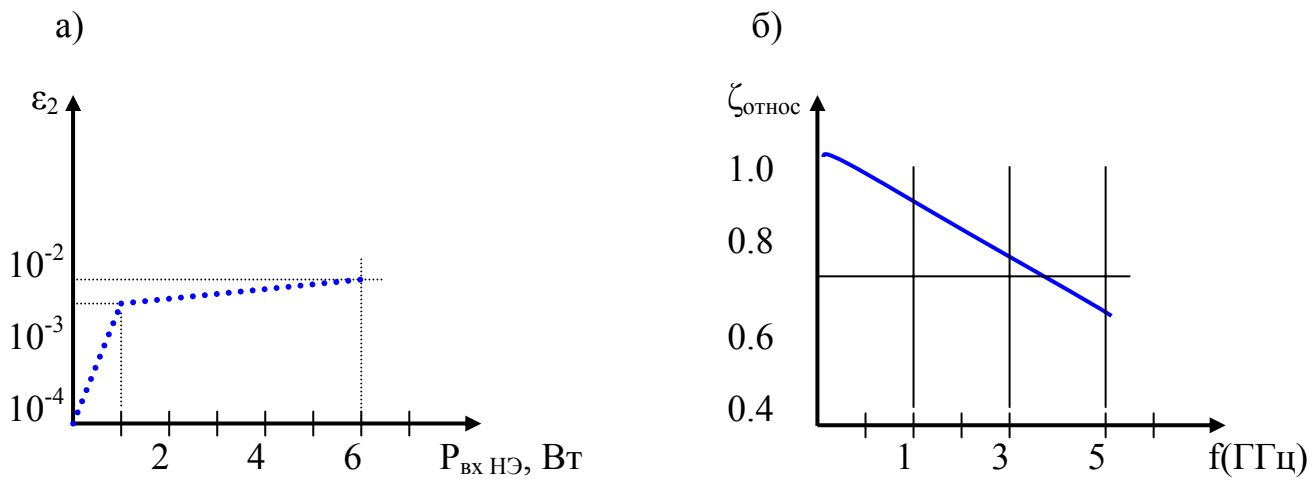


Рис. 8.25

На рис 8.25,б приведена зависимость относительного значения ε_2 от частоты, показывающая, что для получения большего значения ε_2 частоты облучения должны быть меньше 1ГГц. В реальных НРЛ (табл. 8.4) мощность передатчика в импульсном режиме ограничивается значениями 150-300 Вт, частота излучения 680-910 МГц, что согласуется с приведенной формулой для расчета $P_{Nпр}$ и графиком рис 8.25.

Технические характеристики НРЛ

Для потребителей НРЛ среди технических характеристик, приведенных в табл. 8.4, наиболее интересными являются диаграмма направленности главного лепестка, поляризации антенных устройств,
а также, оставленные за рамками таблицы, данные по дальности обнаружения РЗ на фоне коррозийных нелинейных отражателей, возможность достоверного подтверждения наличия РЗ и безопасность эксплуатации. Кратко осветим эти вопросы.
Диаграмма направленности НРЛ существенно влияет на удобство эксплуатации. Чем шире диаграмма направленности главного лепестка, тем больше шансов, что рабочие радиотехнические устройства помещения попадут в зону облучения НРЛ и создадут ложный сигнал. Поэтому при работе с НРЛ “Родник-23”, “Циклон-МIА”, имеющих ширину лепестка 100^0-110^0, приходится выносить оборудование из помещения, что не совсем удобно.

Поляризация антенной системы может быть линейной, эллипсоидной, круговой. Если при круговой и эллипсоидной поляризации (НРЛ типа NR-900, циклон-МIА) плоскость исследуется за один раз, то при линейной поляризации за два раза в двух взаимоперпендикулярных направлениях (НРЛ типа Родник 23) что приводит к двукратному увеличению времени проверки [17].
Дальность обнаружения РЗ тем больше, чем больше мощность облучения. НРЛ с импульсным мощным облучением позволяют обнаружить РЗ в толще строительных конструкций на глубине 20 – 25 см, НРЛ с непрерывным излучением поиск РЗ на глубине до 10 –15 см.

Возможность достоверного подтверждения наличия РЗ чаще всего обеспечивается физическим поиском. Только небольшое число НРЛ (например, Родник 23) позволяет дополнительно подтвердить, что работает РЗ т.к. при облучении работающей РЗ будет прослушиваться акустика помещения.

Безопасность эксплуатации СВЧ техники является важным параметром для человека. Маломощные НРЛ (типа Родник 23) не вносят помех работающей бытовой технике и не оказывают вредного влияния на здоровье человека. Мощные импульсные

НРЛ так же не должны влиять на человека из-за большой скважности сигналов, то есть малой средней мощности. Однако, испытания НРЛ серии NR показали, что у “оператора после часа работы начинают болеть глаза (так как именно глаза наиболее чувствительны к СВЧ- излучению” [17]; чем это вызвано – не исследовалось.

Итак, НРЛ позволяет обнаружить как работающие, так и не работающие РЗ. Импульсные НРЛ не рекомендуется использовать в помещении, где работают люди. НРЛ не может обнаружить РЗ, установленную в какую-нибудь электронную аппаратуру, так как сигнал отклика от РЗ будет замаскирован откликом от аппаратуры, в которую она вмонтирована. Поэтому в комплекте с НРЛ должен использоваться панорамный приёмник.

Стоимость НРЛ весьма высокая, например, HP-900M стоит 6000 долларов, HP-900E стоит 8500 долларов [18]; комплектация службы безопасности такими устройствами приводит к значительным затратам.

Вопрос о виде применяемой поисковой аппаратуры решает заказчик обследования с учетом рекомендаций бригады поиска.

9. ТЕЛЕФОННЫЙ КАНАЛ УТЕЧКИ ИНФОРМАЦИИ

В данной главе рассматриваются различные технические аспекты перехвата информации, курсирующей по проводным и радиотелефонным каналам. Обсуждаются методы и средства несанкционированного съема информации (НСИ) в телефонных каналах, методы и средства противодействия НСИ для обеспечения безопасности передачи информации. Автор работы [5] предлагает телефонную систему связи представить следующим образом: телефонный аппарат абонента, телефонный провод от аппарата до распределённой коробки РК, магнитный кабель от коробки до автоматической телефонной станции АТС. Далее сигнал распространяется по многоканальным кабелям, либо по радиоканалу до следующей АТС. Наиболее опасными зонами с точки зрения вероятности применения подслушивающих устройств, считаются зоны от ТА до АТС.

Способы несанкционированного подключения к проводной телефонной линии и телефону

Съем информации возможен как при телефонном разговоре абонентов, так и за счет прослушивания помещения при положенной телефонной трубке.

НСИ чаще всего осуществляется следующими методами:

1) подключение к телефонной линии:

- непосредственное подключение к телефонной линии;
- подключение с использованием трансформаторов, индуктивных датчиков, преобразователей Холла.

2) использование микрофона телефона для прослушивания разговоров на объекте при положенной телефонной трубке:
- с доработкой телефонного аппарата (ТА);
- беззаходовые варианты.

3) использование диктофонов.
4) использование ретрансляторов.

9.1. Контактный и бесконтактный метод съема информации за счет непосредственного подключения аппаратуры к телефонной линии

9.1.1. Непосредственное подключение к телефонной линии

Наиболее просто подслушать телефонный разговор можно за счёт подключения своего аппарата в линию, по которой ведется передача. Подключение обычно осуществляется тонкими иголками и проводами, так что визуально определить место подключения трудно. При подключении аппарата напряжение в линии уменьшается из-за низкого входного сопротивления телефона. Этот эффект легко обнаруживается, поэтому агент подключается к линии через дополнительное сопротивление R (рис. 9.1). Применение резистора R позволяет сохранить напряжение в линии, но в то же время основная часть сигнала будет гаситься на этом сопротивлении, и прослушивание будет затруднено [5].

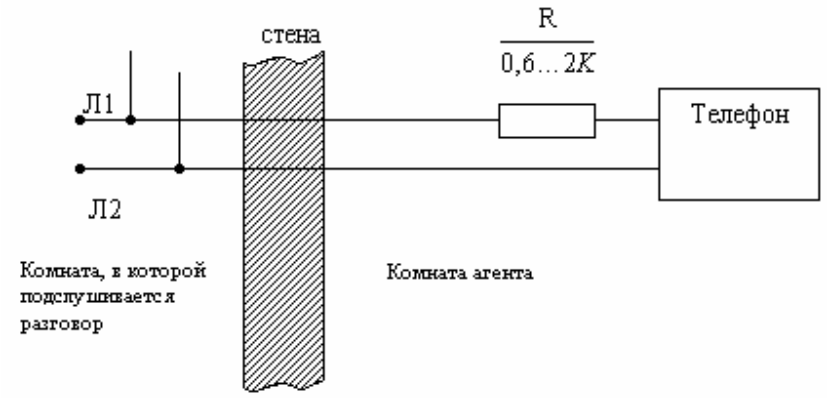


Рис. 9.1

9.1.2. Применение трансформаторов

Применение согласующего трансформатора [5] позволяет сохранить и напряжение в линии, и полезный сигнал. Возможно последовательное (рис. 9.2,а) и параллельное (рис. 9.2,б) подключение трансформатора в линию. При последовательном подключении в связи с тем, что активное сопротивление первичной обмотки трансформатора мало, режим в телефонной линии по постоянному току не изменится, т. е. эффект подключения не может быть обнаружен. Полезный сигнал через трансформатор без ослабления (в зависимости от соотношения числа витков первичной и вторичной обмоток) поступает на телефон агента. В качестве такого трансформатора может, например, использоваться реле РЭС 15 (РЭС 49); обмотка реле используется в качестве первичной, вторичную обмотку наматывают поверх обмотки реле проводом 0,1 мм. Недостаток такого метода подключения – необходимость разрыва линии в комнате, в которой прослушивается разговор, с целью подключения трансформатора.

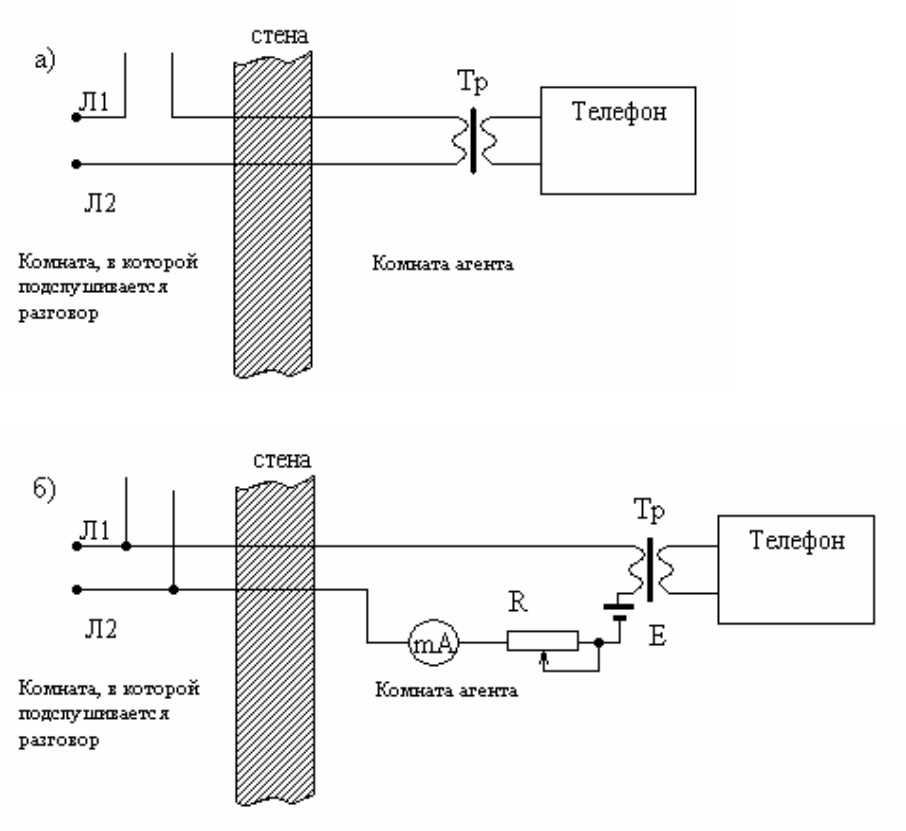


Рис. 9.2

При параллельном подключении трансформатора (рис. 9.2,б) линия Л1-Л2 не разрывается. Для того, чтобы трансформатор не шунтировал телефонную линию, он подключается через источник питания E и резистор R. Изменением сопротивления резистора R добиваются нулевых показаний миллиамперметра. Подслушивающее устройство при этом будет иметь бесконечно большое входное сопротивление и не может быть обнаружено простейшими защитными устройствами.

9.1.3. Применение индуктивных датчиков

Индуктивные датчики позволяют снимать информацию с телефонной линии без контактного подключения (рис. 9.3). При ведении разговора в линии протекает переменный ток I, который наводит
в индуктивности L переменное напряжение U_x, которое затем подается на наушники (рис. 9.3,а). На рис.9.3,б приведена упрощенная схема снятия информации с кабеля, уложенного в телефонном колодце. На кабель надевается индуктивный датчик, состоящий из магнитного сердечника 1 и сердечника 2, на котором намотана индуктивность L. Сердечники соединяются зажимами. С индуктивности L снимается информация.
По данному принципу работает система “Крот” производства США, позволяющая при соответствующей обработке снимать информацию с кабеля, в который заложено 60 каналов. Информация записывается на магнитофон [13].

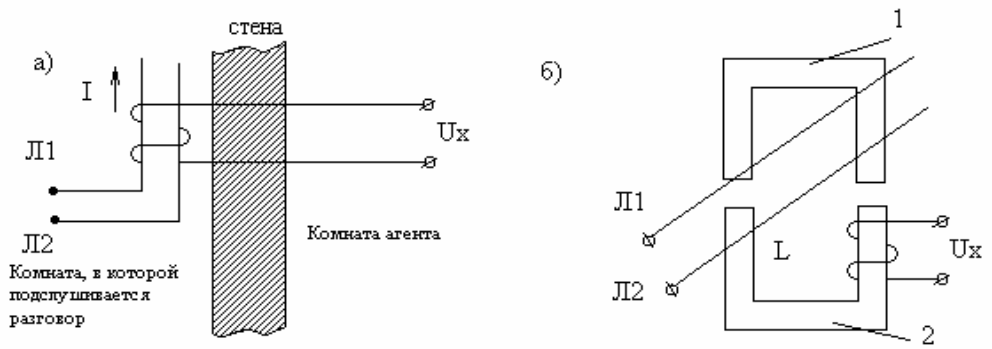


Рис.9.3

9.1.4. Применение преобразователей Холла

Бесконтактный съём информации с линии возможен также при использовании в качестве преобразователя датчика Холла. Преобразователь Холла представляет собой небольшую полупроводниковую пластину (выполненную, например, на основе

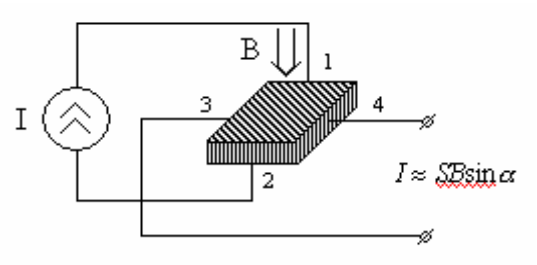


Рис. 9.4

арсенид-фосфид-индия, индий-арсениума и т. д.). Пластина имеет
4 вывода (рис. 9.4): два токовых вывода 1-2 и два вывода 3-4 для снятия напряжения. К выводам 1-2 подключается источник тока.

При отсутствии внешнего магнитного поля носители тока (дырки, электроны) равномерно перемещаются от вывода 1 к выводу 2, поэтому на зажимах 3-4 ЭДС равна нулю (e=0). При воздействии внешнего магнитного поля с индукцией B носители тока под действием силы Лоренца отклоняются к одной из боковых граней (3-4), вследствие чего на одной из граней создаётся избыток зарядов одного знака, а на противоположной грани возникает заряд другого знака. В результате появляется ЭДС Холла

$$e = SB\sin\alpha$$

где S – чувствительность преобразователя Холла,

α - угол между вектором магнитной индукции B и плоскостью датчика.

Наиболее часто в технике измерений используются датчики ПХЭ 602817, X 511 и др. Ориентировочные их характеристики: S = 1 В/Тл
(в старой системе 10 мкВ/Гс при токе 0,1 А); температурный коэффициент чувствительности 0,001 %/^{0}С; ЭДС неэквипотенциальности 10 мкВ (e=10мкВ при B=0); размеры 1x1x0,2 мм.

Схема снятия информации с помощью датчика Холла приведена на рис. 9.5. При разговоре по линии Л1-Л2 протекает переменный ток, который создает переменный магнитный поток, воздействующий на преобразователь Холла ПХ; на выводах 3-4 возникает переменное напряжение, которое усиливается и подается на динамик.

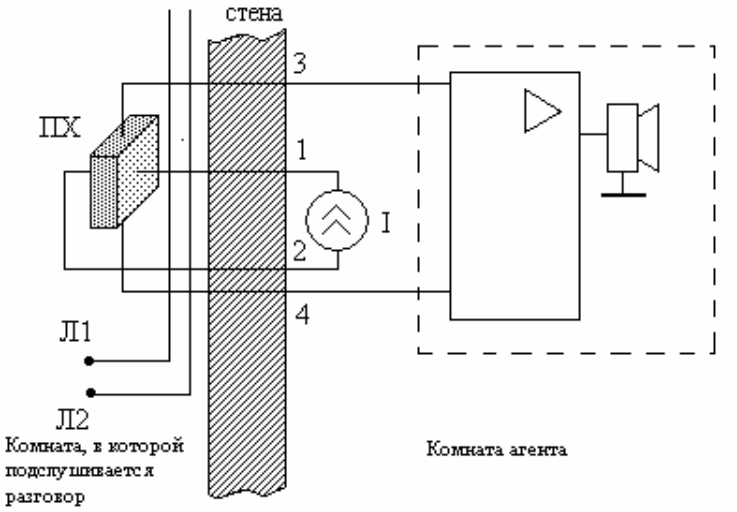


Рис. 9.5

Сведения о некоторых промышленных устройствах несанкционированного подключения к телефонной линии [13] приведены в табл. 9.1

Табл. 9.1

Марка	Габаритные размеры, мм	Питание	Тип первичного преобразователя
UM-122	100x50x18	Автономное 9В	Контактная игла
БД 1	—	Автономное	Индуктивный датчик
STG-4525	125x75x25	Автономное 9В	Индуктивный датчик
PRO-1213	95x58x25 и 50x22x10	Автономное 9В	Эффект Холла

9.2. Использование микрофона телефонного аппарата при положенной телефонной трубке

9.2.1. Общий принцип работы телефонного аппарата

Прежде чем перейти к рассмотрению схем, ознакомимся с принципом работы телефона на примере аппарата ТАН-70 (рис. 9.6).

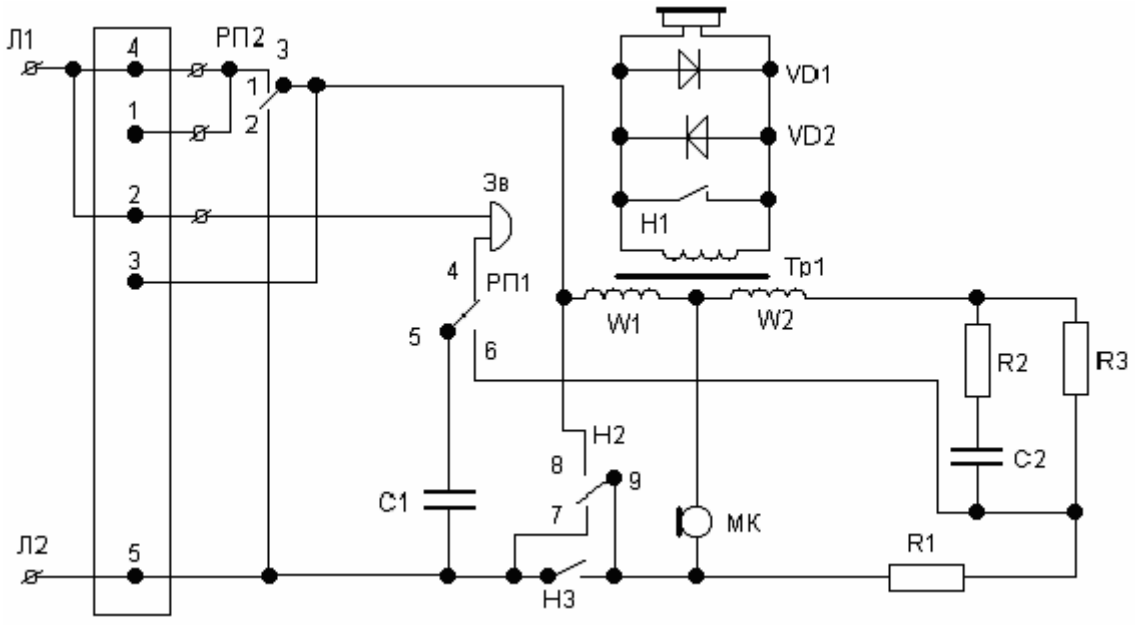


Рис.9.6

На рисунке приведены следующие обозначения: *Зв* – звонок, *МК* – микрофон, *Т* – телефон, *РП1, РП2* – рычажные переключатели (на рисунке показано состояние переключателей при положенной трубке), *Н1, Н2, Н3, Н4* – переключаемые контакты номеронабирателя. Эквивалентная схема в исходном состоянии приведена на рис. 9.7.
В исходном состоянии МК рычажным переключателем *РП2* (рис. 9.7) отключен от линии *Л1* и зашунтирован контактами *Н2* и *Н4*; телефон *Т* зашунтирован контактами *Н1*. Напряжение с линии *Л1-Л2* (~ 120 В) подводится к звонку, но оно недостаточно для работы звонка. При звонке от абонента

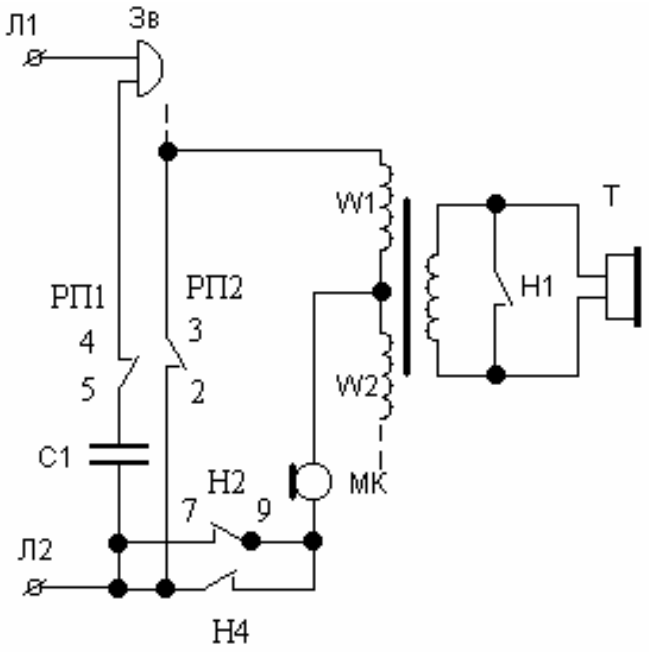


Рис. 9.7

напряжение в сети увеличивается, что приводит к срабатыванию звонка. После получения звонка снимается трубка, срабатывают рычажные переключатели *РП1* и *РП2* (замыкаются контакта 1-3 *РП2* и 5-6 *РП1*), размыкаются контакты *Н1*, переключатель *Н2* сохраняет свое положение.

Эквивалентная схема аппарата при переговорах между абонентами приведена на рис. 9.8.

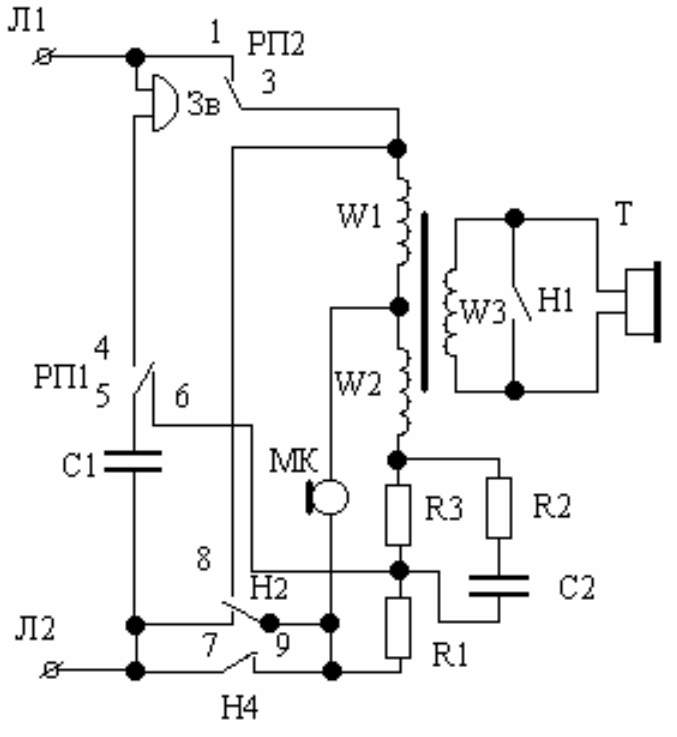


Рис. 9.8

Если собеседник передает сообщение, то переменный сигнал проходит через обмотки *W1, W2* и сопротивления *R3, R1*, которые частично или полностью зашунтированы конденсаторами *С2 и С1*. Обмотки *W1, W2* для сообщения включены последовательно, поэтому во вторичной обмотке *W3* будет суммарный сигнал, который прослушивается в телефонных наушниках. Микрофон только частично шунтирует обмотку *W2*. При снятой трубке *Н1* разомкнут.

При передаче сообщения собеседнику сигнал с микрофона через обмотку *W1* и ключи *РП2* и *Н2*||*Н4* поступает в линию; в своей трубке сигнал не прослушивается, так как токи от микрофона в обмотках *W1* и *W2* текут во встречных направлениях.

При наборе номера положения *РП1* и *РП2* сохраняются; контакты *Н1* замыкаются, шунтируя телефон; переключатель *Н2* устанавливается в положение 8, шунтируя микрофон, контакты ключа *Н4* периодически размыкаются в зависимости от набранной цифры. Промежуток времени, когда линии *Л1-Л2* замкнута, определяется набираемой цифрой. Сочетание таких импульсов является кодом для вызова абонента. Упрощенная схема работы телефона при вызове абонента приведена на рис. 9.9.

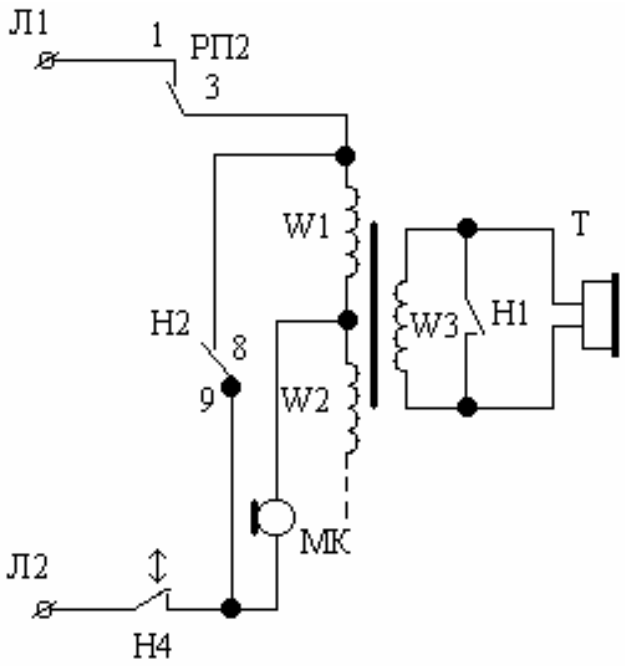


Рис. 9.9

На основании рассмотренного принципа работы телефона можно сделать вывод, что при положенной трубке сигнал с *МК* в линию не поступает; для подключения *МК* в линию с целью НСИ в помещении при положенной трубке необходимо дистанционно переключить *РП2* или подключить точку соединения *МК*, *W1*и *W2* к линии *Л1*.

9.2.2. Доработка телефонного аппарата с целью использования его микрофона

Существуют различные варианты доработки телефонного аппарата с целью снятия информации о разговорах в помещении за счёт микрофона положенной трубки ТА на объекте. В обычный телефонный аппарат (например, рис.9.6) устанавливается модуль, который своими выводами подключается к соответствующим контактам аппарата.

В настоящее время выпускаются устройства ELSY, TS-20-1, БОКС-Т и др., [5, 13], которые обеспечивают прослушивание помещения из любой точки земного шара при положенной трубке на объекте.

Рассмотрим принцип работы такого устройства. Агент набирает номер абонента, аппарат которого доработан; первые 2 звонка у абонента «проглатываются, т.е. аппарат не звонит. Затем агент кладёт трубку и через 30...60 секунд вновь набирает номер, даёт специальный сигнал. При этом, телефон на объекте включается на режим прослушивания и не реагирует на другие входящие звонки. Недостатком подобных устройств является то, что для переключения аппарата на прослушивание помещения необходимо делать два звонка и надеяться, что между этими двумя звонками никто не позвонит абоненту. Однако на Западе есть уже система TELE-MONITOR (стоимость 5000$), подключающая прослушивание без предварительного звонка. Принципиальные схемы этих устройств в открытой литературе пока не опубликованы.

По логике работы весьма близким к указанным устройствам является *блок телефонной системы дальнего оповещения* [20]. Рассматриваемое устройство является отдельным самостоятельным блоком, подключаемым к телефонной линии на объекте. Агент, находясь за тысячи километров от объекта по телефонной линии через телефонную станцию вызывает номер объекта. При вызове номера объекта устройство реагирует подобно автоответчику, на телефонный звонок оно реагирует шунтированием линии сопротивлением приблизительно 0,6...1,0 кОм,
в результате чего телефонная станция переключает линию в режим «приём-передача». Точно не известно, как будет реагировать обычный телефонный аппарат, включенный параллельно устройству. Можно предположить, что успеет раздаться один звонок, а затем включится блок. Если на объекте не успеют снять трубку, то блок будет работать,
а телефон объекта будет отключен. Если на объекте снимут трубку, то информация в линию будет поступать как с блока, так и через телефонную трубку. Отключиться от связи с агентом можно только при условии, что он сам снимет связь.

Рассмотрим работу структурной схемы блока (рис. 9.10). Всю работу можно разбить на 4 этапа (обозначим их **1**, **2**, **3**, **4**). При наборе агентом номера на объекте в линии *Л1-Л2* появляются сигналы вызова, срабатывает цепь **1** включения устройства, и коммутатор питания включает источник питания 12 В и, соответственно, таймер *А*. При включении таймера *А* срабатывает реле *К1*, и в линию *Л!-Л2* подключается сопротивление 0,6...1,0 кОм, которое является имитатором поднятой трубки. На этом заканчивается второй этап работы **2**. Телефонная станция воспринимает данный сигнал в качестве режима “поднятая трубка”, и линия (а также устройство на объекте) переводятся в режим “прием-передача”.

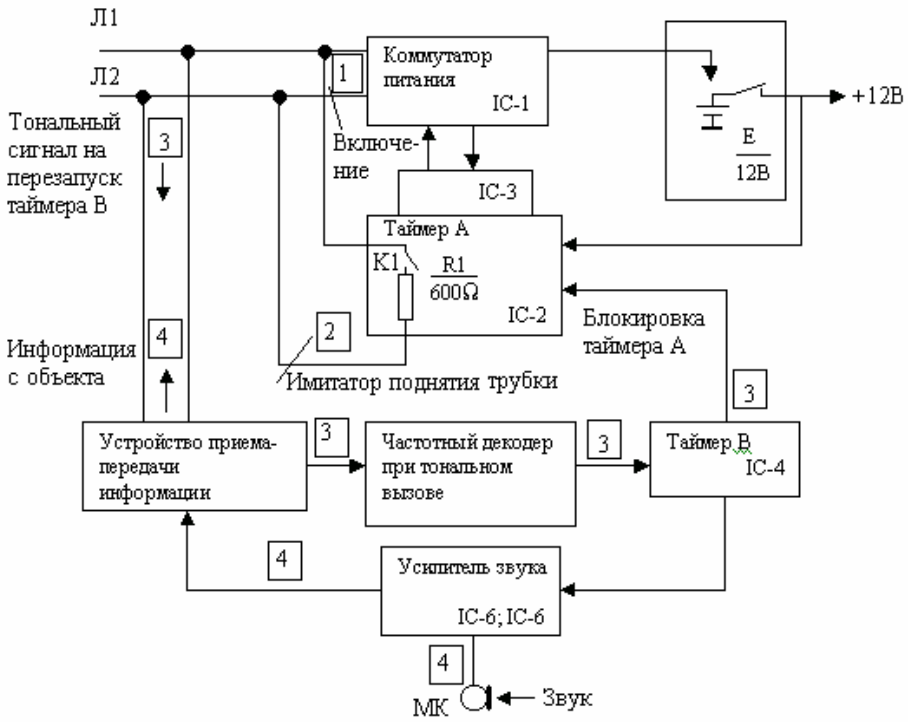


Рис. 9.10

Тональный сигнал вызова **3** успевает пройти через устройство приема-передачи информации, частотный декодер и запускает таймер *В*, который подключает усилитель звука и блокирует таймер *А*, то есть сохраняет имитацию режима “поднятая трубка”. Для сохранения режима подслушивания тональный сигнал подается через каждые 20...30 с.

При включении усилителя звука начинается четвертый этап работы **4**. Информация с объекта (звук) поступает на микрофон *МК* и далее через усилитель звука и устройство приема-передачи информации посылается в линию *Л1-Л2*, к которой подключен агент.

9.2.3. Беззаходовый НСИ

С микрофона телефонного аппарата при положенной трубке можно снять информацию и без доработки телефонного аппарата на объекте. Такие варианты снятия информации называются “*беззаходовыми*”. В основном при этом используются или недостатки конструкции телефонных аппаратов, или эффект “навязывания”.

В некоторых видах конструкций телефонных аппаратов элементы электромеханического звонка могут являться датчиком разговора, происходящего в помещении (рис. 9.11).

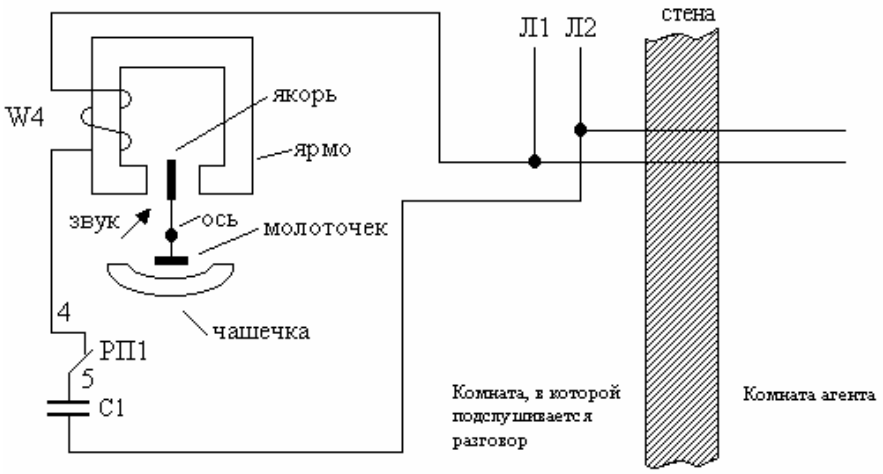


Рис. 9.11

При положенной телефонной трубке электромеханический звонок *Зв*, состоящий (рис. 9.11) из обмотки *W4*, ярма, якоря с молоточком и чашечки, подключён через реле *РП1* (рис. 9.6, рис. 9.11) и конденсатор *С1* к телефонной линии *Л1-Л2*. При разговоре в помещении звук воздействует на якорь и молоточек приводит к их перемещению около оси. В обмотке *W4* возникает небольшой переменный сигнал (примерно 0,5...10 мВ), который передается в линию *Л1-Л2* и может быть прослушан агентом. Так как сигнал весьма мал, то практически съём информации возможен на расстоянии до десятков метров.

Известны методы “навязывания” [5] с целью подключения микрофона отключённого телефонного аппарата в линию (рис. 9.12).

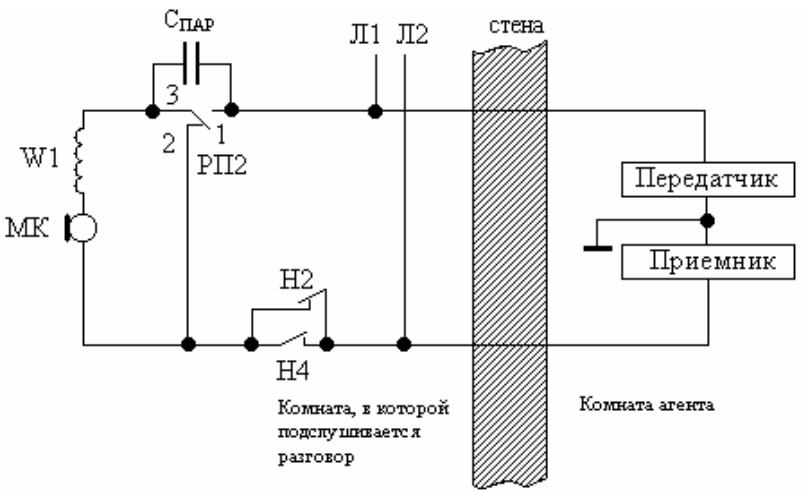


Рис. 9.12

Высокочастотный передатчик, имеющий частоту более 150 кГц, излучает сигнал в телефонную линию. Высокочастотный сигнал воздействует на элементы аппарата. На высоких частотах тумблеры, реле, переключатели рассматриваются как элементы с распределенными параметрами, поэтому контакт 3-2 *РП2* нарушается, и сигнал с передатчика частично поступает через $C_{параз}$ и *W1* на микрофон и далее на приемник. В указанной цепи течёт высокочастотный ток, промодулированный звуком от микрофона, который воспринимается приёмником. Из-за потери двухпроводной линии дальность съёма информации не превышает десятков метров.

9.3. Применение диктофонов

Особенность диктофона с правовой стороны заключается в том, что он не является спецсредством и не надо получать разрешение на его применение.

Различные типы диктофонов рассмотрены ранее в п.6.4 ниже будет рассмотрена одна из возможных схем подключения диктофона в телефонную сеть.

Использование диктофонов позволяет агенту находиться основную часть времени вне объекта и не привлекать к себе внимание. Для записи переговоров используется специальный диктофон со встроенной системой VOX, т.е. системой управления магнитофоном от голоса. Встроенная система VOX обеспечивает экономию ленты и потребления энергии, так как двигатель магнитофона включается только при разговоре или наличии сообщения в линии. Простейшая схема доработки обычного магнитофона для фиксации переговоров по телефонной линии приведена на рис.9.13.

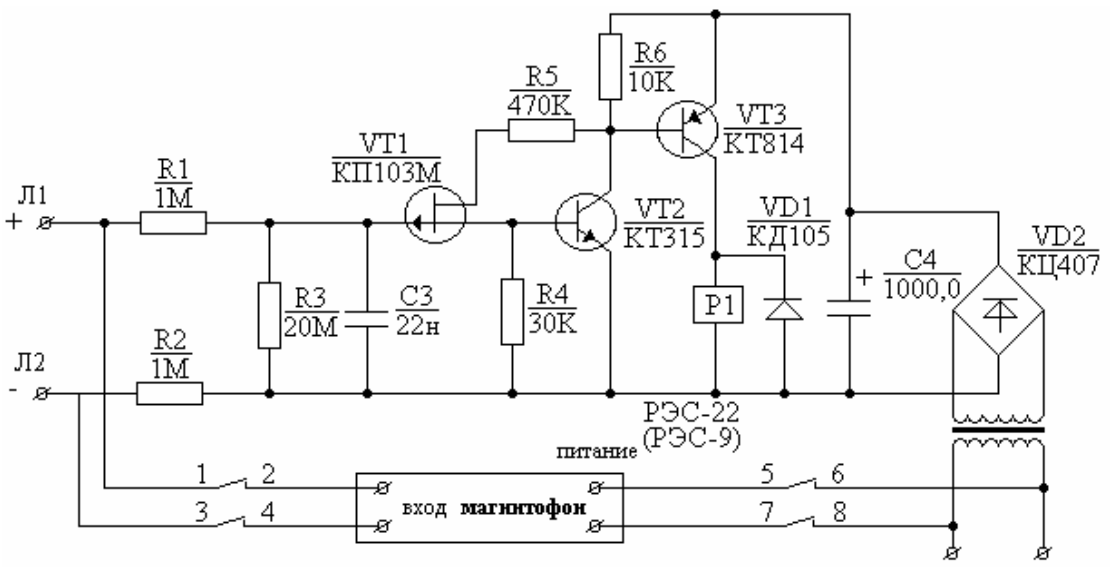


Рис.9.13

В исходном состоянии магнитофон включён “на запись”, но контактами реле *Р*1 1-2, 3-4, 5-6, 7-8 отключен от линии *Л1-Л2* и от источника питания 220 В. Пока трубка в комнате, в которой подслушивается разговор, не снята, напряжение в линии *Л1-Л2* на объекте большое, транзистор *VT1* закрыт и, соответственно, закрыты транзисторы *VT2* и *VT3*, реле *Р1* обесточено, и магнитофон отключен от входной цепи и цепи питания.

Если осуществляется связь на линии *Л1-Л2*, то напряжение в ней уменьшается, открываются транзисторы *VT1, VT2, VT3*; срабатывает реле, и магнитофон подключается к линии *Л1-Л2* и цепи питания, т. е. начинается запись. При завершении разговора и отключении от абонента напряжение в линии *Л1-Л2* повышается, закрываются транзисторы *VT1, VT2, VT3*; отключается реле *Р*1, и, соответственно, выключается микрофон. Использование указанного модуля позволяет экономить ленту, а также энергию при питании от автономного источника.

На основании данного принципа работают микрофоны РК-1985, MCV LD, MK7 APLD и др.; они выключаются приблизительно через 10 секунд после пропадания звука, обеспечивают запись на встроенный микрофон на расстоянии не менее 15 метров, имеют размеры пачки сигарет. Стоимость малогабаритного микрофона составляет 300...700$. диктофоны, подключаемые непосредственно в линию *Л1-Л2*, это, вероятно, РК-135S и LCT-AD, их уточненные характеристики пока не приводятся.

9.4. Телефонные ретрансляторы

В телефонных ретрансляторах первичным преобразователем является или микрофон телефонного аппарата или электрический сигнал, циркулирующий в телефонной линии. Этот низкочастотный сигнал ретранслятором преобразуется в высокочастотный модулированный сигнал, который может через антенну передаваться в эфир или вновь передаваться в телефонную линию. Если сигнал принимается с эфира, то агент использует приёмник, настроенный на определенную частоту. Если сигнал передавался в телефонную линию, то агент вынужден найти эту линию и подключиться к ней. В этом состоит недостаток последнего метода. Достоинство его в том, что в эфир ничего не излучается и, соответственно, обнаружить ретранслятор сложно. Обычно телефонные ретрансляторы используют эту же линию для питания, что позволяет обеспечить долговечность работы такого ретранслятора и его малые габариты. Ток потребления закладок $I_{пот}$ обычно мал, менее 3мА.

Если сделать более мощную закладку, то параметры линии будут нарушены и закладка будет легко обнаружена. Наиболее часто используются устройства без кварцевой стабилизации частоты, включенные в линию последовательно с телефонным аппаратом. Нестабильность источника питания приводит к уходу частоты передатчика (в пределах до 1% от номинала) и осложняет процесс снятия информации. Устройства с кварцевой стабилизацией частоты дороже, они используются и для последовательного и параллельного включения в линию. Рассмотрим ретранслятор [13], выполненный в виде модуля А, вмонтированного внутрь телефона (рис. 9.14).

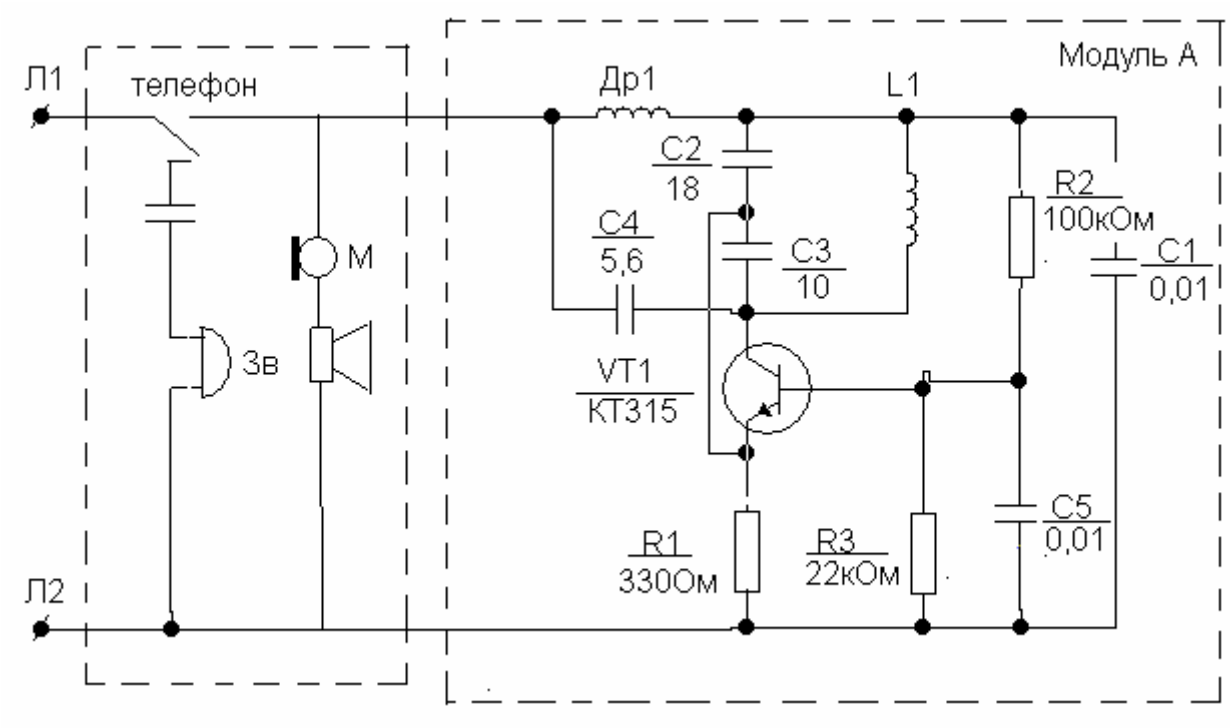


Рис.9.14

Питание модуля А осуществляется от линии Л1 - Л2 только при снятой трубке абонента, что дополнительно затрудняет его обнаружение. Дроссель Др1 и конденсатор С1 являются фильтром по цепи питания; точка покоя транзистора VT1 устанавливается делителем R2, R3. Частота генератора, выполненного на транзисторе VT1, определяется индуктивностью L1 и емкостью $C = C2\,(C3+C_{кэv}T)/[C2+(C3+C_{кэv}T)]$. Сообщение в линии, являясь низкочастотным сигналом, через индуктивность L1 воздействует на переход коллектор-эмиттер транзистора, изменяя его емкость. Изменение емкости $C_{кэvt}$ приводит к частотной модуляции генератора. Сигнал с генератора через конденсатор С4 передается в телефонную линию, которая используется в качестве антенны. Съем информации обеспечивается на расстоянии до 100 м
в УКВ диапазоне. По данным [13] L1 - бескаркасная катушка 4 мм,
W = 6 - 7 с диаметром провода 0,3 мм; Др1, служащий для разделения НЧ и ВЧ сигналов, имеет индуктивность 30 мкГн (тип ДПМ- 0,1)
Примером телефонной закладки может служить закладка РК 170 [5] с размерами 30 X 30 X 20 мм; вес 180г.; рабочая частота 100 кГц; используется частотная модуляция; в комплекте с закладкой поставляется приёмник. Закладка Model SIM-RMM также комплектуется передатчиком и приёмником. При положенной трубке телефона разговор в помещении контролируется встроенным высокочувствительным микрофоном. При снятии трубки передатчик переключается на контроль телефонных переговоров; размеры передатчика 28 X 10 X 7 мм; ток потребления
3 мА.

9.5. Утечка информации по сотовым цепям связи

Сотовые радиотелефонные каналы широко используются для связи как отдельными лицами так и фирмами. Одно из основных достоинств этих каналов - возможность поддерживать связь при передвижении и из трудно доступных мест. Основные проблемы, которые возникают при использовании радиоканалов, следующие:

защита от несанкционированного прослушивания;

помехозащищенность, скрытность местоположения абонента;

защита от двойников.

С позиций безопасности сотовые системы можно разделить на стандарты первого поколения (NMT, A, MPS и другие аналоговые стандарты) и стандарты 2 - ого поколения (GSM и другие цифровые стандарты. Существуют три участка, на которых возможно подслушивание:

а) радиолиния между абонентом и базовой станцией,

б) линия между базовой станцией и коммутатором подвижной службы

в) коммутатор.

Наиболее вероятным для использования является первый участок. Прослушивание переговоров по системам связи, использующим стандарты первого поколения, осуществляется радиолюбительскими, измерительными и специальными средствами:

а) Радиолюбительские средства НСИ

Для съёма информации могут использоваться сами радиотелефоны и " сканеры ". Радиотелефон в случае отключения своего передатчика и дополнением его " конвертором линии вверх " позволяет прослушивать чужие телефоны. Сканеры также позволяют прослушивать чужие переговоры, так как они являются перестраивающимися радиоприемниками. Недостатком данных устройств являлась необходимость нахождения агента недалеко от источника информации из-за существенного уменьшения отношения $U_c/U_ш$ с ростом расстояния.

б) Измерительные средства фирм покупаемые и используемые агентами для НСИ. Каждая фирма выпускает " измерительные" средства для технического обслуживания сотовых связей. Такое оборудование (купленное агентом) позволяет контролировать информацию, и месторасположения объекта информации при больших расстояниях между объектом и агентом (до 50 км)

в) " Специальные средства " НСИ.

Для контроля сотовой связи, поисков двойников, сопровождения входящих и исходящих звонков абонентов при переходе из соты в соту, проверки радиослышимости базовых станций фирмы выпускают программно - аппаратные комплексы контроля сотовых систем связи. Комплексы обладают большими возможностями, чем измерительные установки, но и стоят значительно дороже. Закупка агентами этих комплексов позволяет им контролировать аналоговые сотовые системы. Рассмотренные выше средства НСИ используются для прослушивания и записи переговоров, ведущихся по " аналоговым стандартам ". Шифрование в стандартах первого поколения не обеспечивает защиты от прослушивания. Связь по стандартам второго (цифрового) поколения (например, GSM) позволяет надежно шифровать (за отдельную плату) информацию. Отдельным лицам и не очень мощным организациям расшифровка информации недоступна. Только владельцы, имеющие очень большие средства, способны купить нужные комплексы для расшифровки (например, Siginit/Comint Spectra фирмы Hollandes Signaal).

9.6. Деконспирационные признаки

Наиболее информативными параметрами для обнаружения посторонних подключений являются напряжение в телефонной линии при положенной трубке телефона, напряжение в линии при снятой трубке, ток и напряжение в линии при появлении сигнала " Ответ станции "
(длинный гудок), рис. 9.15.

При подключении аппарата агента значения напряжений и токов получат отклонения от ежедневной нормы, существовавшей до подключения. Типичные значения подобных отклонений, определенные экспериментально для наиболее распространенных устройств НСИ, приведены в табл. 9.2.

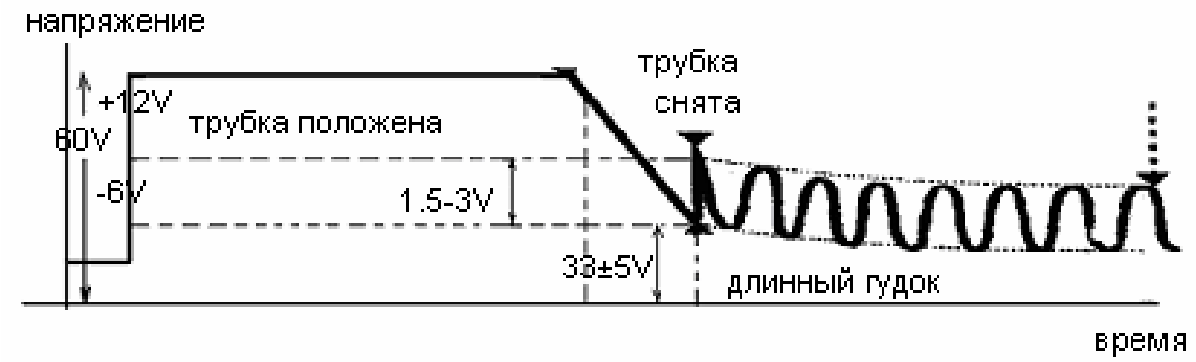


Рис. 9.15

Таблица 9.2

Вид подключения	**Параллельно е**	**Последовательное**
Изменение напряжения, В	2.5...4	0,8...2.2
Изменение тока, мА	0...0.8	3...5

Изменения напряжения относительно номинального для данной телефонной линии отмечаются как при положенной телефонной трубке, так и при снятой, а изменение тока через телефонный аппарат можно обнаружить только при снятой трубке. Нетрудно заметить, что значение падения напряжения, обусловленное подключением устройств любого типа, питающихся от телефонной линии, невелико и может быть принято за случайное отклонение в силу естественных причин. Обычно среднее значение напряжения телефонной линии при положенной телефонной трубке на различных АТС находится в пределах 60$\pm$12В, хотя плавные отклонения от среднего значения, характерные для конкретной линии, намного меньше и не превосходят единиц вольт. Поэтому по результатам однократного измерения нельзя судить о появлении постороннего подключения, а следует обязательно регулярно проводить измерения напряжения и тока линии и регистрировать значения в специальном журнале. Изменения параметров телефонной линии происходят при непосредственном подключении аппарата к линии и при подключении устройств, получающих питание от телефонной линии (ретрансляторов, модулей доработки телефонного аппарата). Устройства, в которых применяются индуктивные датчики, трансформаторы, преобразователи Холла (при автономном питании) , а также устройства с беззаходовым съёмом информации при своем подключении не изменяют параметров телефонной линии и, соответственно, не имеют технических деконспиративных признаков, то есть технически не могут быть обнаружены. Рассмотренные устройства съёма информации требуют первоначального

присутствия агента на месте установки аппаратуры, что приводит к возможности его физического обнаружения.

9.7. Устройства защиты от утечки информации по телефонному каналу

9.7.1. Обнаружение устройств, потребляющих ток из телефонной сети

Обнаружение подслушивающих устройств обеспечивается пробниками, индикаторами, а нейтрализация подслушивающих устройств обеспечивается устройствами, ставящими помеху. Рассмотрим простейший пробник.

Принцип действия пробника основан на измерении и анализе параметров телефонной линии. Устройства, потребляющие ток из телефонной сети, изменяют ее параметры. Вначале необходимо набрать статические данные и получить средние значения напряжения и тока при положенной трубке, снятой трубке, наборе номера и разговоре в разное время суток. Для проведения сравнительных характеристик желательно проводить измерение параметров нескольких примерно аналогичных линий. На рис. 9.16 приведена схема пробника, определяющего несанкционированное подключение к линии при ведении разговора.

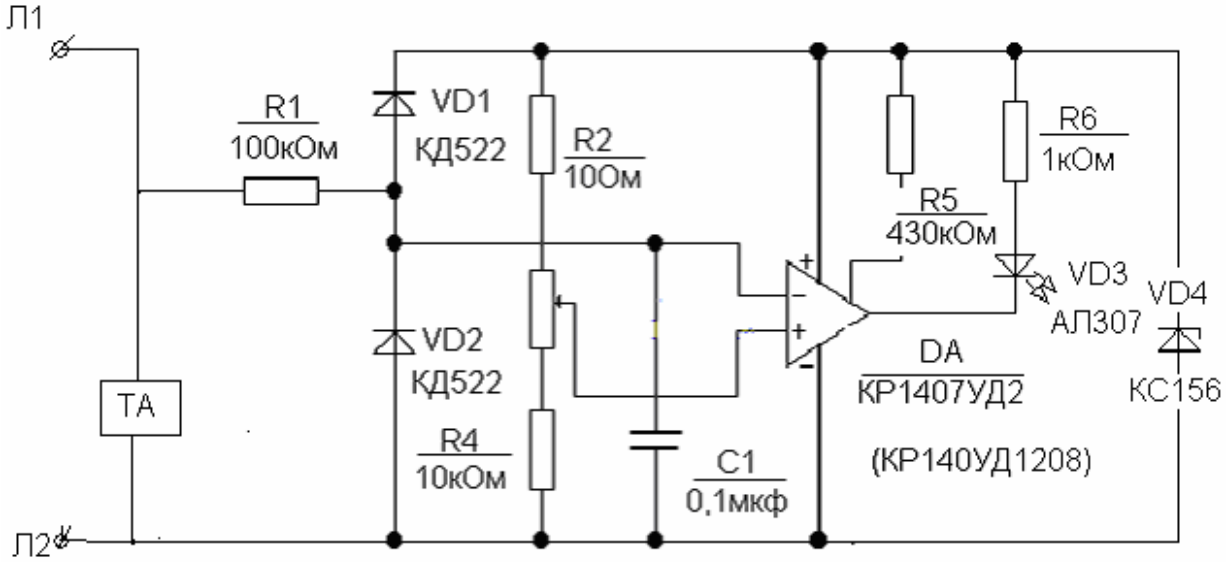


Рис. 9.16

При обычном подключении абонентов e+ > e- ; $U_{ВЫХ DA1}$ >0 (настройка производится при наличии разговора со знакомым абонентом; за счёт регулировки добивались, чтобы VD3 был погашен). При несанкционированном подключении Uл1-л2 уменьшается, уменьшается e+, e- сохраняется, т.к. напряжение стабилизировано стабилитроном VD4, VD3 излучает свет, сигнализируя о несанкционированном подключении (VD1, VD2 защищают операционный усилитель (ОУ) от изменения полярности в сети; C1 защищает ОУ от помех).

Рассмотренный принцип обнаружения подслушивающих устройств используется во многих пробниках, в том числе в изделии ЛСТ-1007 (телефонный страх). Основным достоинством индикаторов является низкая цена. Недостатками индикатора являются невозможность выявления устройств с бесконтактным подключением к линии и необходимость настройки индикатора под каждую конкретную телефонную линию.

9.7.2. Устройства, предотвращающие использование

микрофона телефонного аппарата

а). Защита звонковой цепи телефонного аппарата

Под воздействием голоса колеблются части электромеханического звонка и в линию наводится ЭДС до 500 мкВ, что может быть прослушано "агентом". Для устранения этого метода подслушивания в аппарат ставятся диоды. Они не пропускают информацию в линию; телефонный разговор имеет сигнал 1...3 В и проходит практически без затухания (есть патенты США, Великобритании, СССР).

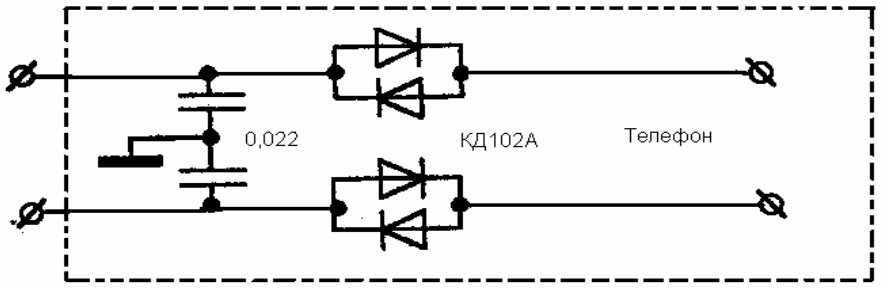


Рис. 9.17

б). Защита микрофона от воздействия внешнего высокочастотного сигнала

При воздействии ВЧ облучения переключатели, реле, тумблеры являются *распределенными индуктивностью и емкостью*, через которые микрофон подключается к телефонной линии и с линии будет сниматься сигнал. Для устранения этого эффекта параллельно телефонной линии включается блокировочный конденсатор, снижающий более, чем в 10 тысяч раз эффект этого подключения.

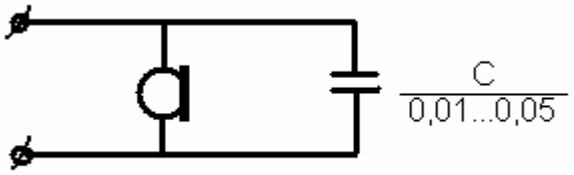


Рис. 9.18

в). Включение блокирующих устройств между телефонной линией и ТА

Устройства типа МТ203, МТ205 фирмы "МиниТех", включенные между телефонной линией и аппаратом, обеспечивают невозможность использования микрофона в положенной трубке ТА для прослушивания помещения (рис. 9.19).

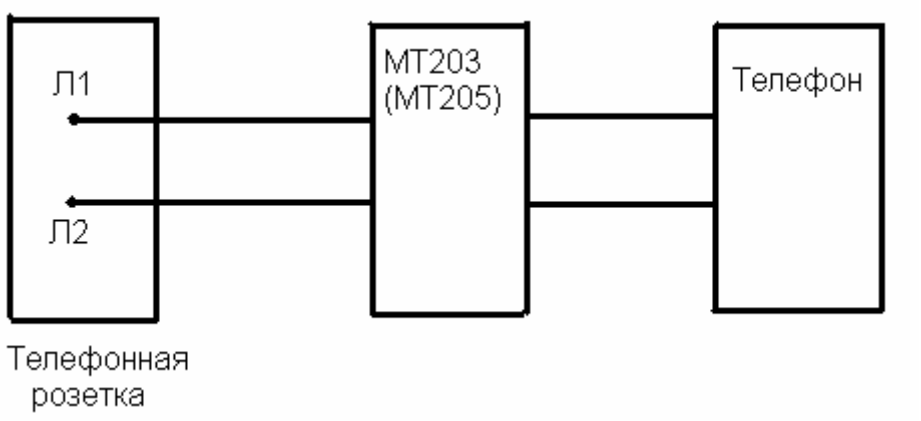


Рис. 9.19

9.7.3. Устройства, предотвращающие включение магнитофона, включающегося при подъеме трубки

Существуют специализированные магнитофоны, которые включаются при уменьшении напряжения в сети вследствие снятия трубки. Если трубка положена, то при несанкционированном подключении $U_{Л1-Л2}$ уменьшается и становится меньше $U_{01опущ}$ и загорается светодиод (рис. 9.20). Если трубка снята, то вместо U_{01} подключается U_{02} и при несанкционированном подключении $U_{Л1-Л2}$ уменьшается, и загорается светодиод.

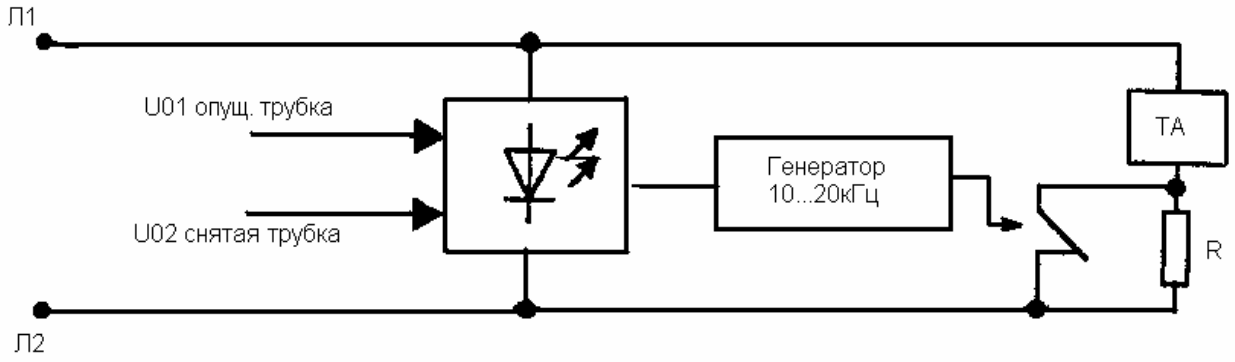


Рис. 9.20

При снятии трубки R расшунтируется и создается имитация, что ТА не подключен к разговору, т.к. $U_{Л1-Л2}$ не снижается, поэтому несанкционированный магнитофон, подключаемый по падению напряжения, не включится.

9.7.4. Многофункциональные устройства индивидуальной защиты телефонных линий [5]

Рассмотренные ранее принципы и ряд более сложных принципов используются в многофункциональных средствах защиты линий, например: Phone Guard 2, NG-303, Shark, SE-2001; Sl-2020; Sprut, Протон и т.д. Приведём характеристики одного из устройств Sl-2020. Это устройство обеспечивает:

- защиту линии, как при поднятой, так и при положенной трубке;
- модуляцию тока в телефонной линии широкополосным спецсигналом;
- цифровую индикацию напряжения в линии;
- противодействие передатчика с питанием от телефонной линии;
- противодействие работе магнитофонов, подключаемых к линии (при положенной трубке имитируется режим снятой трубки, что приводит к холостому прокручиванию ленты; а при снятой трубке имитируется режим положенной трубки, то есть не даёт возможности записи разговора);
- противодействие аппаратуре ВЧ- навязывания;
- активизацию при положенной трубке телефонных радиозакладок, что значительно облегчает их поиск.

Рассмотрим более подробно принцип работы защитных устройств, ставящих помеху. Для предотвращения съёма информации в телефонную линию от защитных устройств подается *пассивная или активная помеха*. Постановка *пассивной помехи* заключается в изменении напряжения
в телефонной линии при разговоре. Такая пассивная помеха уже достаточно эффективна, так как в большинстве случаев из-за жёстких требований к габаритам и потребляемой мощности схемотехника устройств УНСИ настроена на стандартное питание, т. е. на стандартное значение тока и напряжения линии при разговоре, поэтому даже простое увеличение напряжения на 3...5 В приводит к уходу несущей частоты
и снижению мощности излучения, затрудняя прием радиосигналов при помощи специального приемника с фиксированной настройкой. При перестройке приемника возможен прием, но разборчивость речи падает; дальность передачи сокращается, примерно, в 2 раза. Постановка *активной помехи* заключается в подмешивании в линию специальных сигналов большой амплитуды. С частотой выше частотного спектра, защищённого сигналами. Эти помехи вызывают перегрузку устройств агента, к выходу их из линейного режима. Как следствие, агент слышит только шум в своих наушниках. Кроме того, при положенной трубке большой сигнал активизирует устройства, включаемые голосом, и идёт бесполезная трата ленты в записывающем магнитофоне, а также напрасно тратится энергия элементов питания. Для замены кассет и элементов питания необходимо дополнительное и весьма опасное посещение объекта. Для того, чтобы помеха не мешала владельцу прибора, она компенсируется перед подачей на его телефонный аппарат. Чтобы помеха не мешала второму абоненту, она подбирается из сигналов, которые сильно затухают в линии и легко фильтруются АТС. Недостатком этого метода защиты являются возможность перехвата информации со стороны противоположного абонента.

9.7.5. Защита от НСИ в радиотелефонных каналах

Защита осуществляется кодированием. Оба разговаривающих абонента должны иметь кодирующие устройства. Без них связь невозможна. Кодирующие устройства

разделяются на аналоговые и цифровые. Аналоговые устройства (типа NMT , AMPS др.) более дешевы, но обеспечивают недостаточную криптостойкость (дешифрация занимает от нескольких часов до нескольких дней). Цифровые устройства шифрования (метод временных перестановок, инверсия спектра сигнала, преобразование временного масштаба и т.д.) более криптостойкие; надо помнить, что защита подключается за дополнительную плату. Для обеспечения шифрованной связи с рядом абонентов в США создана сеть специальных телефонных аппаратов, насчитывающая уже более 700 тысяч таких аппаратов. Применяемый телефон STU-3 ценой 2000$ позволяет обмениваться цифровой информацией со скоростью 2,4 Кбит/с. Ключи для связи изготавливаются в АНБ (Агентство Национальной Безопасности) - для правительственных организаций и в фирме GTE для коммерческих организаций. Для включения аппарата в защищённый режим пользователь вставляет ключ (пластиковую карточку) в приёмное устройство. После идентификации производится связь, при этом в АНБ автоматически проверяется, не была ли эта карточка утеряна кем - либо. Малогабаритный телефон типа STU – 3 стоит около 10 000$. Курс шифрования рассматривается в отдельной дисциплине «криптология».

В табл. 9.2 приведены характеристики некоторых вокодеров.

Таблица 9.2

Наименование изделия	**Количество ключей**	**Тип шифрования**	**Габариты, мм**	**Доп. данные**
Туман	1	инверсия спектра	200x250x60	приставка к ТА
Эхо 01	1	инверсия спектра	200x250x60	в корпусе ТА
Эхо 02	256	инверсия спектра	--	приставка к ТА
УЗТП	256	инверсия спектра	225x150x55	приставка к ТА
АКТП	1	инверсия спектра	--	приставка к ТА
Базальт	10	временной	210x290x40	Подставка под ТА
Базальт - 2	10	временной	--	в корпусе ТА
УЗА	10	временной	--	в дипломате, переносной вариан
Grupset	10	цифровой	--	в корпусе ТА, идентификация абонента с помощью магнит.карты
ILS 3130	52000	инверсия спектра	--	

Продолжение табл. 9.2

VS - 1	13122	инверсия спектра	--	
PASI - ТЛФ	10	цифровой	210x290x60	приставка к ТА
TTS 3200	10 x 10	частотный	--	в дипломате
АРСН-68 М	2x10	временной	--	
Орех-А	--	частотно-временной	--	подставка под ТА
РК1235-5	10	цифровой	450x110x33	в дипломате
УГРА	2,5 x 10	цифровой	200x250x65	

9.7.6. Устройства уничтожения закладок

Данные устройства носят название ’’телефонные киллеры.’’

Эти устройства подают в телефонную линию высоковольтные импульсы (порядка 1500 В), которые выжигают закладки. Существенным недостатком этих устройств является то,

что необходимо очень точно выполнять инструкцию по их использованию, иначе можно выжечь и свои телефонные аппараты, файлы, модемы и АТС. При их использовании обычно телефонная линия отключается от АТС в коммутационной коробке. Примерами таких устройств являются Bugroaster, Кобра, КС-1300; ПТЛ-1500.

10. ЭЛЕКТРОСЕТЕВОЙ КАНАЛ УТЕЧКИ ИНФОРМАЦИИ

10.1. Особенности передачи сигнала по электросетевому каналу

Провода электросети могут успешно использоваться для скрытой передачи информации от радиозакладки. Обычная закладка дополняется устройством согласования с сетью и подключается прямо в линию электросети. Информация снимается приёмником с линии электросети.

Электросеть имеет очень малое активное сопротивление, но оно не закорачивает “радиозакладку”, так как подводящие провода имеют большую длину и, соответственно, большую индуктивность.

Электросетевые закладки обладают рядом существенных *преимуществ* по сравнению с другими видами закладок. По сравнению с радиозакладками – повышенной скрытностью (так как эти устройства невозможно обнаружить с помощью радиоприёмных устройств), а также неограниченным сроком работы, так как не требуется замены источников питания. Электросетевые закладки по сравнению с проводными микрофонами обеспечивают большую безопасность для агента, так как невозможно точно установить место установки приемного оборудования. По сравнению с телефонными ретрансляторами электросетевые закладки обеспечивают возможность передачи больших мощностей, так как ток потребления из сети не ограничен.

Недостатки рассматриваемых устройств следующие.

1. Необходимость проведения работ на объекте по скрытному подключению к сети 220В.
2. Возможность работы только в пределах одной фазы до ближайшей трансформаторной будки, так как трансформаторы силовой сети не пропускают высокочастотный сигнал.
3. Высокий уровень сетевых помех.
4. Возможность случайного отключения части силовой цепи потребителем.

Радиозакладки обычно изготавливаются двух типов:

- низкочастотные (несущая частота < 300 кГц);
- высокочастотные (несущая частота десятки МГц).

Сигналы с низкой несущей частотой имеют следующие достоинства по сравнению с высокочастотными:

- большая дальность распространения, чем у высокочастотных, так как потери в линии из-за ее сопротивления $X_L = j\omega L$ меньше;
- большая скрытность, так как их излучение не может контролироваться обычными приемниками, спектр работы которых начинается с 500 кГц.

Недостатком сигналов с низкой несущей частотой является то, что по одной фазе можно передавать только один сигнал с места контроля, в то время как у устройств с высокой несущей частотой по одной фазе можно передавать несколько сигналов на разных частотах.

10.2. Низкочастотное устройство съема информации

Устройство (рис. 10.2) состоит из блока питания, предварительного усилителя сигнала с микрофона, генератора и усилителя мощности.[13] Для питания устройства

используется промышленная сеть 220 В. Это напряжение выпрямляется мостом КЦ407, фильтруется RC-фильтрами
R3-C4, R6-C7, R13-C11. Стабильность напряжения обеспечивается за счёт применения стабилитронов VD2, VD3 и светодиода VD4. Предварительный усилитель сигнала с микрофона МК выполнен на транзисторе VT2. Сигнал с коллектора усилителя подаётся через конденсатор C9 на задающий генератор DD1.Задающий генератор выполнен на микросхеме DD1 по схеме мультивибратора. Напряжением U_0 можно изменять напряжение на входах DD1.3 и DD1.4, а, следовательно, изменять их момент открывания, т.е. можно изменять частоту генератора. В связи с тем, что частота сигнала с микрофона значительно меньше частоты генератора, то сигнал с усилителя VT2 (рис. 10.2) можно рассматривать как дополнительное медленное изменение U_0. Следовательно, сигнал с микрофона обеспечивает частотную модуляцию генератора.

Усилитель мощности собран на транзисторе VT1, его нагрузкой является контур, состоящий из индуктивности первичной обмотки трансформатора Тр1 и конденсатора C2. Применение резонансного контура позволяет получить синусоидальный сигнал; отсутствие гармоник обеспечивает трудность обнаружения на более высоких частотах. Через трансформатор Тр1 сигнал генератора подается в сеть 220 В и принимается приемником, подключенным к этой же сети.

Приведём недостающие данные, не указанные в схеме. Трансформатор Тр1 выполнен на кольцевом сердечнике К12х7х3 мм марки 600НН; первичная обмотка намотана проводом ПЭВ диаметра 0,1 мм и имеет число витков
W_1 = 100; вторичная обмотка намотана проводом в изоляции диаметра 0,15...0,3 мм и имеет число витков W_2 = 20. Примерами низкочастотных устройств съёма информации могут служить изделия IPS MCX (f=120 кГц, габариты 33X67X21 мм), Mode SIM – ACC (f=140 кГц, 24X9X7 мм).

Диапазон частот низкочастотных устройств находится в пределах от 50 кГц до 300 кГц. При меньших частотах сильно сказываются сетевые помехи; при больших резко возрастает затухание в проводах и, кроме того, они становятся радиоизлучателями, что сводит на нет преимущества по скрытности [13].

10.3. Высокочастотное устройство съёма информации

Питание передатчика (рис. 10.3) осуществляется от сети 220 В; для гашения излишков напряжения используется конденсатор C8; в отличие от резистора он не нагревается и не выделяет тепло, что благоприятно влияет на режим передатчика [13]. Однополупериодный выпрямитель собран на диодах VD3 и VD4, сглаживание пульсации обеспечивается конденсатором C7. В связи с тем, что в этой цепи действует высокое напряжение 220 В, необходимо выбирать диоды VD3, VD4 и конденсаторы C8, C9 с рабочим напряжением ≥ 330 В, а при настройке и эксплуатации устройства особое внимание уделить технике безопасности. Постоянное напряжение
с конденсатора C7 подается на параметрический стабилизатор R5, VD2, C6, обеспечивающий стабильное напряжение 9 В при колебаниях сети от 80 до 260 В. Резистор R1 и светодиод VD1 используются для получения необходимого режима питания микрофона.

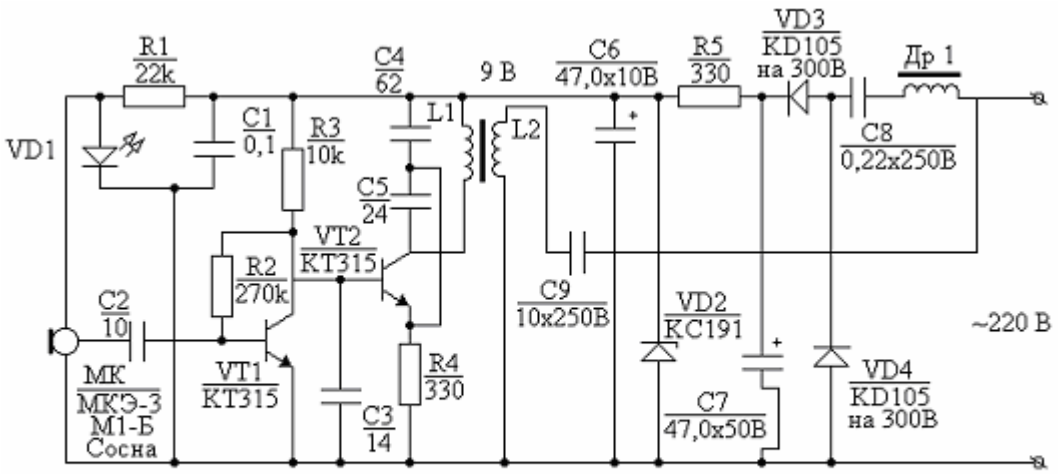


Рис. 10.3

Сигнал с микрофона подается на усилитель низкой частоты, выполненный на транзисторе VT1; резистор R2 предназначен для установки режима по постоянному току (напряжение на базе VT1 устанавливается равным 3,5 В). Сигнал с выхода УНЧ поступает на генератор VT2, собранный по схеме емкостной трёхточки, и изменяет напряжение на базе VT2. Изменение последнего приводит к изменению тока покоя I транзистора VT2, а, следовательно, к изменению его крутизны S ($S = I/U_T$, где U_T = 26 мВ – термическая разность потенциалов при температуре 300^0 К). Изменение S приводит к амплитудной модуляции (АМ)сигнала высокочастотного генератора (см. рассмотренные ранее принципы АМ). Частота генератора определяется параметрами L1, C4 и C5 (f = 27...30 МГц). С контура генератора сигнал через индуктивность L2 и конденсатор C9 подаётся в сеть 220 В, провода которой используются в качестве линии передачи.

Для того чтобы высокочастотный сигнал не попадал в источник постоянного напряжения, в схему введен дроссель Др1 с индуктивностью 50...90 μГн (дроссель можно намотать также на ферритовом стержне ∅2,8 мм, l = 14 мм, W = 100...150 проводом ПЭВ 0,1 мм). Недостающие параметры элементов следующие: индуктивности L1 и L2 намотаны на стандартном ферритовом стержне ∅2,8 мм, l = 14 мм проводом ПЭП 0,23; W_1 = 14, W_2 = 3 с намоткой поверх индуктивности L1.

Прием передачи ведется на штыревую антенну или с подключением приемника в сеть через адаптер (рис. 10.4). Адаптер подключается к сети через конденсатор C1 и представляет собой 2-х контурный фильтр сосредоточенной селекции, состоящий из контура L2, C2, связанного через конденсатор C3 с контуром L3, C4. Сигнал снимается с индуктивности L4 и через конденсатор C5 подается на вход приемника.

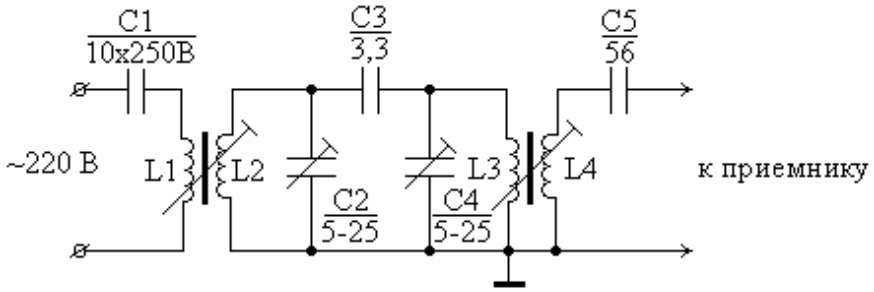


Рис. 10.4

Индуктивности намотаны на каркасах катушек коротковолнового диапазона обычного приемника проводом ПЭВ 0,23 и имеют следующее число витков: $W_1 = 2$; $W_2 = W_3 = 14$; $W_4 = 4$.

Примером высокочастотного устройства съёма информации может служить изделие SIM – SCB (f=7 кГц, 30X30X8 мм)

10.4. Деконспирационные признаки

Деконспирационными признаками являются:

1. Наличие в силовой сети сигналов несущей частоты.
2. Наличие электронного изучения на высокой несущей частоте около проводов электросети (этот способ обнаружения подслушивающих устройств не используется, так как внешние помехи значительно выше излучения применяемых устройств).

10.5. Системы защиты от утечки по электросетевому каналу

Обнаружение подслушивающих устройств производится на основе анализа вида сигнала в сети 220 В. Структурная схема системы обнаружения приведена на рис. 10.5.

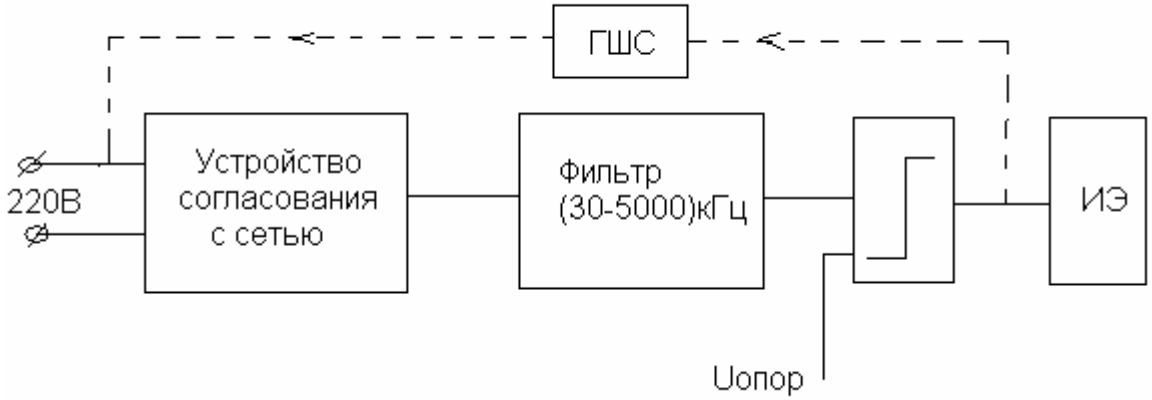


Рис.10.5.

К сети 220 В через согласующее устройство подключается фильтр с полосой пропускания от 30 до 5000кГц. При работе подслушивающих устройств на выходе фильтра появляется сигнал. При его достаточном уровне компаратор срабатывает и включает исполнительный элемент ИЭ, включающий световую и звуковую сигнализацию. По указанной структурной схеме выпускается изделие ШТРАФ фирмы ЩИТ. Это изделие обнаруживает сигналы в сети с уровнем ≥ 100 мВ [3]. Для предотвращения возможности съёма информации по цепи 220 В используется изделие ШПАГА фирмы ЩИТ. Принцип работы этого изделия аналогичен работе изделия ШТРАФ. Дополнительным устройством является формирователь шумового сигнала, генерирующий шум в сеть при срабатывании компаратора (рис. 10.5. пунктир).

11.ВИЗУАЛЬНЫЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

Для получения видовых характеристик объектов широко используются:

- бинокли;
- фотоаппараты, камуфлированные под бытовую технику;
- телескопы (фотоаппараты с телеобъективом; позволяют получать качественные фотоснимки с расстояния до 10 км [1]; размеры телескопа 46.0 х 112 см²; вес 54 кг);
- приборы ночного видения;
- телевизионные системы наблюдения.

Принцип получения видовых изображений с помощью биноклей, фотоаппаратов и телескопов понятен. Поэтому остановимся на принципах работы приборов ночного видения и телевизионных систем наблюдения.

11.1. Приборы ночного видения

В темноте человеческий глаз практически ничего не видит. Для наблюдения объекта его надо подвесить, но обычная световая подсветка выдаёт агента. Спектральная чувствительность глаза
в относительных единицах приведена на рис.11.1.

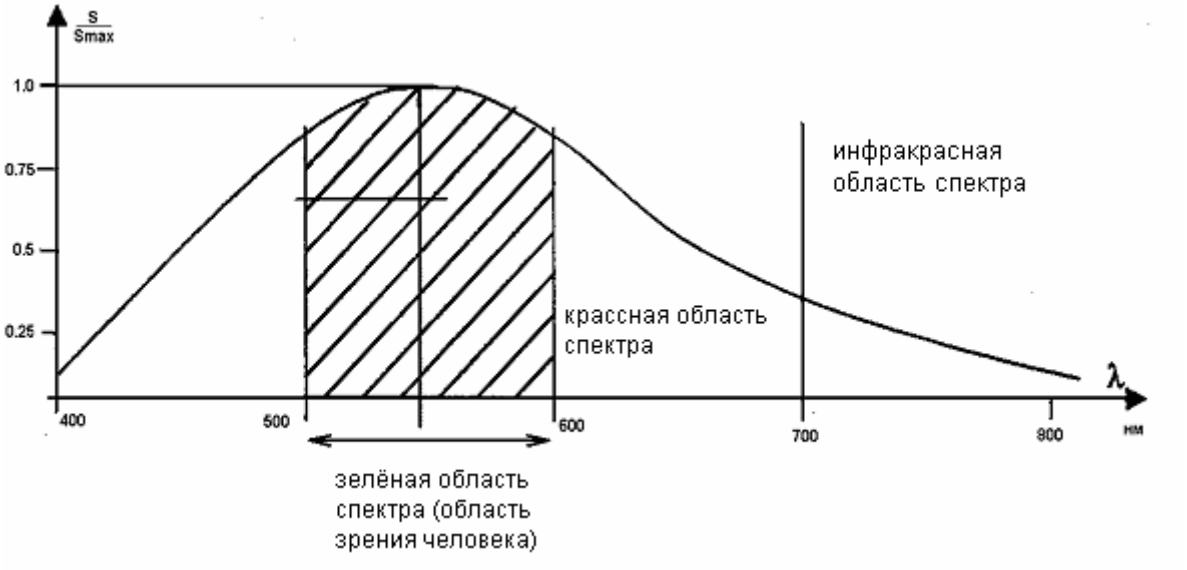


Рис.11.1

Для того, чтобы человек не видел подсветки, необходимо объект подсветить лучами невидимыми для глаза; отражение от объекта происходит теми же лучами. Поэтому отраженный луч нужно затем преобразовать в видимый спектр. Структурная схема такого устройства приведена на рис.11.2.

Тепловизор состоит из излучателя и приёмника. Лазерный диод VD1 с целью увеличения контрастности изображения запитывается пульсирующим напряжением (частота коммутации напряжения 2÷15 Гц). Диод излучает инфракрасные лучи в диапазоне 820÷980 нм ($I_{пит}$=100÷160 мА, $P_{изл}$=20÷40 мВт); эти лучи фокусируются оптическими линзами и направляются на объект, подсвечивая его в невидимой инфракрасной области. Для наблюдения на небольших расстояниях используются широкоугольные объективы (угол поля зрения 30÷60º). Для наблюдения на больших расстояниях берётся объектив с углом поля зрения 5÷15º; ИК прицелы имеют угол поля зрения 0.01-0.5º. Отраженный от объекта луч

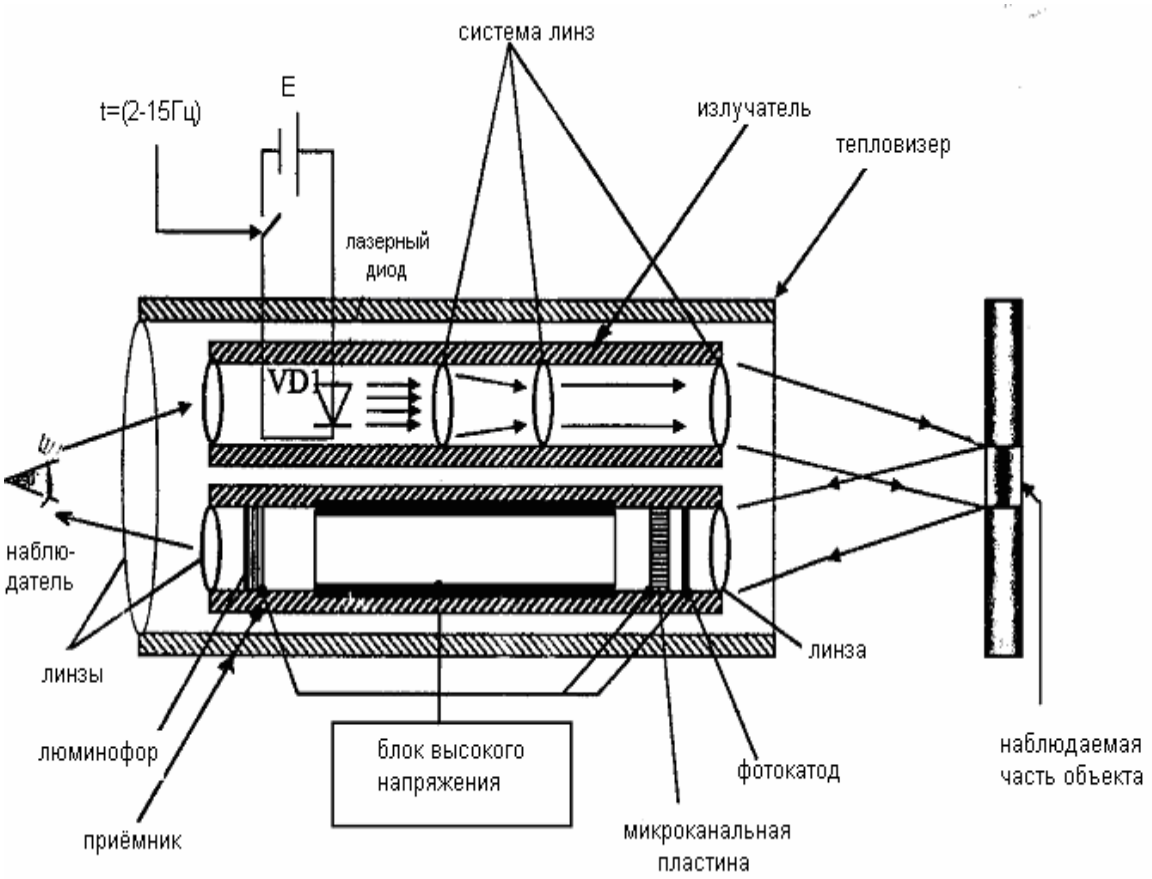


Рис. 11.2

попадает на фотокатод приёмника (его максимальная чувствительность лежит в ИК зоне); затем, для увеличения чувствительности, луч подается на микроканальную пластину. Это матрица микроскопических полых диэлектрических каналов со специальным покрытием стенок. За счёт этой пластины чувствительность увеличивается примерно в 10 раз. В ней происходит умножение электронов, которые затем фокусируются и приобретают скорость из-за имеющегося высоковольтного поля; далее, ускоренные электроны попадают на люминофор со свечением в зеленой области.

Таким образом, подсветка в ИК области преобразуется в изображение в видимом спектре. По данным работы [9] угол расхождения лучей составляет 0.02÷0.06º при наблюдении на расстоянии до 500м.

Недостатками приборов ночного видения ПНВ являются:

1. близость их максимальной спектральной чувствительности (λ=820нм) к зеленой области спектра. Это приводит тому, что подсветки на фотокатод от фар машин, огней города и т. п. значительно снижают контрастность изображения.
2. Возможно обнаружить ПНВ не только другими ПНВ, но и человеческим глазом, если на зрачок попадает не рассеянный ИК луч, а концентрированный луч от ПНВ.

11.2. Телевизионные системы наблюдения

Для съема информации часто используются скрытые системы телевизионного наблюдения. Структурная схема системы приведена на рис.11.3.

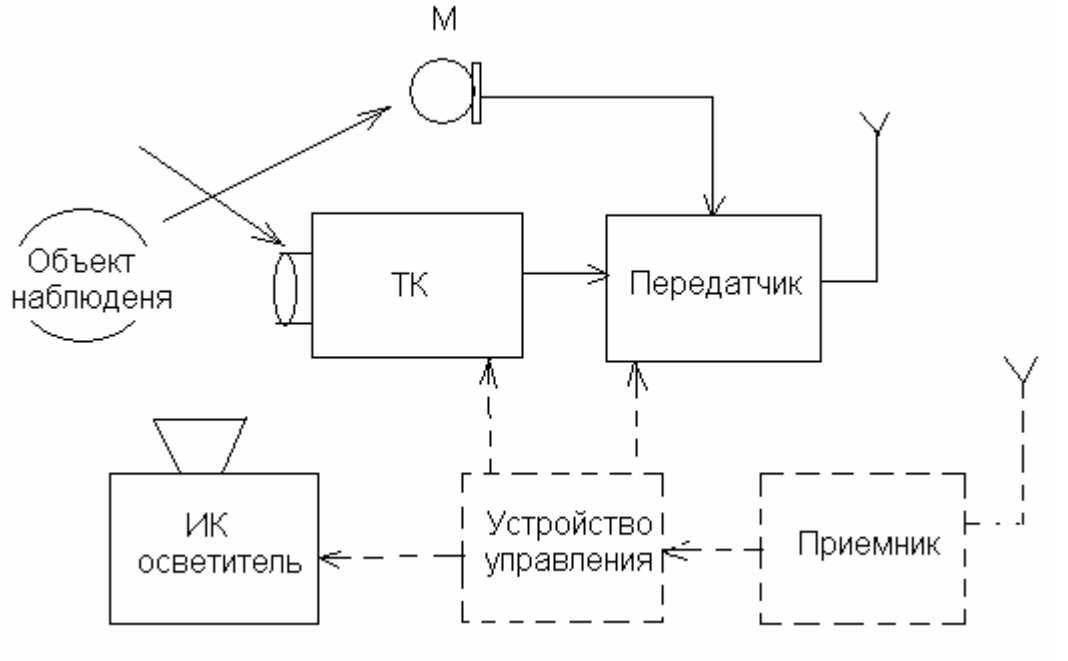


Рис.11.3

Система состоит из передающей телевизионной камеры ТК, сигнал с которой через передатчик излучается в эфир. Для обеспечения съёма информации в темноте используется инфракрасный осветитель (типовой ИК осветитель с длиной волны λ=870 нм, током потребления I=600 мА обеспечивает подсветку на расстоянии до 4 м, при этом чувствительность ТК повышается до 0.04лк, то есть до чувствительности человеческого глаза). Применение микрофона М позволяет передавать акустическую информацию о событиях в помещении. Дальность передачи зависит от диапазона и мощности используемых передатчиков. Включение всей системы возможно от детекторов движения с выносного пульта. Для этого в систему вводится приёмник и устройство управления. Размеры ТК настолько малы, что эти устройства можно камуфлировать в обычные бытовые предметы (книга, ваза, картина в рамках и т.д.) Например, в работе [9] приводятся следующие данные о системе OV3-25-5: Информация снимается через отверстие мене 1 мм, разрешение камеры составляет 380 линий, чувствительность 0.5 лк, передача ведётся на частотах (400÷500МГц, с мощностью 40 мВт), объектив имеет автоматическую регулировку диафрагмы. При таких высоких показателях устройство характеризуется малым потреблением мощности (питание от источника 12 В, ток потребления 120 мА), малыми габаритами (3.8х4.5х5.9см³) и малым весом (120г). В работе не указана стоимость устройства, однако по данным обзора технической литературы можно вывести среднюю стоимость: стоимость ТК с передатчиком – приблизительно 430 $, сверхчувствительного микрофона 42 $, ИК подсветки – 40 $. Возможно передать сигнал от ТК не через передатчик,

а просто через сеть 220 В. Использование силовой сети объекта позволяет отказаться от внутренних источников питания и большой антенны

(см. раздел радиозакладок). Схема адаптера для приема телевизионных сигналов по силовой цепи с настройкой на фиксированную частоту приведена на рис. 11.4. Сигнал с ТК агента через емкости прямо передаётся в сеть 220 В.

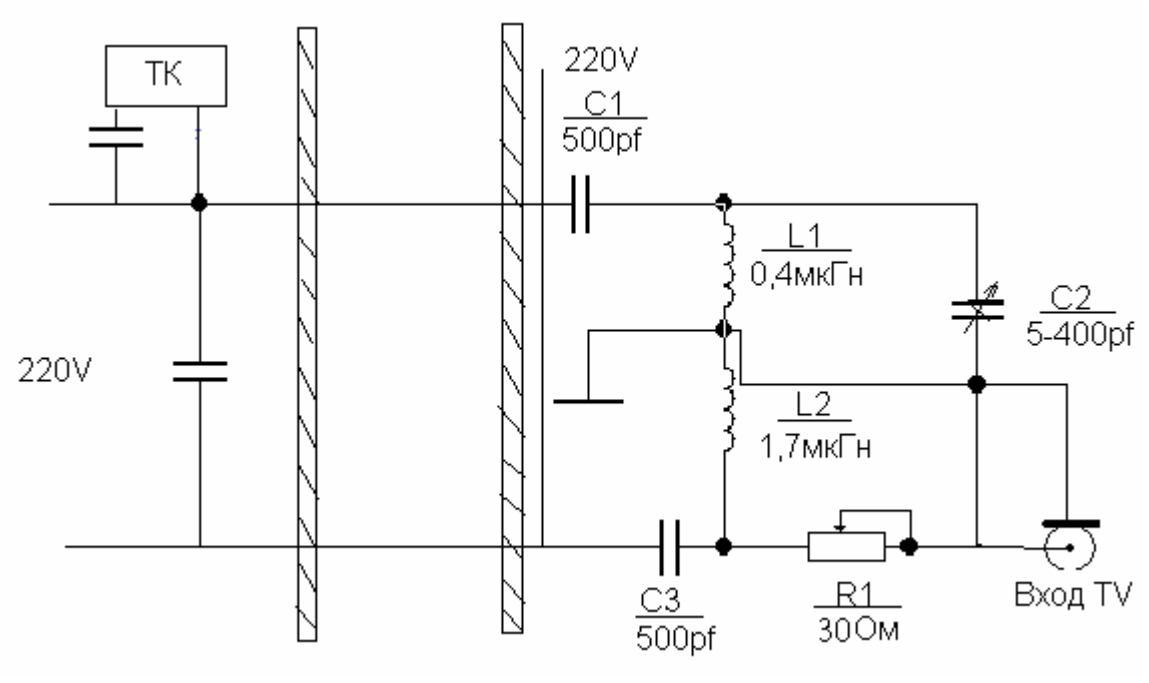


Рис.11.4

Для того, чтобы сигнал 220 В частотой 50 Гц не проходил на вход TV приемника применяется фильтр C1,L1 и C3,L2; конденсатор C2 обеспечивает настройку на заданную частоту. Использование светодиодов позволило создать гибкие приборы наблюдения, которые можно вводить в комнату через любые небольшие отверстия (замочную скважину, отверстия для труб и т. д.) и получать визуальную информацию о том, что происходит в комнате.

12. ПОИСК СРЕДСТВ НЕСАНКЦИОНИРОВАННОГО СЪЁМА ИНФОРМАЦИИ

Правовая основа проведения мероприятий по выявлению средств несанкционированного съёма информации (СНСИ) базируется на Федеральном законе “Об информации, информатизации и защите информации”. Степень защиты коммерческой информации и степень поиска СНСИ выбирает руководитель предприятия.

При проведении мероприятий по поиску СНСИ основными вопросами являются:

- что защищается?
- от кого защищается?
- какими силами и какие объёмы средств финансирования выделяются на поиск?

Что защищать? Обсуждаемая дисциплина «Технические средства защиты информации» рассматривает вопросы защиты только коммерческой тайны. Перечень сведений отнесённых к понятию “коммерческая тайна” и приоритетность этих сведений рассмотрены в гл. 2 данного пособия. В принципе, можно защищать всё и везде, но это будет стоить безумно дорого. Поэтому надо обследовать только ту часть фирмы (персонал, каналы связи, физическая площадь), где циркулирует важная информация. Понятно, что стоимость обследования, например, десяти или одной комнаты существенно отличаются.

От кого защищать? Правильное определение противника позволяет реально оценить его финансовые, оперативные и технические возможности. Заранее в качестве противника принимать суперпрофессионала не имеет смысла (это не государственная разведка), так как для борьбы с ним нужна мощная и разнообразная техника и,

соответственно, затраты на обследование будут велики. Обычно против крупных корпораций используют изощрённую технику (она и оплачивается дороже), а против фирм малого бизнеса более простые устройства, например радиомикрофоны. В подавляющем большинстве случаев сам руководитель предприятия определяет своего потенциального противника, так как он обладает наибольшей информацией о работе своего и конкурирующих предприятий. Зная противника, можно заранее прогнозировать применение конкретных типов СНСИ. Кроме того, возможна и профилактическая проверка помещений.

Какие силы и какое финансирование выделять на поиск? Руководитель предприятия совместно с руководителем службы безопасности определяют состав имеющихся у них средств для обнаружения СНСИ и компетентность сотрудников, способных работать в этой сфере. Если вопрос идёт о серьёзных угрозах, то, вероятно, лучше всего пригласить профессионалов, имеющих соответствующие лицензии.

Рассмотрим рекомендации по поиску СНСИ [5,21]. В соответствии с рекомендациями работы [21] процесс поиска можно разбить на несколько этапов:

- подготовительный этап;
- этап поиска СНСИ;
- заключительный этап.

12.1. Подготовительный этап

Этот этап определяет замысел проведения операции. В состав замысла проведения операции входят:

- ранее определённые руководителем предприятия *масштаб и стоимость поиска;*

- *уточнение деталей поиска* с представителями фирмы противопромышленного шпионажа;

- *легенда,* под прикрытием которой проводится скрытность операции; появление новых людей, развёртывание аппаратуры, характерный шум при поиске не должен настораживать возможного замаскированного осведомителя; в качестве легенды можно использовать [21] проверку телефонистами телефонных линий, проверку состояния охранной, пожарной сигнализаций, заземления, состояния отопительной системы, водопроводных и других инженерно-технических коммуникаций;

- *выбор времени* проведения поиска. Поиск рекомендуется проводить в рабочее время с имитацией правдоподобных важных деловых переговоров. Речь в помещении включает СНСИ, срабатывающую от определённого уровня акустического сигнала. Имитация переговоров, вполне вероятно, заставит противника включить дистанционно управляемые закладки.

Таким образом, правильный выбор времени проведения поиска значительно повысит вероятность обнаружения СНСИ.

- *предварительный осмотр объекта;*

В результате изучения строительных документов и результата осмотра объекта у специалиста должно сформироваться представление о системе охраны, системе защиты информации, доступности рассматриваемого объекта для посетителей и персонала предприятия, об оборудовании, установленном в помещении, инженерно-технических коммуникациях, проходящих через объект, о конструктивных и других особенностях здания. В результате проведённого осмотра специалист решает вопрос

о возможности снятия информации без установки в помещение СНСИ; при этом особое внимание обращается на следующее:

- может ли постороннее лицо проникнуть в зону излучения оргтехники предприятия (напомним, что дальность перехвата излучения дисплеев с пластмассовым корпусом на открытой местности составляет 1200 м, а в городских условиях 50÷80м [21]);
- может ли агент установить стетоскоп на наружную поверхность здания с получением информации из помещения (важна конструкция здания);
- есть ли возможность доступа посторонних лиц к проводным коммуникациям, проходящим через подлежащее проверке помещение;
- есть ли возможность визуального и инфракрасного наблюдения событий в помещении с удалённых зданий, деревьев и т.д.;
- не может ли агент получить информацию за счёт структурных волн (гл. 3), используя конструкцию здания или проведя специфический ремонт здания.

Если такие места существуют, то в ходе поиска СНСИ они берутся под соответствующее наблюдение.

- *выбор аппаратуры для проведения поиска;*

для проведения поиска используем следующие средства:
- устройства визуального осмотра труднодоступных мест, предметов интерьера и т.д.;
- устройства поиска радиоизлучающих устройств;
- устройства проверки проводных коммуникаций.

Один из вариантов перечня поискового специального оборудования [21] приведён в таблице 12.1.

Таблица 12.1

№ п/п	***Наименование оборудования и технических средств***	***Виды работ, при которых используются оборудование и технические средства***
1.	Комплект досмотровых зеркал (ПОИСК-2, ШМЕЛЬ-2)	Визуальный осмотр оборудования, мебели, технологических коммуникаций
2.	Комплект луп, фонарей.	Визуальный осмотр поверхностей и отверстий
3.	Технический эндоскоп с дистальным концом (серия ЭТ, Olimpus)	Визуальный осмотр труднодоступных полостей и каналов
4.	Комплект отвёрток, ключей и радиомонтажного инструмента	Разборка и сборка коммутационных, электроустановочных и других устройств и предметов
5.	Досмотровый металлоискатель (УНИСКАН 7215, АКА 7202, Comet)	Проверка предметов и элементов интерьера на наличие металлических включений
6.	Прибор нелинейный радиолокации (NR-900EM, ОРИОН NGE-400, РОДНИК 23)	Проверка строительных конструкций и предметов на наличие радиоэлектронных компонентов
7.	Переносная рентгенотелевизионная установка (ШМЕЛЬ 90/К, ФП-1, РОНА)	Проверка элементов интерьера на наличие скрытно установленных средств НСИ
8.	Переносный радиоприёмник или магнитола	Озвучивание проверяемых помещений
9.	Многофункциональный поисковый прибор (ПИРАНЬЯ, ПСЧ-5, D-008)	Проверка проводных коммуникаций на наличие информационных сигналов
10.	Низкочастотный нелинейный детектор проводных коммуникаций	Проверка проводных коммуникаций на наличие нелинейности параметров линии

	(ВИЗИР, возможная замена по телефонным линиям: ТПУ-6 или SELSP-18/Т)	
11.	Комплекс обнаружения радиоизлучающих средств и радиомониторинга (КРОНА-6000М, КРК, АРК-Д1, OSC-5000)	Анализ радиоэлектронной обстановки, выявление радиоизлучающих средств негласного съёма информации
12.	Обнаружитель скрытых видеокамер (IRIS VCF-2000, нет аналогов)	Выявление радиоизлучающих видеокамер
13.	Дозиметр поисковый (РМ-1401, НПО-3)	Обнаружение и локализация источников радиоактивного излучения
14.	Комплекс для проведения исследований на сверхнормативные побочные электромагнитные излучения (НАВИГАТОР, ЛЕГЕНДА, ЗАРНИЦА)	Выявление информативных побочных электромагнитных излучений
15.	Комплекс для проведения акустических и виброакустических изменений (СПРУТ-4А)	Выявление акустических и виброакустических сигналов и наводок, исследование звуко- и виброизоляции, проверка систем зашумления

- *Утверждения плана проведения проверки*
  План проведения проверки чаще всего выполняется в виде текстового документа. В этом документе указывается предполагаемый противник, легенда под прикрытием которой ведётся поиск, время поиска, аппаратура поиска, бригады поиска, график проведения работ, стоимость проверки. План утверждается руководителем предприятия.

12.2. Поиск средств несанкционированного съёма информации и использование возможных путей подавления этих средств

При написании этого параграфа используются данные, изложенные в работах [5,21] и даются ссылки на материалы, изложенные в предыдущих главах в параграфах “деконспирационные признаки” устройств.

Рассмотрим методы выявления следующих СНСИ:

- СНСИ, работающих с использованием естественного акустического канала, стетоскопов, а также с использованием проводных и направленных микрофонов;
- СНСИ, работающих в радиоэфире непрерывно и в ждущем режиме;
- СНСИ, установленных в проводных линиях связи (телефонный канал, силовая и осветительная сеть, пожарная и охранная сигнализация, иные виды сигнализации);
- СНСИ-диктофонов.

Для обнаружения всех вышеуказанных СНСИ (кроме первой) используются *два основных метода*:

- Метод поиска СНСИ физических объектов;
- Метод поиска СНСИ как электронного устройства.

12.2.1. Обнаружение СНСИ, использующих стетоскопы, направленные микрофоны, проводные микрофоны, естественные акустические полости в здании

Для обнаружения этих средств физический осмотр территории

и помещения является основой поиска. В соответствии с методикой, предложенной в работе [21], перед началом осмотра конкретного помещения рекомендуется внимательно осмотреть прилегающую к фирме территорию для обнаружения возможно развёрнутых там стетоскопов, направленных микрофонов и радиопунктов для прослушивания информации с радиозакладок. Особое внимание рекомендуется обращать на установленные на внешней стороне помещения какие-либо предметы (возможно стетоскопы), людей в наушниках с не совсем понятными большими предметами в руках (возможно в их руках находятся направленные микрофоны), на долго стоящие автомобили с людьми и с тонированными стёклами (возможно, идёт приём информации с радиозакладок). Следует записать номера автомобилей с последующим выяснением кому они принадлежат.

При визуальной проверке помещений с целью поиска волоконно-оптических проводных микрофонов следует приподнять плинтуса, ковры, паласы, линолеум и внимательно осмотреть пространство под ними.

Для обнаружения возможности просачивания звуковой информации через полости здания поисковая бригада знакомится с документацией на конструкцию здания, исследует вентиляционные короба, ниши, полости в здании и делает соответствующие выводы. Для проведения визуального осмотра в труднодоступных местах используется специальные фонари
и зеркала. Например: фонари Mag-Lite с регулировкой светового пучка от точечного до рассеянного; комплект досмотровых зеркал типа Поис-2, Шмель-3 и т.д.

Контроль труднодоступных мест часто осуществляется с помощью досмотровых портативных телевизионных установок. Портативные телевизионные системы позволяют сочетать высокое качество изображения с удобством пользования. Широкое применение нашли видеоустройства Альфа-4 и система S-1000 (“Кальмар”). Например,
в состав устройства Альфа-4 входят:

- чёрно-белая видеокамера с устройством инфракрасной подсветки, позволяющая досматривать объекты на удалении до 2,5 м;
- телескопическая штанга, через которую проходят провода от камеры и к которой крепится сама видеокамера;
- миниатюрный жидкокристаллический монитор, помещаемый в руке оператора;
- специальный жилет.

Недостатком устройств видеонаблюдения является необходимость длительной повышенной сосредоточенности оператора при досмотре.

12.2.2. Поиск СНСИ, работающих в радиоэфире

В соответствии с рекомендациями работы [5] обнаружение внедрённых закладных устройств (ЗУ) осуществляется с помощью двух методов (рис. 12.1), а именно методы поиска СНСИ как физических объектов и метода поиска СНСИ как электронных устройств.

Первая группа – методы, основанные на поиске ЗУ как физических объектов с вполне определёнными свойствами и массогабаритными характеристиками.

К ней относятся:

- визуальный осмотр мест возможного размещения ЗУ, в том числе с применением увеличительных стёкол, зеркал, средств специальной подсветки;
- контроль труднодоступных мест с помощью средств видеонаблюдения;
- применение металлодетекторов.

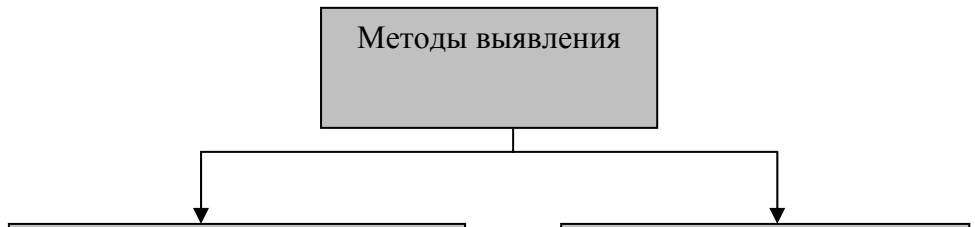


Рис. 12.1

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 радиоприёмных устройств (панорамных приёмников), предназначенных для поиска сигналов по заданным характеристикам с учетом анализа электромагнитной обстановки;
- применение комплексов радиоконтроля и выявления ЗУ;
- обследование помещений с помощью нелинейных радиолокаторов, позволяющих выявлять любые типы ЗУ;

12.2.1.1. Методы поиска ЗУ как физических объектов

Часть принципов поиска ЗУ как физических объектов такая же, как изложенная в п. 12.2.1. Дополним предыдущий подпункт некоторыми рекомендациями специфическими для поиска ЗУ [21]. Рекомендуется при поиске ЗУ обратить внимание на следующее:

- на изменение внешнего вида стен, пола, потолка помещения (следы недавней заделки отверстий, оштукатуривания или свежей окраски части поверхности наводят на мысль о возможности установки СНСИ);
- на следы вскрытия съёмных элементов конструкции помещения, а именно: декоративных стеновых панелей, подвесных потолков, элементов пластиковых оконных рам, плинтусов и наличников, напольных покрытий, элементов декора;
- на смещение предметов, покрытий и мебели с их обычных мест;

- на необходимость особо тщательного осмотра радиаторов системы парового отопления; сложные конструкции радиаторов создают благоприятные условия для установки СНСИ; кроме того, наличие металла и металлических соединений приводят к невозможности обнаружения СНСИ с помощью металлодетекторов и нелинейных локаторов;
- на необходимость детального осмотра кресла, стола и шкафа руководителя фирмы, а так же сейфа, холодильника и стола для проведения переговоров. Именно в эти места чаще всего устанавливаются СНСИ. Особое внимание следует уделить наличию на стандартных канцелярских изделиях инвентарных номеров (в случае их отсутствия это указывает на возможность подмены), целостности пломб и отсутствие следов сверления;
- на необходимость исследования телефонного аппарата, а именно его разборки и проверки линии связи до телефонной коробки

Осмотр мест возможного размещения ЗУ осуществляется с помощью зеркал, подсветки и средств видеонаблюдения. Специфической характеристикой поиска является возможность поиска ЗУ как металлического изделия. Наличие металлических экранов и металлических элементов в ЗУ позволяет применять для их обнаружения металлодетекторы.

Металлодетекторы представляют собой сочетание образцового генератора и генератора, частота которого изменяется при приближении его поисковой катушки к металлу. При наличии металла в радиусе действия поисковой катушки возникает разность частот двух генераторов, что приводит к возникновению звукового сигнала в наушниках. Существует большое количество разновидностей металлодетекторов. Приведём характеристики одного из них [5]: СТЕРХ-92АР-металлодетектор, предназначенный для поиска металлических предметов
в диэлектрических и слабопроводящих средах. Максимальная дальность обнаружения металлических предметов: 250 мм - диск 20х1 мм; 600мм – пластина 100х100х1мм. Питание – “Крона” 9В. Достоинством применения металлодетекторов является отсутствие необходимости повышенного внимания при досмотре. Только когда слышится звуковой сигнал, оператор повышает внимание и более медленно и пунктуально исследует подозрительную область. Одним из основных достоинств металлодетекторов является возможность обнаружения с их помощью радиозакладок (на КМОП элементах), работающих в ждущем режиме. Если такие радиозакладки находятся в экранирующем (металлическом) корпусе, то даже очень дорогие устройства нелинейной радиолокации не способны их обнаружить; металлодетектор же обнаруживает металл экрана. Недостатком металлодетекторов является необходимость изъятия всех бытовых металлических изделий из области обследования.

Тщательный поиск СНСИ как физических объектов [21] может выявить практически все типы подбрасываемых СНСИ и подавляющее большинство СНСИ, требующих незначительного времени для их установки. Для некоторых видов СНСИ данный вид поиска является единственным способом их обнаружения. “Вместе с тем он весьма трудоёмок и требует разборки, а иногда и разрушительного вмешательства в предмет или конструкцию для снятия возникших подозрений, поэтому визуальный осмотр целесообразно сочетать с применением специальной аппаратуры неразрушающего контроля подозрительных мест.”

12.2.2.2. Методы поиска радиозакладок как электронных устройств

СНСИ в большинстве случаев представляет собой сочетание электронных устройств. Эти устройства могут работать непрерывно,

а могут включаться голосом или в определённое время дистанционно. Обнаружение непрерывно работающих СНСИ проще, чем периодически включаемых. Работающее СНСИ создаёт электромагнитное поле, которое передаётся или по радиоканалу или по проводным коммуникациям.

Проверку помещения [21] следует проводить в соответствии с используемой легендой и так, чтобы это не насторожило противника. Перед началом поиска включаются все офисные устройства, тем самым осуществляется перевод в рабочее состояние возможно внедрённых в них СНСИ. Кроме того, в помещении создаётся звуковой фон в виде предварительно записанного на магнитофон доклада, семинара и т.д., не вызывающих настороженности у подслушивающего противника. Звуковой фон решает сразу несколько задач:

- активизация СНСИ, включаемых голосом;
- маскировка звуков от поисковой аппаратуры (например, от излучающих нелинейных локаторов);
- обеспечение работы части поисковой аппаратуры, использующей эффект “звуковой обратной связи”.

Методика поиска СНСИ в разных каналах утечки информации во многом одинакова и, соответственно, для поиска может быть использована одна и та же аппаратура. Рассмотрим вначале методы поиска работающих СНСИ, а затем выключенных СНСИ.

В качестве примерной последовательности производимых *действий по выявлению работающих радиозакладок* можно порекомендовать следующий порядок [5]:

- разместите поисковый прибор в центре контролируемого помещения, установите антенну, оденьте наушники;
- установите регулировки в такое положение, чтобы индикатор поискового прибора показывал среднее значение;
- выключите всю аппаратуру и свет в зоне контроля и близ неё и посмотрите, не изменились ли показания индикатора поискового прибора.
- При изменениях в показаниях индикатора прибора возникает подозрение, что была временно отключена радиозакладка. Надо дополнительно исследовать то изделие, что вызвало изменение показаний. Это может быть или радиозакладка или шумящее изделие;
- 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.

Если информация снимается с микрофона телефона или с телефонной линии с последующей передачей информации в радиоэфир, то для поиска такой закладки производится сканирование эфира вначале при положенной трубке телефонного аппарата, а затем при снятой. При наличии закладки и поднятии трубки в эфире появляется новая станция (или увеличивается уровень излучения) и в наушниках поискового приёмника прослушивается тональный сигнал номеронабирателя и звук в помещении. При отсутствии закладки и поднятии трубки в наушниках будет прослушиваться только короткий щелчок.

В последнее время в качестве СНСИ стали часто использоваться видеокамеры. Сигнал от камер очень слаб и его очень трудно выделить сканирующими приёмниками. В то же время этот сигнал обладает рядом специфических особенностей, таких как наличие синхроимпульсов, специфический спектр сигнала и т.д. Использование этих особенностей легло в основу разработки программно-аппаратных комплексов обнаружения. Например, комплексы OSCOR OSC-5000 Deluxe или КРОНА-6000М обеспечивают автоматическую идентификацию сигналов видеокамер с возможностью просмотра передаваемого видеоизображения [21]. Местоположение закладки определяется сканированием антенной различных точек помещения с получением максимального значения сигнала.

Использование ИК диапазона для съёма информации хоть и встречается, но достаточно редко. ИК или лазерные излучающие диоды устанавливаются противником около стеклянных проёмов. Их луч направленный на стекло модулируется вибрацией стекла от человеческого голоса, отражается от стекла и ловится приёмным устройством нарушителя. Поиск этих СНСИ осуществляется физически или зондами-детерторами ИК-излучений, входящими в состав некоторых радиоэлектронных комплексов. Местоположение диода определяется по повороту антенны комплекса (или частичному перекрытию зоны приёма) и максимуму приёма. Зонды-детекторы входят в состав комплексов ПИРАНЬЯ, OSCOR OSC-5000 и др.

Иногда *сигналы СНСИ маскируются под излучения официальных радиостанций*. Такую закладку достаточно трудно найти. Рекомендуемая методика обнаружения [21] следующая:

- проводить сканирование эфира днем и ночью;
- обратить внимание на появление сигнала вне обычного для него расписания;
- обратить внимание на внезапное возрастание уровня сигнала (при включении закладки к уровню сигнала официальной станции добавляется сигнал от СНСИ);
- обратить внимание на расширение спектра сигнала (кроме случаев с кодируемой модуляцией).

Поиск обесточенных радиозакладок производится с помощью визуального осмотра, нелинейного радиолокатора и металлодетектора.

Вопросы визуального осмотра рассмотрены нами раньше. Принципы работы металлодетектора и нелинейного радиолокатора рассмотрены в п.12.2.2.1 и в п. 8 . Методика поиска СНСИ с помощью радиолокатора и металлодетектора во многом одинакова. Предварительно из зоны поиска удаляются металлические предметы (для работы металлодетектора)
и предметы, содержащие радиоэлементы, в том числе и другие поисковые устройства (для работы нелинейного радиолокатора). Антенна поискового прибора вручную перемещается над поверхностью обследуемого предмета. На наличие в зоне поиска предполагаемого СНСИ указывает характерный звуковой сигнал и показания светового индикатора.

Перемещение антенны рекомендуется проводить по спирали
с одновременным смещением центра спирали (например, слева направо) для просмотра всей поверхности объекта. Скорость перемещения антенны локатора (при благоприятных условиях) около 2 $м^2$ поверхности за секунду [21], глубина зондирования 20÷35см. Основной проблемой поиска с использованием нелинейных радиолокаторов являются ложные срабатывания, вызванные наличием естественных (не радиотехнических) нелинейных элементов, а именно местами соединения двух металлов и коррозийными металлическими конструкциями. В простых дешёвых радиолокаторах приём отражённого сигнала производится только на одной гармонике. Для распознавания вида отражённого сигнала оператор мягким молотком стучит по подозрительному месту. Если в этом месте находится радиотехнический нелинейный предмет, то контакт внутри такого элемента не нарушается. Если это естественный нелинейный элемент, то при ударах контакт элементов нарушается и в наушниках оператора прослушивается треск и шорох. Проблема распознавания облегчена в приборах, обеспечивающих анализ отражённого сигнала сразу на 2-ой и 3-ей гармониках. Если амплитуда 2-ой гармоники больше 3-ей, то в зоне облучения находится электронный нелинейный элемент; если наоборот, то это ложный сигнал. При обнаружении отклика на зондирующий сигнал мощность передатчика и чувствительность приёмника постепенно снижают для более точной локализации источника обнаруженного сигнала. Решение о вскрытии предмета или элемента конструкции для изъятия возможной радиозакладки принимает руководитель предприятия по представлению поисковой бригады. Обычно перед принятием решения

проводится дополнительное обследование скрытого в предмете или стене объекта с помощью флуороскопа или рентгенотелевизионного устройства.

Для применения этих устройств необходимым условием является доступность обеих сторон исследуемого объекта. Методика работы следующая:

- передатчик (рентгеновский аппарат или радио-нуклидный источник гамма-излучения) и устройство визуализации (рентгено-телевизионный преобразователь) помещают по разные стороны от объекта в зоне действия прямого пучка излучения;
- удаляют посторонних из зоны облучения, выполняют правила мер безопасности при работе с рентгеновским оборудованием;
- сравнивают полученное изображение с базой данных разных изображений и делают соответствующие выводы.

Часть специалистов [8] считают, что приборы нелинейной радиолокации обеспечивают почти 100% гарантию выявления
в помещении скрытых радиоэлектронных устройств. К сожалению, приборы нелинейной радиолокации имеют ряд существенных недостатков [5,21]:

- для устранения ложных сигналов вся радиоаппаратура должна быть вынесена за пределы исследуемого помещения;
- закладки на КМОП элементах, помещенные в экранирующий корпус, почти не обнаруживаются нелинейными радиолокаторами. Их поиск осуществляется визуальным способом, металлодетекторами (определяющими экранированные корпуса) и непрерывным обзором и регистрацией работающих и вновь появляющихся радиостанций. Появление в эфире новой радиостанции (особенно, если это спровоцировано проведением на подслушиваемой территории очень важного совещания) указывает на работу СНСИ, работающего в дежурном режиме. При выходе информации в эфир СНСИ обнаруживается методами характерными для обнаружения непрерывно работающих СНСИ.

Наиболее труден *поиск радиозакладок, внедрённых в электронные приборы*. Электронные приборы позволяют легко решить проблему электропитания СНСИ, обеспечивают простоту маскировки закладок, камуфлированных под конденсаторы, фильтры, реле и т.д. Многие электронные приборы сами по себе являются устройствами сбора, обработки и передачи информации, то есть излучают радиосигналы. Обнаружение закладок в приборах возможно только частью поисковой аппаратуры. Применение металлодетекторов и устройств нелинейной радиолокации, обнаруживающих радиозакладки, работающие в ждущем режиме, неэффективно так как электронный прибор сам по себе начинён нелинейными электронными и металлическими элементами. Если поисковая аппаратура показала, что есть подозрения, что радиозакладка находится в электронном приборе, то рекомендуется следующая методика поиска [21]:

- «поиск информативных сигналов на всех входах и выходах прибора, подключаемых к внешним проводным линиям, включая линию электропитания прибора (методика проверки излагается в разделе «12.2.3. Поиск СНСИ в проводных линиях»);
- поиск информативных радиоизлучений прибора;
- разборка и визуальный осмотр элементов прибора».

Для повышения достоверности идентификации СНСИ по информативным сигналам рекомендуется использовать сравнение уровней подозрительного сигнала, принятого в проверяемом помещении и вне него.

Отсутствие информативных сигналов не является гарантией отсутствия СНСИ, так как они могут работать в ждущем режиме. Основой проверки электронных приборов является визуальный осмотр. При осмотре следует обращать внимание на не типичность

маркировки детали или отсутствие этой маркировки, на нестандартность внешнего вида и крепления детали, следы нефабричной пайки, неподключенные полуфабрикаты и т.д. «В некоторых случаях может потребоваться проведение осмотра внутренней структуры подозрительной детали
с помощью флуороскопа или рентгенотелевизионного устройства» [21].

12.2.3. Поиск СНСИ, работающих в проводных линиях

Проверка проводных линий на их использование агентом для передачи информации подразделяется на несколько этапов:

- визуальный осмотр линии и оборудования;
- поиск сигналов от СНСИ в линиях;
- поиск мест подключения к линии СНСИ.

Проверке подлежат [21] оборудование, проводные и кабельные линии, а именно:

- силовой и осветительной электросети;
- офисной и абонентской телефонной сети;
- селекторной связи;
- радиотрансляционной сети;
- пожарной и охранной сигнализации;
- системы невыясненного назначения.

Методика проверки в основном одинакова для линии и оборудования различного назначения. *Рассмотрим вопрос проверки цепей электросети.* Проверка осуществляется в соответствии с имеющимися схемами прокладки при соблюдении правил техники безопасности. Схему обследуемой электросети разбивают на несколько участков, каждый из которых может быть отключён от источника питающего напряжения. Перед *визуальным* осмотром желательно проверяющий участок обесточить. При визуальном осмотре тщательно обследуются силовые щиты, распределённые коробки, розетки, выключатели, электропатроны, удлинители, тройники, люстры, бра, настольные лампы, кондиционеры, вентиляторы и т.д. Каждое из установочных изделий проверяется на отсутствие новых или подменных элементов; выявленные подозрительные детали тщательно осматривать и при необходимости исследуются специальными техническими средствами неразрушающего контроля (например, рентгенотелевизионные устройства). *Для поиска сигналов СНСИ* все электроцепи и приборы должны быть включены. Поисковое устройство с помощью специальных согласующих устройств подключается к электросети. Автоматически или вручную перестраивают приёмник по частоте с целью просмотра всего контролируемого диапазона частот. При обнаружении сигналов в сети (сотни кГц, единицы и десятки МГц) уточняют положение СНСИ, либо последовательным перемещением вдоль участка электросети (сигнал возрастает при приближении к СНСИ), либо поочерёдным отключением от сети потребителей энергии. Если процессу обследования мешает высокий уровень шума в проверяемой линии (чаще всего это дефектные люминисцентные лампы или блоки питания), то следует этот источник шума отключить с дальнейшей его тщательной проверкой на наличие СНСИ.

Дальнейшим этапом проверки сети является проверка линии не на наличие сигналов, а на простое подключение СНСИ к линии. Проверка осуществляется с использованием нелинейного детектора (локатора) проводных коммуникаций. Примером таких устройств являются LBD-50, “Визир”. Методика работы следующая [21]:

- проверяемый участок электросети отключается от источника питающего напряжения;
- от участка отключаются все официальные потребители энергии (вывинчиваются лампочки, вилки приборов вынимаются из розеток, но выключатели освещения должны оставаться во включенном состоянии, чтобы не укорачивать проверяемый участок);

- прибор подключается к линии в начале проверяемого участка сети, к противоположному концу сети подключается испытательная нагрузка;
- в линию с прибора подаётся зондирующий сигнал;
- оператор на экране анализирует отраженный сигнал; если к линии подключены СНСИ (в состав которых обязательно входят нелинейные радиотехнические элементы), то в отраженном сигнале будут присутствовать высшие гармоники, свидетельствующие о факте нелегального подключения к линии.

Приведем некоторые технические характеристики локатора “Визир”: длина обследуемых линий не более 100 м, напряжение зондирующего импульса 220 В (50 В), частота 50 Гц, минимальная обнаруживаемая мощность СНСИ 1 мВт [5].

Проверка абонентской телефонной сети осуществляется в той же последовательности. Уточним некоторые детали. Около 70% СНСИ, обнаруживаемых в ходе поисковых работ, составляют средства, непосредственно сжимающие информацию с телефона, с телефонной линии или использующие телефонную линию для передачи снятой информации [21]. Во многих случаях агенты используют комбинированные СНСИ, обеспечивающих перехват информации при снятой телефонной трубке за счёт сигналов, циркулирующих в телефонной линии; в паузах между телефонными разговорами информация из помещения снимается за счёт внешнего микрофона или за счёт специального подключения микрофона телефонной трубки.

Визуальный осмотр телефонного аппарата, линии от аппарата до распределительной коробки и от коробки до телефонного щита должен производиться весьма тщательно, так как бесконтактный съём информации нельзя обнаружить ни одним прибором. Поиск сигналов в телефонной линии может осуществляться теми же приборами, что использовались для проверки электросети. Аппаратура поисковой бригады через специальные токосъёмники подключается к телефонной линии. Вначале трубка не поднимается, поисковый прибор исследует линию на наличие низкочастотного (разговорного) сигнала от внешнего микрофона или от микрофона положенной трубки при его специальном включении. Если в наушниках будет прослушиваться акустический фон помещения, то это будет сигнализировать о наличии СНСИ. Следующим этапом является поиск высокочастотных информативных сигналов. В этом случае для активации СНСИ поднимается телефонная трубка. В широком диапазоне частот ищется высокочастотный сигнал в линии. Наличие такого сигнала информирует о подключении к линии СНСИ. Типичными представителями анализаторов проводных линий являются приборы CCTA-1000 и SP18-T. В работе [5] указываются следующие характеристики прибора SP18-T. Прибор полностью автоматизирован, не требует “чистой линии” на момент подключения, обеспечивает обнаружение гальванически подключенных к телефонным линиям СНСИ на участке от анализатора до АТС.

Прибор обеспечивает:

- контроль нелинейности телефонной линии при разомкнутом и замкнутом шлейфах;
- определение наличия сигналов ВЧ-навязывания;
- определение параллельного подключения к линии во время телефонных переговоров;

- длительность тестирования 3-10 мин.

Габариты прибора 160х160х45 мм.

Для проверки телефонной линии на факт подключения даже неработающего СНСИ используют *кабельный локатор*.

Кабельные локаторы бывают двух типов [5]:

- рефлектометры (кабельный радар);
- нелинейный детектор.

Рефлектометр позволяет обнаружить не только факт подключения, но и определить расстояние до места подключения. Принцип его работы заключается в том, что в линию посылается импульс, который отражается от неоднородности линии, возникающей от подключения к ней устройств. Расстояние до места подключения определяется по осциллографу, регистрирующего время задержки отраженного импульса. При проведении этих исследований двухпроводная линия с известными параметрами сравнивается с контролируемой. В России выпускаются приборы Р5-9; Р5-10; Р5-13; ИКЛ-5 и т.д. Эти приборы предназначены для определения места повреждения линии и одновременно могут использоваться для выявления СНСИ. Специальная аппаратура, предназначенная именно для поиска закладных устройств, немного отличается от рассмотренных ранее изделий. Примером таких устройств являются приборы ТПУ-5, Дигифлекс Т12/3 и д.р. Импульсный эхометр Т12/3 (Германия [5]) имеет следующие характеристики:

- диапазон измерений 0,5; 1; 2,5; 10км;
- длительность импульсов 50; 100; …; 2000 нс;
- габариты 255х155х250 мм.

Нелинейный детектор реже, чем кабельный радар, используется для обнаружения СНСИ из-за сложности работы и неоднозначности получаемых результатов [5]. Принцип его работы заключается
в исследовании отраженного сигнала. Если к линии подключены устройства с нелинейными элементами (СНСИ), то в отраженном сигнале будут присутствовать сигналы второй и третьей гармоник (подробно см. п. 8…). При проведении испытаний линия абонента в телефонном шкафу отключается от АТС; в линию (в сторону телефонного аппарата) подключается нелинейный детектор; в место телефонного аппарата подключается испытательная нагрузка. Дальнейшая методика работы описана в п. 8 и вначале пункта 12.3. Примером нелинейных детекторов являются приборы LBD-50, “Визир” и т.д. Для анализа телефонных линий используются так же устройства позволяющие исследовать линии без отключения линии от АТС. Примером таких устройств являются ТПУ-6, SEL.SP-18/T. Последний прибор работает в автоматическом режиме, что существенно облегчает работу оператора.

При проверке других проводных систем применяется та же методика поисковых работ, что рассмотрена выше.

12.3. Заключительный этап комплексной проверки помещений

В состав комплексного этапа входят:

- обработка результатов поиска, уточнение временных и денежных затрат на поиск;
- изучение принципа работы найденных закладок и определение возможного ущерба от их работы;
- разработка рекомендаций по повышению защищенности помещений;
- составление акта проведения комплексной проверки помещений.

Целью обработки результатов поиска являются подготовка по рабочим материалам документов для оформления итогового отчёта заказчику. Кроме того, руководитель бригады обобщает опыт, накопленный бригадой за время проведения проверки, с целью

повышения уровня профессиональной подготовки своих специалистов. Уточняется возможность сокращения временных и денежных затрат при осуществлении дальнейших проверок.

При обнаружении закладок специалисты изучают (уточняют) принцип их работы, определяют их технические характеристики и определяют возможный объём информации, полученный противником. Для получения ответов на эти вопросы не нужно иметь точной измерительной аппаратуры [21]. Путем осмотра места установки и самого СНСИ можно оценить характеристики этого устройства. Если в качестве СНСИ используется радиомикрофон, то радиус съёма информации не превышает 6-8 метров; если СНСИ питалось от автономного источника питания, то по току потребления и оставшейся ёмкости батареи можно судить о времени его установки; по уровню сигнала и значению несущей частоты можно судить о дальности передачи; при подключении СНСИ к проводной линии можно определить возможные участки съёма информации, а также (если ведётся журнал вызова ремонтных бригад) и возможное время подключения СНСИ [21]. Исследованные технические и технологические характеристики СНСИ позволяют сделать вывод о месте съёма информации и, соответственно, руководство предприятия может оценить объём снятой информации и возможный причиненный ущерб. Найденные закладки рекомендуется сдать службам ФСБ, иногда они частично нейтрализуются (например, заклеивается микрофон; при этом акустическая слышимость резко падает, передатчик же продолжает работу; противник не догадывается что он обнаружен) или используется для дезинформации.

Руководству предприятия интересны как результаты поиска, так и *рекомендации по повышению защищенности помещений.* Утечка информации может происходить по искусственно созданным противником каналам утечки (проводные микрофоны, диктофоны, стетоскопы, проводные и радиозакладки и т.п.) и естественным техническим каналам утечки информации. В отличии от искусственно созданных каналов, естественные каналы утечки информации не обеспечивают комфортных условий приёма перехваченной информации, но существуют постоянно и могут быть использованы противником
в любой момент [21], поэтому они и носят название потенциальных каналов. Определение потенциальных каналов утечки информации осуществляется чаще всего качественным путем за счёт анализа документации о конструкции здания, визуального осмотра проверяемых
и соседних с ними помещений, а также за счёт проверки наличия сигналов на границе зон, в пределах которых исключено неконтролируемое пребывание посторонних лиц. Поиск сигналов в искусственных каналах утечки информации более прост, чем в естественных, так как величина сигнала достаточно велика. Для поиска таких сигналов используется ранее рассмотренная аппаратура, в том числе многофункциональный поисковый прибор Пиранья. Поиск слабых сигналов по естественным потенциальным каналам весьма дорог; осуществляется он высокочувствительными специализированными программно-аппаратными комплексами типа Навигатор, Спрут-5 и др..

Поиск закладок, определение потенциальных каналов утечки информации, закрытие этих каналов не должно быть очень дорогим; стоимость должна быть адекватна степени угроз. На основании анализа результатов обследования руководитель бригады должен предложить такую комбинацию организационных и инженерно-технических способов защиты, которая бы была близка к оптимальной по критерию “эффективность-стоимость”.

Завершающим этапом всех работ является *Акт проведения комплексной проверки помещения*. По рекомендациям работы [21], акт включает в себя:

- время проведения обследования;
- состав поисковой бригады;
- перечень обследованных помещений и объектов;

- перечень и объем основных поисковых работ и сопутствующих исследований;
- перечень использовавшейся и исследовательской аппаратуры;
- результаты проверки;
- места обнаружения средств СНСИ, их состояние и краткие характеристики;
- принятые по отношению к обнаруженным средствам меры (изъятие, нейтрализация, консервация с целью последующей дезинформации);
- выводы из оценки степени защищённости помещений и объектов от утечки защищаемой информации по различным каналам;
- рекомендации по повышению защищённости помещений и объектов и предотвращению утечки информации по выявленным техническим каналам её утечки.

Представленный в пособии материал не может охватить все виды угроз, и все методы борьбы сними; тем более что и первые, и вторые непрерывно совершенствуются. Поэтому данные материалы могут рассматриваться как введение в эту сферу защиты информации.

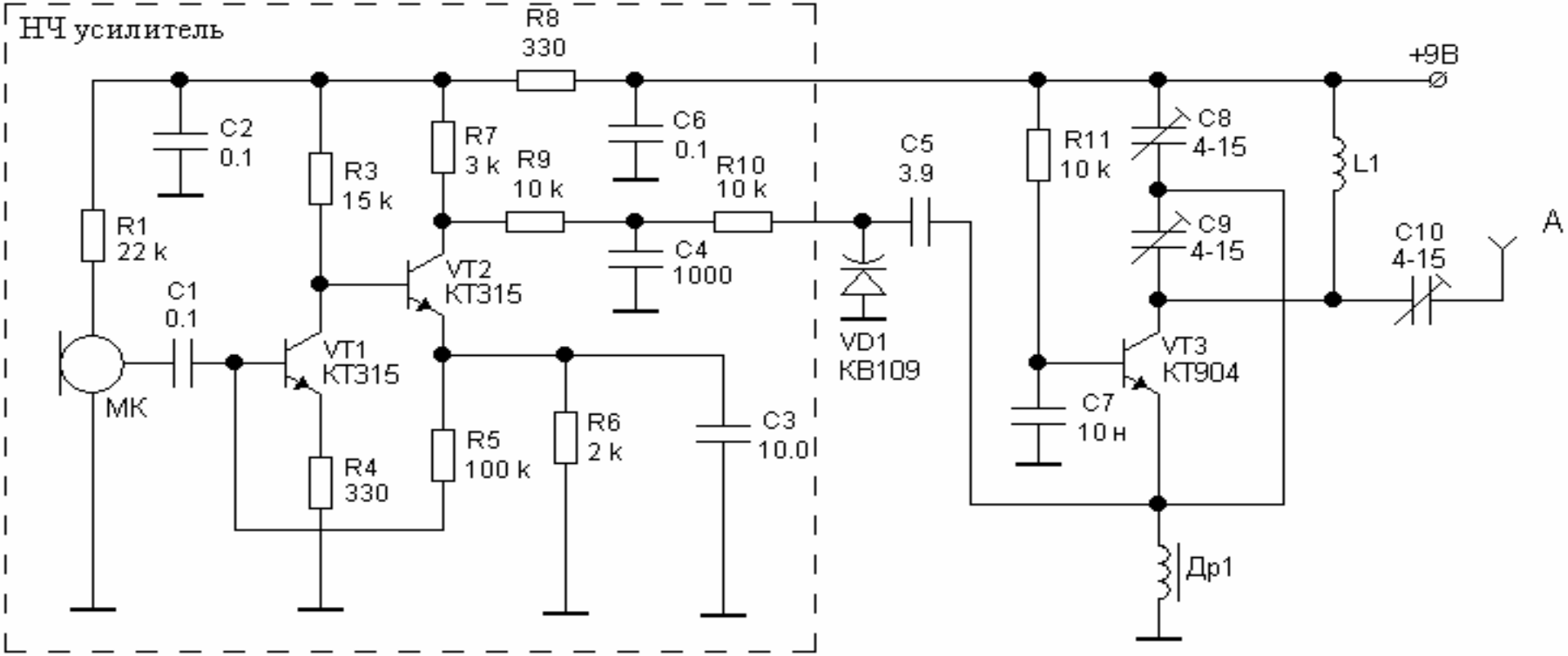

НЧ усилитель
R8
330
+9В
C2
0.1
R3
15 k
R7
3 k
R9
10 k
C6
0.1
R10
10 k
C5
3.9
R11
10 k
C8
4-15
L1
R1
22 k
C9
4-15
C10
4-15
A
C1
0.1
VT2
КТ315
C4
1000
VD1
КВ109
VT1
КТ315
VT3
КТ904
МК
C7
10 н
R6
2 k
C3
10.0
R5
100 k
R4
330
Др1

Рис. 8.14

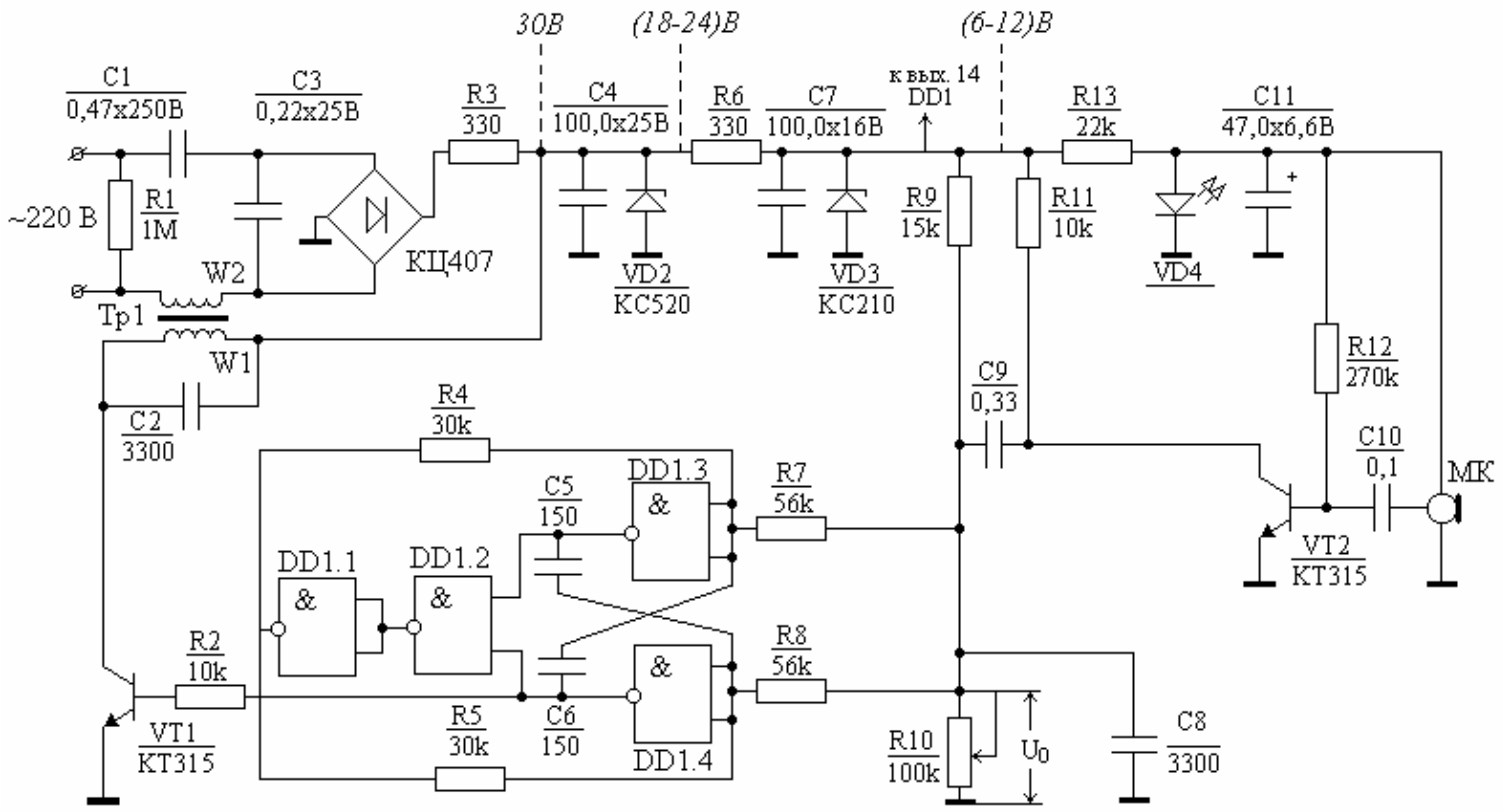

30В
(18-24)В
(6-12)В
к вых. 14 DD1
C1
0,47x250В
C3
0,22x25В
R3
330
C4
100,0x25В
R6
330
C7
100,0x16В
R13
22k
C11
47,0x6,6В
~220 В
R1
1M
W2
КЦ407
VD2
КС520
VD3
КС210
R9
15k
R11
10k
VD4
Тр1
W1
C2
3300
R12
270k
C9
0,33
R4
30k
C10
0,1
МК
C5
150
DD1.3
R7
56k
VT2
КТ315
DD1.1
DD1.2
R2
10k
R8
56k
VT1
КТ315
R5
30k
C6
150
DD1.4
R10
100k
U0
C8
3300

Рис. 10.2