ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ЭКОНОМИКИ И СЕРВИСА

С.Н. Павликов

ЗАЩИТА АУДИО И ВИДЕО ИНФОРМАЦИОННЫХ КАНАЛОВ

Владивосток 2009

УДК 65.0
ББК 32.884
П20

Рецензенты: кафедра вычислительной техники ТОВМИ, заместитель начальника кафедры к.т.н., доцент Карелин А.Н. и кафедра акустических приборов и технических средств судовождения Дальрыбвтуза (Технического университета), заведующий кафедрой к.т.н., профессор Карасев В.В.

Павликов С.Н.

П. 20. Защита аудио и видео информационных каналов. - Владивосток: ВГУЭС. 2005. – 152 с.

Учебно-методический комплекс подготовлен для дисциплины " Защита аудио и видео информационных каналов " и предназначен для студентов высших учебных заведений, обучающихся по специальности 210305 -“Средства радиоэлектронной борьбы ”. Может быть использовано для студентов по смежным специализациям и специальностям направления 210300. Обобщены достижения теории и практики защиты аудио и видео информационных каналов.

Павликов Сергей Николаевич

Редактор Л. Д. Стрикаускас

Технический редактор И. Д. Стукалов

Подписано в печать Формат 60 х 84/ 16

Печать офсетная. Усл. Печ. Л. 9.5 Уч.-изд. л.

Тираж 100 экз. Заказ Цена «С»

Отпечатано в типографии издательства ВГУЭС.

Владивосток, ул. Гоголя, 41

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В XX1 веке информация пронизывает все сферы жизнедеятельности людей. Объем и достоверность имеющейся информации влияет на качество принятого решения. И наоборот, чем меньшим объемом информации и достоверность о вас у вашего конкурента, тем шире у вас простор для маневра.

Поэтому информация и процедуры работы с ней должны быть под контролем. Сегодня очень актуальной становится проблема обеспечения информационной безопасной деятельности не только государственного служащего, но и бизнесмена, предпринимателя, юриста, публичного политика, да и простого человека.

По мнению компетентных экспертов, в случае полного рассекречивания информации о деятельности коммерческой фирмы, то последняя в условиях нашего «дикого» порядка просуществует не долго.

Таким образом, проблема защиты информации и обеспечения конфиденциальности коммерческой деятельности и личной жизни приобретает актуальность для очень многих людей. И, конечно, каждому хочется для укрепления своей безопасности использовать самые надежные, современные методы и средства, учитывающие все особенности приемов несанкционированного добывания сведений.

Для того чтобы умело защищаться необходимо знать о методах и средствах добывания информации, а также владеть техникой защиты информации от несанкционированного доступа.

Положение усугубляется тем, что современный российский предприниматель не имеет традиций поведения в условиях промышленного шпионажа. А те, кто ранее освоил это ремесло в государственных учреждениях продают свой опыт, как правило, нечестным предпринимателям, а простой человек становится для них легкой добычей.

Развитие рыночных отношений обострило конкуренцию и информационную борьбу.

Информация стала одним из важнейших ресурсов предприятия, при этом информация не только о своем предприятии, но и о рынке, посредниках и о конкурентах, а также о предстоящих изменениях в законодательной базе по всем вопросам экономической деятельности.

Данное учебное пособие позволяет получить представление о методах и аппаратуре получения информации, а также содержит рекомендации по формированию системы защиты информации личности и предприятия.

ГЛАВА 1. ЗАКОНОДАТЕЛЬНАЯ БАЗА О ПРОМЫШЛЕННОМ ШПИОНАЖЕ

1.1. Основные понятия

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

Сущность промышленного шпионажа - это стремление к овладению секретами конкурентов с целью получения максимальной коммерческой выгоды. Он заключается в получении любой информации о новейших научно-технических разработках (патентах, промышленных образцах, программных продуктах, технологий и ноу-хау), коммерческих планах, состоянии дел и т. п. ведется всеми доступными средствами, включая применение специальных технических средств, агентурными методами, а также путем подкупа должностных лиц.

Считается, что промышленный шпионаж в прямой постановке не затрагивает интересы государства. Эта позиция не только неверна, но и вредна. От сильного хозяйствующего субъекта и государство становится сильнее. Промышленный шпионаж является незаконной деятельностью, так как покушается на конституционные права граждан и права государства. Поэтому государство стоит на защите этих прав, а значит, их нарушение ведет к уголовной ответственности.

Для того чтобы эффективно бороться с промышленным шпионажем, необходимо знать приемы, методов и средств противника, который пытается негласного получить или исказить конфиденциальную информацию.

В соответствии со статьей 13 закона «Об оперативно-розыскной деятельности», право на негласное получение информации с использованием специальных технических средств имеют только те органы, которым разрешено осуществлять оперативно-розыскную деятельность на территории Российской Федерации. К ним относятся:

- органы внутренних дел Российской Федерации;
- органы федеральной службы безопасности;
- федеральные органы налоговой полиции;
- федеральные органы государственной охраны: Главное управление охраны Российской Федерации и Служба безопасности Президента Российской Федерации;
- органы пограничной службы Российской Федерации;
- таможенные органы Российской Федерации;
- Служба внешней разведки Российской Федерации;
- органы внешней разведки Министерства обороны Российской Федерации;
- органы внешней разведки Федерального агентства правительствен-

ной связи и информации при Президенте Российской Федерации.

Однако сотрудники этих подразделений не могут по первому желанию вторгаться в личную жизнь граждан, так как **статья 8** упомянутого закона определяет условия проведения соответствующих оперативно-розыскных мероприятий. В частности, в ней сказано: «...Проведение оперативно-розыскных мероприятий, которые ограничивают конституционные права граждан на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также право на неприкосновенность жилища, допускается на основании судебного решения».

Подробно: «...в случаях, которые не терпят отлагательств, допускается проведение оперативно-розыскных мероприятий ...с обязательным уведомлением суда (судьи) в течение 24 часов. В течение 48 часов с момента начала оперативно-розыскных мероприятий орган, его осуществляющий, обязан получить судебное решение о проведении такого оперативно-розыскного мероприятия либо прекратить его проведение».

Вышеперечисленные положения подкрепляются законом **«О частной детективной и охранной деятельности в Российской Федерации»** (закон № 2487-1 от 11 марта 1992 года). Статья 7 этого закона вводит соответствующие ограничения в сферу деятельности частного детектива. В ней сказано следующее: Частным детективам запрещается:

• осуществлять видео- и аудиозапись, фото- и киносъемку в служебных или иных помещениях без письменного согласия на то соответствующих должностных лиц;

• разглашать собранную информацию, использовать ее в каких-либо целях, вопреки интересам своего клиента или в интересах третьих лиц;

• проведение сыскных действий, нарушающих тайну переписки, телефонных переговоров, и телеграфных сообщений либо связанных с нарушением гарантий неприкосновенности личности или жилища, влечет за собой установленную законом ответственность.

Таким образом, с точки зрения закона только органы, уполномоченные на проведение оперативно-розыскных мероприятий, и только на основании судебного решения могут осуществлять негласный сбор информации о физических и юридических лицах. Однако если кто-то из читателей все же решит воспользоваться изложенными сведениями для неблаговидных целей проникновения в чужие секреты, то он должен знать об ответственности. Полезно их знать и свои права в том случае, если вы чувствуете чье-то незримое присутствие в своих делах.

Основные определения приведены на стр. 127 - 132.

1.2. Статьи Уголовного кодекса

Ниже приведены статьи **Уголовного кодекса (УК) Российской Федерации (РФ)** (в редакции от 1 января 1997 года), предусматривающие ответственность за информационные преступления.

«Статья 137. Нарушение неприкосновенности частной жизни

1. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрируемом произведении или средствах массовой информации, если эти деяния совершены из корыстной или иной заинтересованности и причинили вред правам и законным интересам граждан, - наказывается штрафом в размере от 200 до 500 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от 2 до 5 месяцев, либо обязательными работами на срок от 120 до 180 часов, либо исправительными работами на срок до 1 года, либо арестом на срок до 4 месяцев. То же деяние, совершенное лицом с использованием своего служебного положения, - наказывается штрафом в размере от 500 до 800 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от 5 до 8 месяцев, либо лишением права заниматься определенной деятельностью на срок от 2 до 5 лет, либо арестом на срок от 4 до 6 месяцев».

«Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений

1.Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан, - наказывается штрафом в размере от 50 до 100 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период до 1 месяца, либо обязательными работами на срок от 120 до 180 часов, либо исправительными работами на срок до 1 года, либо арестом на срок до 1 года.

2. То же деяние, совершенное лицом с использованием своего служебного положения или **специальных технических средств, предназначенных для негласного получения информации,** - наказывается штрафом в размере от 100 до 300 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от 1 до 3 месяцев, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет, либо арестом на срок от 2 до 4 месяцев.

3. Незаконное производство, сбыт или приобретение в целях сбыта специальных технических средств, предназначенных для негласного получения информации, - наказывается штрафом в размере от 200 до 500 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от 2 до 5 месяцев, либо ограничением свободы на срок до 3 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет.

Статья 139. Нарушение неприкосновенности жилища

1. Незаконное проникновение в жилище, совершенное против воли проживающего в нем лица, - наказывается штрафом в размере от 50 до 100 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период до 1 месяца, либо обязательными работами на срок от 120 до 180 часов, либо исправительными работами на срок до 1 года, либо арестом на срок до 3 месяцев.

2. То же деяние, совершенное с применением насилия или с угрозой его применения, - наказывается штрафом в размере от 200 до 500 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от 2 до 5 месяцев, либо лишением свободы на срок до 2 лет.

3. Деяние, предусмотренное частями первой и второй настоящей статьи, совершенное лицом с использованием своего служебного положения, - наказывается штрафом в размере от 500 до 800 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период - от 5 до 8 месяцев, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5лет, либо арестом на срок от 2 до 4 месяцев, либо лишением свободы на срок до 3 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет.

Статья 183. Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну

1. Собирание сведений, составляющих коммерческую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом в целях разглашения либо незаконного использования этих сведений, - наказывается штрафом в размере от 100 до 200 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от 1 до 2 месяцев, либо лишением свободы на срок до 2 лет.

2. Незаконное разглашение или использование сведений, составляющих коммерческую или банковскую тайну, без согласия их владельца, совершенные из корыстной или иной заинтересованности и причинившие крупный ущерб, - наказывается штрафом в размере от 200 до 500 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от 2 до 5 месяцев, либо лишением свободы на срок до 3 лет со штрафом в размере до 50 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период до 1 месяца либо без такового.

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе в ЭВМ, сис-

теме ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом в размере от 200 до 500 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от 2 до 5 месяцев, либо исправительными работами на срок от 6 месяцев до 1 года, либо лишением свободы на срок до 2 лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, - наказывается штрафом в размере от 500 до 800 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от 5 до 8 месяцев, либо исправительными работами на срок от 1 года до 2 лет, либо арестом на срок от 3 до 6 месяцев, либо лишением свободы на срок до 3 лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами,- наказывается лишением свободы на срок до 3 лет со штрафом в размере от 200 до 500 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от 2 до 5 месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок от 3 до 7 лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ, или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование, модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, - наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет, либо обязательными работами на срок от 180 до 240 часов, либо ограничением свободы на срок до 2 лет. Те же деяния, повлекшие по неосторожности тяжкие последствия,- наказываются лишением свободы на срок до 4 лет.

Выводы по главе:

1. Таким образом, с точки зрения закона только органы, уполномоченные на проведение оперативно-розыскных мероприятий, и только на основании судебного решения могут осуществлять негласный сбор информации о физических и юридических лицах.

Вопросы для самоконтроля:

Вопрос 1. Назовите основные статьи Уголовного кодекса по данной теме

Вопрос 2. Какие организации имеют право на негласное получение информации с использованием специальных технических средств?

Вопрос 3. В чем отличие ст. 272 от ст. 273 Уголовного кодекса РФ?

Вопрос 4. Что запрещается детективам по данной теме?

Методические рекомендации.

Изучив материал главы, ответьте на вопросы. При возникновении трудностей обратитесь к материалам для закрепления знаний в конце пособия.

Для углубленного изучения воспользуйтесь литературой:

основной: 1 – 3; дополнительной: 4 – 6 и повторите основные определения, приведенные в конце пособия.

ГЛАВА 2. ОСНОВНЫЕ МЕТОДЫ ВЕДЕНИЯ ПРОМЫШЛЕННОГО ШПИОНАЖА

2.1. Основные методы ведения промышленного шпионажа.

За многовековой период своего развития человечество разработало огромную массу знаний о способах и средствах ведения разведки противоборствующей (конкурирующей) стороны. Естественно, что в основном это опыт военного характера, но он нашел благодатную почву и для «мирной» реализации на ниве промышленного шпионажа. Рассмотрим основные способы ведения разведывательных (шпионских) действий.

Все они, независимо от того, кто и против кого их предпринимает, могут быть представлены в виде трех основных групп:

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

К использованию открытых источников относятся способы добывания информации, реализуемые путем анализа газет, книг, научных и технических изданий, официальных отчетов, патентов и рекламных материалов. Подобным образом работают большинство разведок мира. Понятно, что основная работа при этом ложится на специально подготовленных аналитиков, которые пропускают через себя горы материалов, отсеивая и накапливая необходимую информацию. Главными источниками получения открытого доступа к конфиденциальной информации являются:

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

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

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

Известно, что собирать открытую информацию легко и дешево, но она

недостаточно достоверна, так как не менее легко дать по этому каналу и дезинформацию.

Использование субъектов - носителей информации принадлежит к другой группе способов промышленного шпионажа. Дело в том, что в ряду источников конфиденциальной информации люди занимают особое место, ибо способны выступать не только обладателями неких сведений, но и субъектами злонамеренных действий: продажа, шантаж.

В отличие от технического устройства их можно подкупить, шантажировать или просто обмануть, но при этом люди являются не просто обладателями и распространителями информации в пределах своих функциональных обязанностей, их возможности гораздо шире. Так, любой человек, кроме того, что он является носителем информации, может ее анализировать, обобщать и делать выводы, то есть получать требуемые сведения по совокупности косвенных данных.

При определенных условиях люди способны скрывать, воровать, продавать информацию и совершать иные криминальные действия вплоть до вступления в устойчивые преступные связи со злоумышленниками. Правда, процесс выявления кандидата в агенты является достаточно сложным. Вначале проводится оценка и разработка кандидата, под, чем понимается изучение его личных качеств и способностей, а также изыскание способов его наиболее эффективной вербовки и использования. Далее производится сама вербовка на почве шантажа, подкупа, идейных соображений, личного неприятия руководителя компании и т. д.

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

Обнаружение скрытого агента - очень сложная и трудоемкая задача, требующая специальных навыков оперативной контр-разведовательной работы. При правильной организации деятельности фирмы большинство агентов (особенно обслуживающий персонал) не может обладать всей полнотой информации. В этом случае их используют для легального проникновения в помещения с целью установки подслушивающих устройств и исследования содержимого бумаг и мусорных корзин.

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

Для некоторого затруднения деятельности таких агентов необходимо, прежде всего, определить строгий порядок и выделить специальные оборудованные помещения для ведения деловых бесед, чтобы исключить даже кратковременное «случайное» присутствие посторонних, в том числе и из

своих сотрудников.

Таблица 1.

Объект, физическое явление, способ и устройства для получения информации

	Объект	Физическое явление	Способ и устройства съема информации
1	2	3	4
1	Разго-вор	Акустиче-ский сигнал	Подслушивание, Диктофон, Закладные устройства с передачей информации по имеющимся коммуникациям: (трубам, цепям сигнализации, силовым сетям, телефонным линиям); Специально проложенным коммуникациям; радио, инфракрасному каналу (ИК) и др.; направленный микрофон
		Виброакустический сигнал	Стетоскоп, вибродатчик с передачей информации по: радиоканалу, проводам, коммуникациям, ИК-каналу, оптический лазерный микрофон.
		Гидроакустический сигнал	Гидроакустический датчик
		Акусто-электрический сигнал	Радиоприемник специального назначения
		Движение губ	Визуально, в том числе с использование оптических средств; Камера, в том числе с передачей по проводам или радиоканалу
2	Раз-го-вор по теле-фону	Акустиче-ский сигнал	Подслушивание, Диктофон, Закладные устройства с передачей информации по имеющимся коммуникациям: (трубам, цепям сигнализации, силовым сетям, телефонным линиям); Специально проложенным коммуникациям; радио, инфракрасному каналу (ИК) и др.; направленный микрофон
		Электриче-ский сигнал в линии	Параллельный телефон, прямое подключение, через электромагнитный датчик, телефонная радиозакладка
		Побочные электро-магнитные излучения и наводки	Специальные приемные радиотехнические устройства

Продолжение табл. 1.

1	2	3	4
3	Разговор по радиотелефону	Акустический сигнал	Подслушивание, Диктофон, Закладные устройства с передачей информации по имеющимся коммуникациям: (трубам, цепям сигнализации, силовым сетям, телефонным линиям); Специально проложенным коммуникациям; радио, инфракрасному каналу (ИК) и др.; направленный микрофон
		Электромагнитные волны и наводки	Специальные приемные радиотехнические устройства
4	Документ	Бумага, плакат, чертеж	Визуально, в том числе с использование оптических средств; Камера, в том числе с передачей по проводам или радиоканалу
5	Документ на бумажном носителе в процессе размножения	Следы на нижнем листе, копировальной бумаге, красящей ленте и др.	Кража, визуально
		Шумы принтера	Спец. аппаратура контроля полей принтера
		Побочные электромагнитные излучения и наводки	Специальные приемные радиотехнические устройства
6	Почтовые отправления	Конверты, бандероли, посылки, контейнеры	Прочтение со вскрытием или без вскрытия
7	Документ на небумажном носи-	Магнитные, оптические, механические и др.	Копирование, вскрытие и несанкционированное использование

	теле		

Окончание табл. 1.

1	2	3	4
		Изображение на дисплее	Визуально, в том числе с использование оптических средств; Камера, в том числе с передачей по проводам или радиоканалу
		Побочные электромагнитные излучения и наводки	Специальные приемные радиотехнические устройства
		Электрические сигналы в сетях коммуникаций	Специальные приемные радиотехнические устройства и закладки
8	Передача документа на небумажном носителе	Электрические сигналы в сетях коммуникаций	Прямое или косвенное подключение, через электромагнитный датчик, радиозакладка, имитация пользователя

Представленная таблица содержит лишь самую общую классификацию. При этом каждый канал, способ или устройство может быть эффективным и опасным, все зависит от профессионализма нападающей и защищающейся сторон. Подробно о каждом техническом канале и используемых в нем средствах будет рассказано далее.

2.2. Методы и устройства передачи информации по радиоканалу

2.2.1. Принцип работы закладных устройств.

Один из эффективных путей негласного получения коммерческой информации основан на применении так называемых закладных устройств (ЗкУ), скрытно устанавливаемых в местах возможного нахождения объектов наблюдения либо подключаемых к используемым ими каналам связи.

В настоящее время создано огромное количество типов таких устройств, различающихся принципом функционирования, способом передачи информации, дальностью действия, а также размером и внешним оформлением.

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

Для того чтобы систематизировать представление о таких устройствах, целесообразно ввести пять признаков их классификации (Рис. 1):
- по каналу передачи информации;
- по способу восприятия информации;
-по наличию устройства управления;
-по внешнему виду;
-по используемому источнику питания.

Рассмотрим отдельно каждый из признаков. В зависимости от **канала передачи информации** различают следующие типы ЗкУ, см. Рис. .2. –Рис. 4: - радиозакладки;

- инфракрасные закладки;
- закладки с передачей информации по токоведущим линиям;
- закладки с записью на запоминающие устройства.

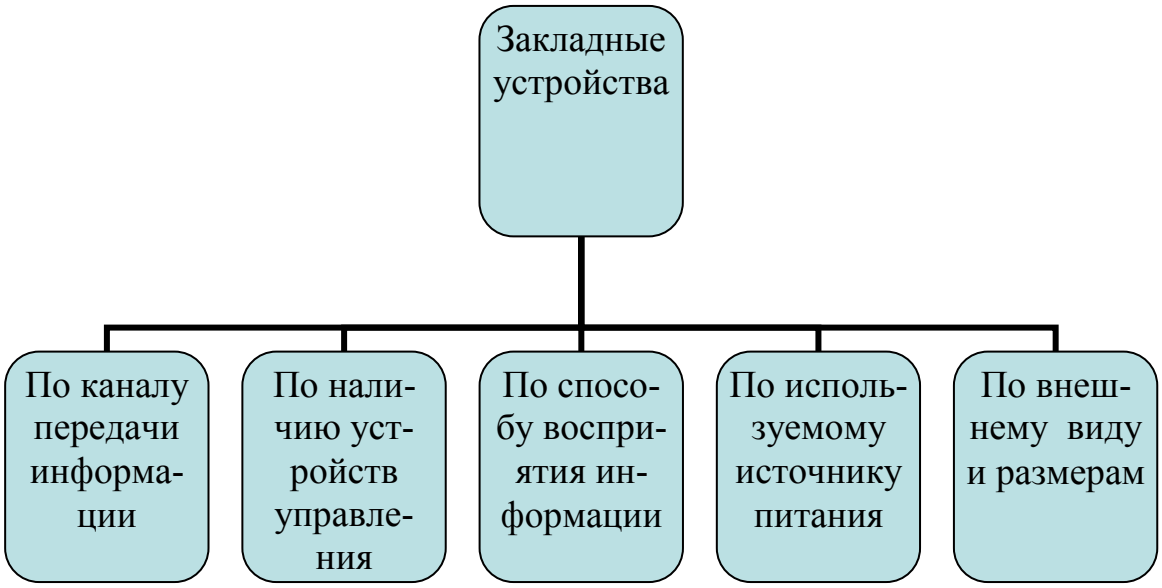


Рис. 1. Классификация закладных устройств

В радиозакладках для передачи информации используется энергия электромагнитных волн, не улавливаемых органами чувств человека, способных распространяться на значительные расстояния, преодолевая естественные и искусственные препятствия. Благодаря этим двум свойствам радиозакладные устройства позволяют с помощью специальной приемной аппаратуры вести скрытное наблюдение за интересующим объ-

ектом из удаленной точки. С технической точки зрения, закладки могут работать практически в любом диапазоне радиоволн. Однако из конструктивных соображений и свойств ослабления сигнала, наиболее используемые частоты - от 100 до 1000 МГц.

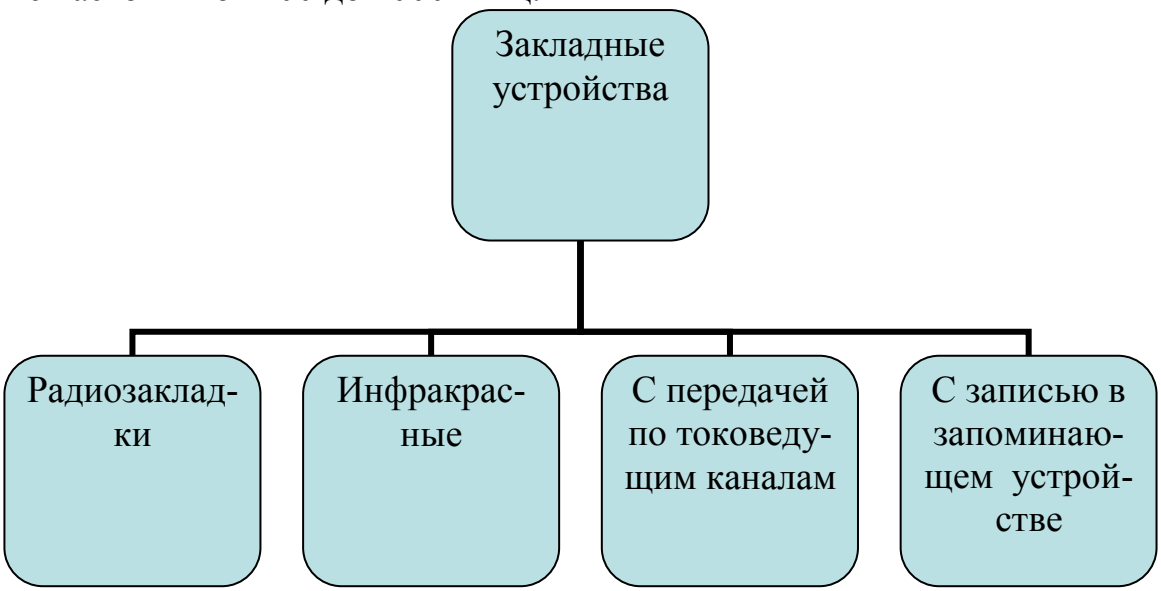


Рис. 2. Классификация закладных устройств по каналам передачи информации

В инфракрасных закладках для передачи информации также используется энергия электромагнитных волн, но не радиодиапазона, а невидимой части оптической области спектра - инфракрасного диапазона.

Благодаря малой длине такие волны распространяются узким пучком в заданном направлении, и их трудно обнаружить даже с помощью специальной аппаратуры. Дальность передачи информации от инфракрасных ЗкУ достигает 500 м.

Однако высокая скрытность таких устройств существенно усложняет их применение. Так, инфракрасная закладка должна постоянно находиться в зоне прямой видимости приемника оптического излучения, а случайно попавший на линию визирования предмет, человек или автомобиль, а также изменившиеся погодные условия могут привести к существенному ухудшению качества или даже пропаданию сигнала в аппаратуре регистрации. Такие ЗкУ не применимы на мобильных объектах.

В силу перечисленных недостатков инфракрасные закладки не нашли широкого использования в практике промышленного шпионажа.

Закладки с передачей информации по токоведущим линиям используют свойство электрических сигналов распространяться на значительные расстояния по проводникам. Такие ЗкУ обладают существенными достоинствами: высокой скрытностью передачи информации, большой дальностью действия, отсутствием необходимости в дополнительных источниках питания. Кроме того, они хорошо маскируются под элементы электрических цепей и токоприемники (розетки, тройники, электрические удлинители, настольные лампы и т. д.). В качестве токопроводящих линий использу-

ются либо специально проложенные провода, либо кабели электрических и телефонных сетей. В силу перечисленных обстоятельств ЗкУ такого типа часто применяются недобросовестными конкурентами для получения сведений конфиденциального характера. В случаях, когда отсутствует необходимость получения оперативной информации в реальном масштабе времени, а также имеется возможность скрытного извлечения и замены кассеты или магнитной ленты, закладка может оснащаться запоминающим устройством вместо блока передачи по одному из рассмотренных каналов. Такой способ, как правило, применяется только в тех случаях, когда есть потенциальная угроза обнаружения объектом наблюдения канала передачи информации (например, с помощью специальной аппаратуры контроля).

В зависимости от способа восприятия информации различают три типа ЗкУ , см. Рис. 3:

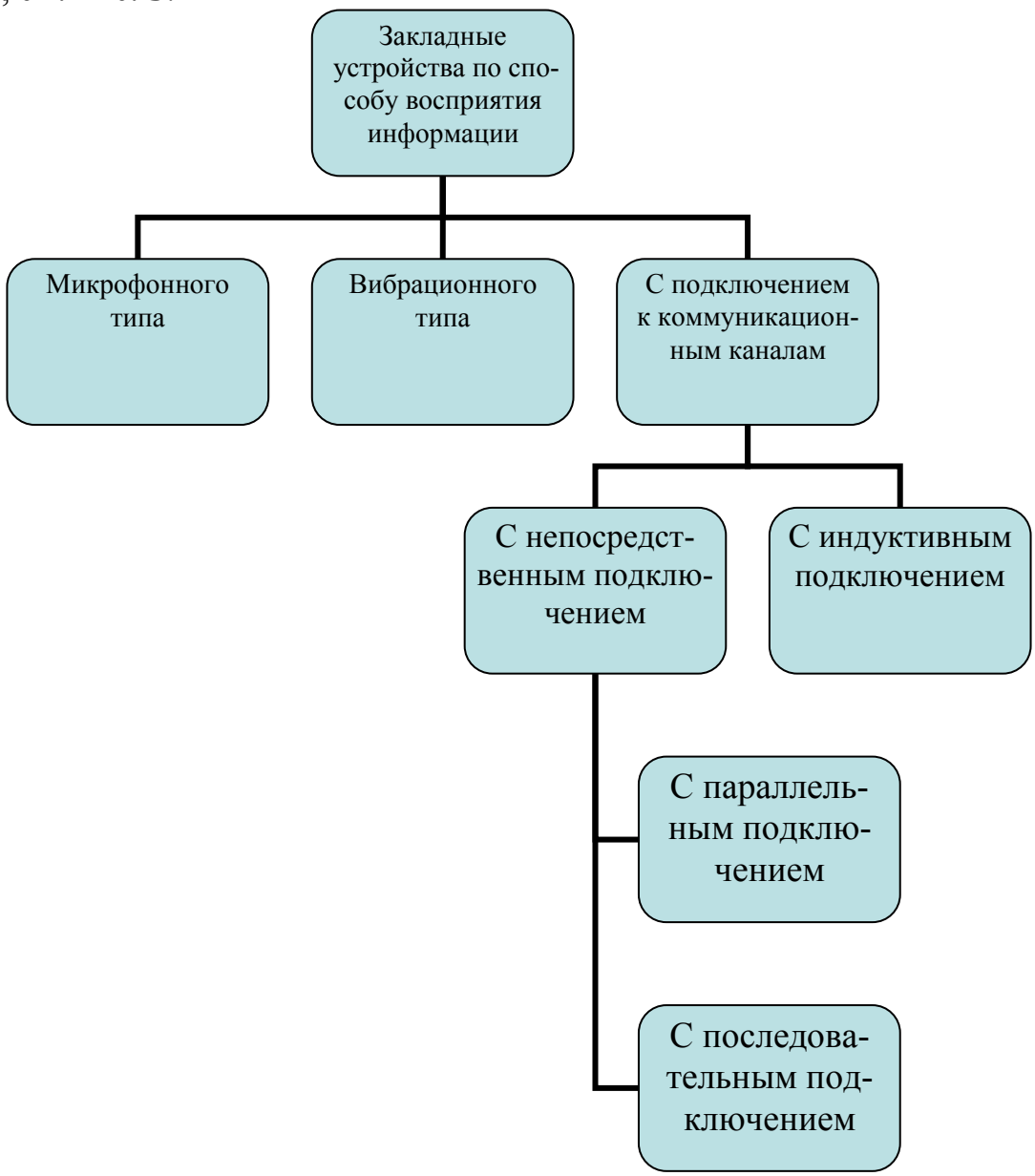


Рис. 3. Классификация закладных устройств

Принцип действия ЗкУ микрофонного типа основан на преобразова-

нии акустических атмосферных колебаний в электрические сигналы и передаче их потребителю одним из вышеперечисленных способов.

ЗкУ вибрационного типа (стетоскопы) перехватывают акустические колебания твердых сред (вибрации), возникающие вследствие давления атмосферных акустических волн на среды. В качестве чувствительных элементов в таких устройствах обычно используются пьезомикрофоны, электронные микрофоны или датчики акселерометрического типа. Они наиболее эффективны при фиксации на тонких «площадных» поверхностях (межкомнатных перегородках, стеклах, дверях и т. п.). Для передачи информации потребителю, как правило, используется радиоканал, и такие ЗкУ обычно называют радиостетоскопами.

ЗкУ с подключением к коммуникационным линиям предназначены для негласного перехвата информации, циркулирующей в телефонных или волоконно-оптических линиях.

Они позволяют скрытно получать информацию о содержании телефонных переговоров, а также текстовых сообщений (телеграфных, факсимильных, электронной почты и т. д.). Для передачи информации с подключаемых ЗкУ обычно используется радиоканал, а такие устройства называются радиозакладными. По способу подключения к телефонным линиям радиозакладки делят на две группы:

- с непосредственным подключением;
- радиозакладки с индукционным подключением.

Они подключаются либо одновременно к обоим проводам параллельно абоненту, либо в разрыв одного из проводов - последовательное подключение.

Такие способы позволяют получить достаточно большой уровень сигнала (его хорошее качество) на входе радиозакладки, а также обеспечить ее питание от линии. Однако закладки с непосредственным подключением могут быть легко обнаружены по изменению параметров линии.

Этого недостатка в значительной степени лишены устройства второй группы - радиозакладки с индукционным подключением. В таких закладках чувствительным элементом выступает специальным образом построенная антенна, устанавливаемая вплотную к проводам телефонной линии. Электромагнитное поле, окружающее телефонные провода, наводит в антенне токи, содержащие информацию о характере сообщения. Эти токи усиливаются, преобразуются и далее полученная информация передается на пункт регистрации. Закладные устройства для снятия информации с волоконно-оптических линий принципиально отличаются от рассмотренных выше только способом снятия информации. Для этих целей применяются специальные устройства сжатия волоконных линий, вызывающие интерференционные процессы на поверхности оптического волокна, которые и считываются фотоприемником.

По наличию устройства управления ЗкУ условно можно разделить на три группы: с непрерывным излучением;

•с дистанционным управлением;

•с автоматическим включением при появлении сигнала.

ЗкУ с непрерывным излучением наиболее просты в изготовлении, дешевы и предназначены для получения информации в течение ограниченного промежутка времени. Работа на излучение таких ЗкУ начинается с момента подключения питания. Если источник питания автономный, то, как правило, время работы такого ЗУ не превышает 1-2 часа из-за большого потребления энергии на передачу сигнала. Время работы Зк У, питающихся от линий (силовых или телефонных), практически неограниченно. Однако общим существенным недостатком для всех ЗкУ с непрерывным излучением является возможность их обнаружения по излучению. Существенно увеличить время непрерывной работы устройств с автономным питанием и повысить скрытность позволяет применение дистанционного управления ЗкУ. Оно позволяет переводить устройство в режим излучения только в тех случаях, когда объект наблюдения ведет переговоры либо передает информацию по каналам связи. Время излучения может быть дополнительно сокращено, если закладка содержит устройство накопления и сжатия сигнала. Но это усложняет устройство, повышает его стоимость и снижает надежность.

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

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

По используемому источнику питания, как было отмечено выше, ЗкУ делятся на два вида: с собственным источником; с питанием от внешнего источника. К первому виду относятся любые ЗкУ, имеющие собственный встроенный аккумулятор. Ко второму - ЗкУ с передачей информации по токоведущим линиям и ЗкУ с непосредственным подключением к коммуникационным линиям. Время работы этих устройств практически неограничено.

По **внешнему виду** ЗкУ могут быть в обычном или закамуфлированном исполнении. В обычном исполнении устройства имеют, как правило, металлический корпус (окрашенный или нет) и форму параллелепипеда. Они

достаточно универсальны и применяются в различных условиях обстановки. Маскируются одеждой, предметами интерьера, либо местными предметами, пропускающими акустические и электромагнитные колебания. В закамуфлированном виде ЗкУ применяются только в соответствии с конкретной обстановкой. Так, например, в виде силовой или телефонной розетки только в том случае, если другие неиспользуемые розетки в помещении имеют такой же внешний вид, в виде личных вещей (часов, зажигалки, заколки...), если они соответствуют общему имиджу применяющего их человека.

2.2.2. Закладные устройства с передачей информации по радиоканалу.

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

Радиозакладные устройства как радиотехнические средства обладают рядом специфических особенностей, не свойственных другим ЗкУ В соответствии с этими особенностями для классификации радиозакладок могут быть использованы следующие признаки:

- принцип формирования сигнала;
- способ закрытия передаваемой информации;
- дальность действия, см. Рис. 4.

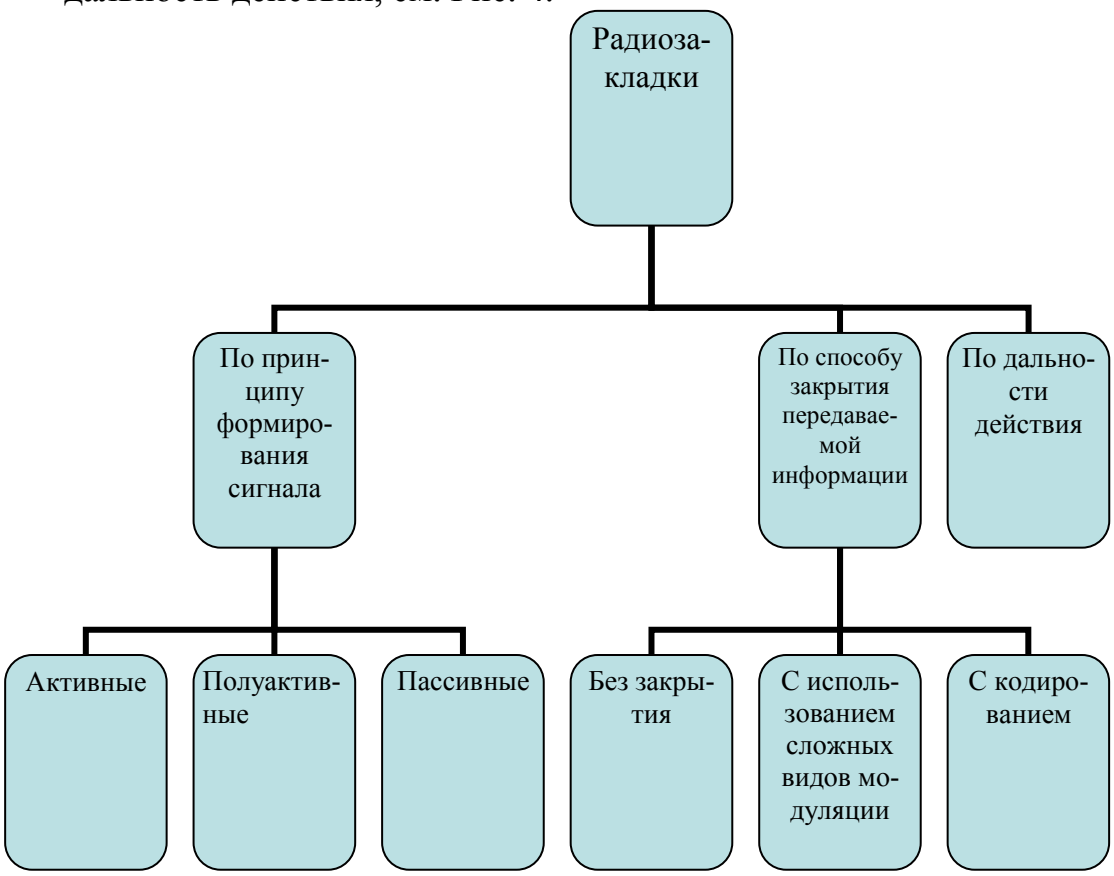


Рис. 4. Классификация радиозакладных устройств

В соответствии с принципом формирования сигнала РЗУ могут быть:

• активные; пассивные; полуактивные.

Активные РЗУ наиболее распространены. В общем виде они могут быть представлены структурной схемой, изображенной на рис. 5.

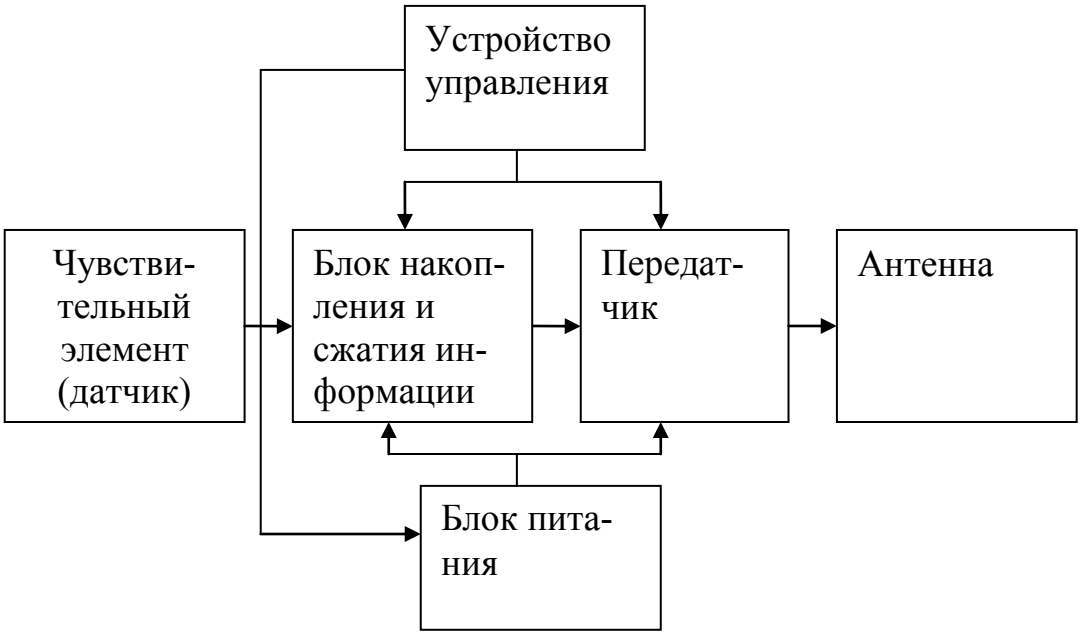


Рис.5 Структурная схема активной радиозакладки

Полуактивные РЗУ характеризуются существенно большим временем функционирования от автономного источника питания: до 4000 часов. Положительный эффект достигается за счет комплексного использования энергии внешнего специально сформированного мощного зондирующего сигнала и энергии, собственного питающего элемента. При этом энергия собственного аккумулятора тратится лишь на модуляцию принимаемого высокочастотного сигнала и его усиление. Так как такие радиозакладки могут работать только при наличии внешнего зондирующего электромагнитного поля, то они получили название «аудиотранспондеры» («аудиоответчики») от английского «audmtransponder». Структурная схема полуактивного РЗУ показана на Рис.6.

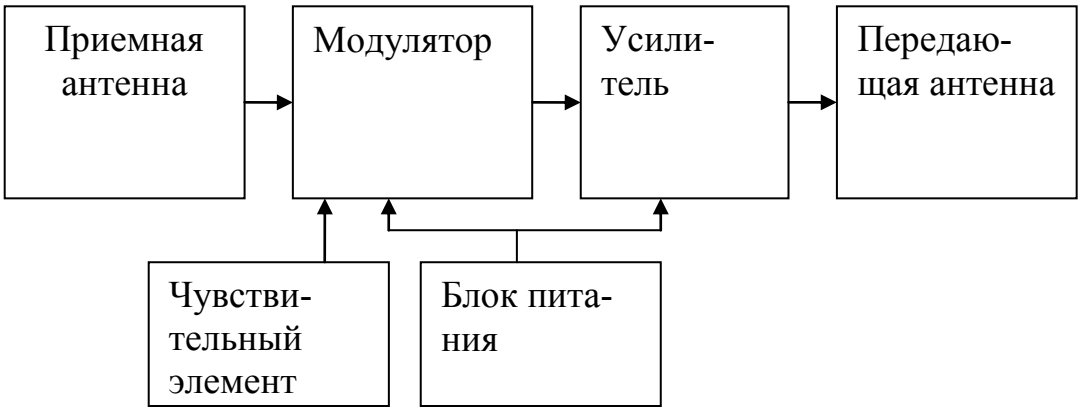


Рис.6. Структурная схема полуактивной радиозакладки

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

Однако мощный зондирующий сигнал является демаскирующим признаком применения полуактивного ЗУ, что для руководителя службы безопасности должно послужить толчком к проведению соответствующих мероприятий по защите информации. Принцип работы радиозакладок приведен на Рис. 7.

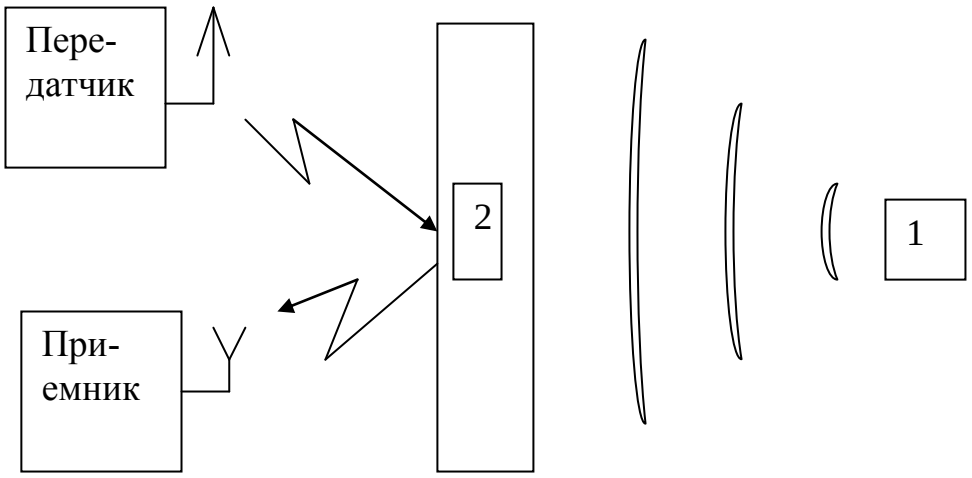


Рис. 7. Принцип работы радиозакладок: 1- Источник сигнала; 2- полуактивная либо пассивная радиозакладка

Примером аудиотранспондеров могут служить радиозакладки **S1M-ATP-16** и **SIM-ATP-40** (см. Приложение 1, табл. П2)

SIM-ATP-16 - аудиотпанспондер имеющий размер 90х90х4 мм.

SIM-ATP-40 - отличается от SIM-ATP-16 тем, что имеет габариты 130х75х250 мм и работает в диапазоне 800....950 МГц. Необходимая мощность облучающего сигнала лежит в пределах от 0,1 до 20 мВт. Дальность активации системы передатчиком - 10 м. Время работы транспондера от внутренней батареи напряжением 3 В - до 4 месяцев. Для облучения и приема переизлученного сигнала используются направленные директорные антенны. Потери на переизлучение составляют около 8 дБ.

Принцип действия пассивных РЗУ был разработан еще в середине 40-х годов. Одна из таких радиозакладок в течение многих лет проработала в посольстве США в, Москве, спрятанная в гипсовый герб Соединенных Штатов, установленный над рабочим столом в кабинете посла. Выявлена она была с большим трудом и только после того, как ЦРУ стало точно известно, что утечка информации происходит именно из этого кабинета.

Однако пассивные РЗУ в настоящее время не нашли достаточно широкого применения. Полуактивные РЗУ обладают существенным преимуществом. Примером серийно выпускаемой пассивной закладки может служить SIPE **MM1** - пассивная радиозакладка, выполненная в виде стержня длиной около 30 см и диаметром 2,5 см. Дальность действия - 100 м. Поставляется в комплекте, состоящем из закладки, источника облучения с питанием от электросети и приемного устройства.

Принцип применения пассивных и полуактивных радиозакладок иллюстрируется на рис. 8. По способу закрытия информации, передаваемой в радиоканале, РЗУ делятся на три вида:

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

Естественно, что наиболее простым видом ЗкУ являются радиозакладки без закрытия информации. Однако их применение ограничено возможностью перехвата информации любым лицом, имеющим приемник, работающий на частоте РЗУ. К радиозакладкам с использованием сложных видов модуляции относятся устройства с двойной модуляцией сигнала - на поднесущей и основной частоте излучения, например, **РК1970-SS** (см. Приложение 1, табл. П2). Частота поднесущей выбирается много больше 20 кГц. Поэтому прием информации возможен только на специальный приемник с двойным детектированием, что существенно повышает ее скрытность. Попытка прослушивания сигнала обычным приемником ни к чему не приведет, так как выходной сигнал будет превышать верхний частотный уровень чувствительности человеческого уха. К более эффективным способам закрытия информации относится использование сложных шумоподобных сигналов и различных способов кодирования информации. Так, например, шумоподобные сигналы с фазовой манипуляцией используются в радиозакладках **РК1970** и **SIM-PR-9000T,** а аналоговое скремблирование (наиболее часто применяемый способ шифрования) - в радиозакладках **РК2010S** (простая инверсия спектра) и в устройствах **«Брусок-ЛЗБ ДУ», РК1380-SS** или **РК540-SS** (сложная инверсия спектра).

Более сложный способ шифрования речевой информации - кодирование ее в цифровом виде. Такой способ закрытия применен, например, в радиозакладках **РК1195-SS, РК2050, SIM-PR-9000T** и **РК1970** (см. Приложение 1, табл. П2).

В зависимости от мощности передатчика РЗУ делятся на три вида - малой, средней и большой дальности действия. Радиозакладные устройства малой дальности способны передавать информацию на расстояние, не превышающее несколько десятков метров, поэтому без ретранслятора (приемно-передающего блока) они, как правило, не используются. РЗУ средней дальности позволяют вести уверенный прием информации на удалении несколько сот метров, а радиозакладки большой дальности способны работать с радиоприемными устройствами, расположенными на

удалении 1000 м и более. В качестве иллюстрации можно привести характеристики некоторых типов серийно выпускаемых закладных устройств:

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

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

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

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

РК560-S - передатчик, закамуфлированный под электролампочку. Дальность перехвата акустических сигналов - 20 м, дальность передачи радиосигналов - 300 м. Питается от электросети переменного тока с напряжением 110/220 В. Не может быть использован в качестве источника света. Рекомендуемые приемники для работы с радиомикрофонами: **РК830-SS, РК825-S, РК101S-SS.**

РК570-S - передатчик, закамуфлированный под пепельницу. Габариты -125х12х30 мм, вес - 275 г. Дальность передачи радиосигналов - 250 м. Источник питания - батарея с напряжением 9 В, время непрерывной работы - 50 часов. Дистанционное управление режимом излучения.

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

STG 4005 - радиомикрофон с «акустоматом», работает в диапазоне частот 130... 150 МГц, вид модуляции - широкополосная частотная, выходная мощность - 6 мВт. Габариты - 45х30х15 мм, вес - 35 г, напряжение питания - 6 В, тип антенны - гибкая.

STG 4007 - радиомикрофон с «акустоматом», работает в диапазоне частот 395...415 МГц, вид модуляции - узкополосная частотная, выходная

мощность - 15 мВт. Габариты - 66х27х14 мм, вес - 52 г, напряжение питания - 6 В, тип антенны - гибкая.

GTG 4215 - радиомикрофон с дистанционным управлением, работает в диапазоне частот 115... 150 МГц, вид модуляции - широкополосная частотная, выходная мощность - 5 мВт. Габариты - 67х36х25 мм, вес - 70 г, напряжение питания - 110/220 В электросети переменного тока, антенна - провод электросети. Устройство дистанционного управления работает в диапазоне частот: 800... 1000 Гц. Выходная мощность - 50 мВт, команда - кодированная. Габариты - 155х60х20 мм, вес - 70 г.

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

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

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

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

Схемы применения приведены на Рис. 8. /1/. Для того чтобы дать представление о принципах построения закладных устройств, на Рис. 9 - 10 приведены несколько вариантов принципиальных схем радиомикрофонов /1, 2/.

2.2.3. Приемники излучения радиозакладных устройств

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

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

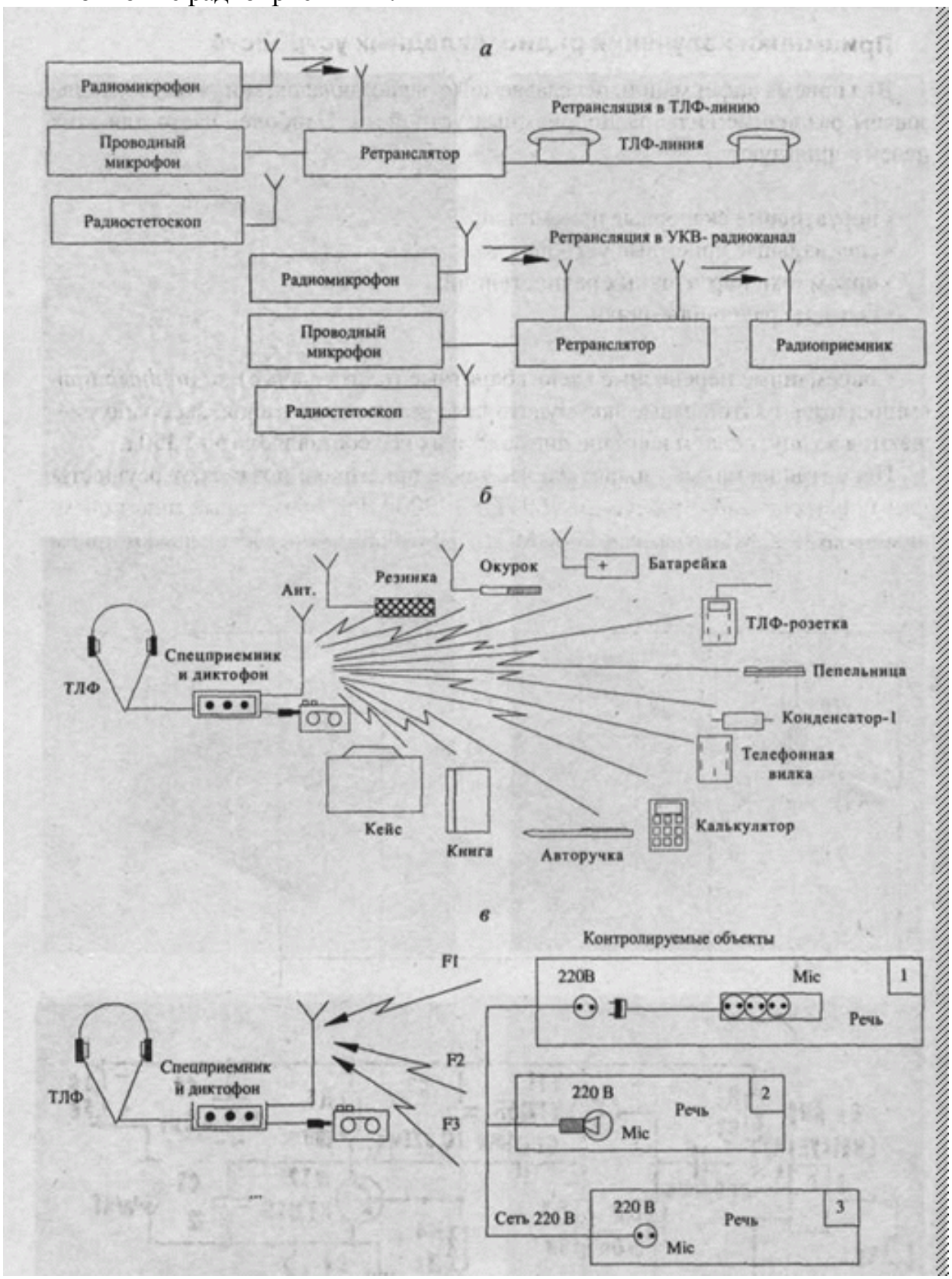


Рис. 8. Схемы применения радиозакладных устройств

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

Несмотря на малые габариты и вес такие приемники позволяют осуществлять прием сигналов в диапазоне 100 кГц... 1300 МГц, а некоторые типы приемников - до 1900 МГц и даже до 2060 МГц («**HSC-050**»).

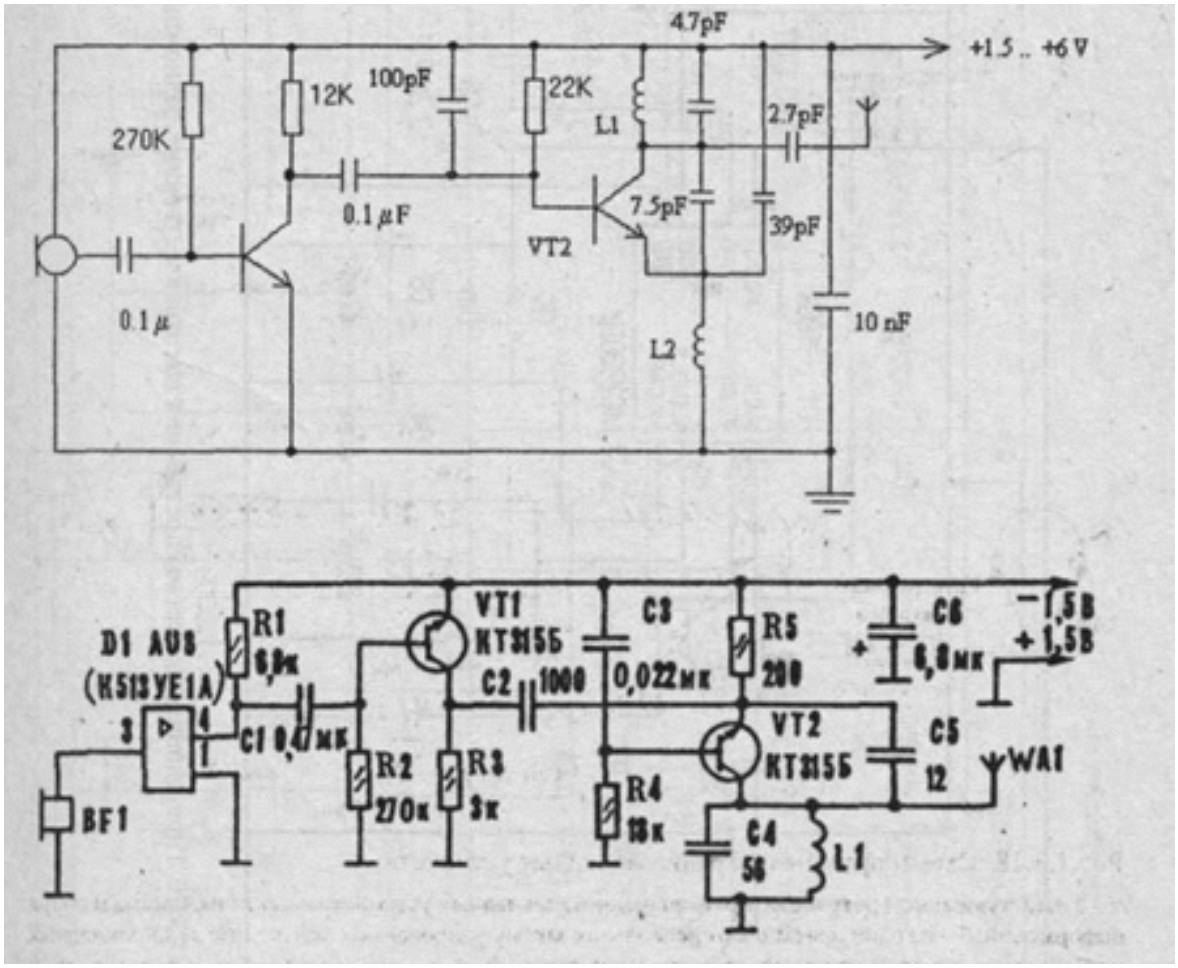


Рис. 9. Принципиальные схемы радиомикрофонов

Они обеспечивают прием сигналов с амплитудной, узкополосной и широкополосной частотной модуляцией, а их чувствительность лежит в пределах от 0,35 до 6 мкВ. Полоса пропускания в режиме приема узкополосных сигналов - 12... 15 кГц, а широкополосных (текстовых) - **150... 180** кГц.

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

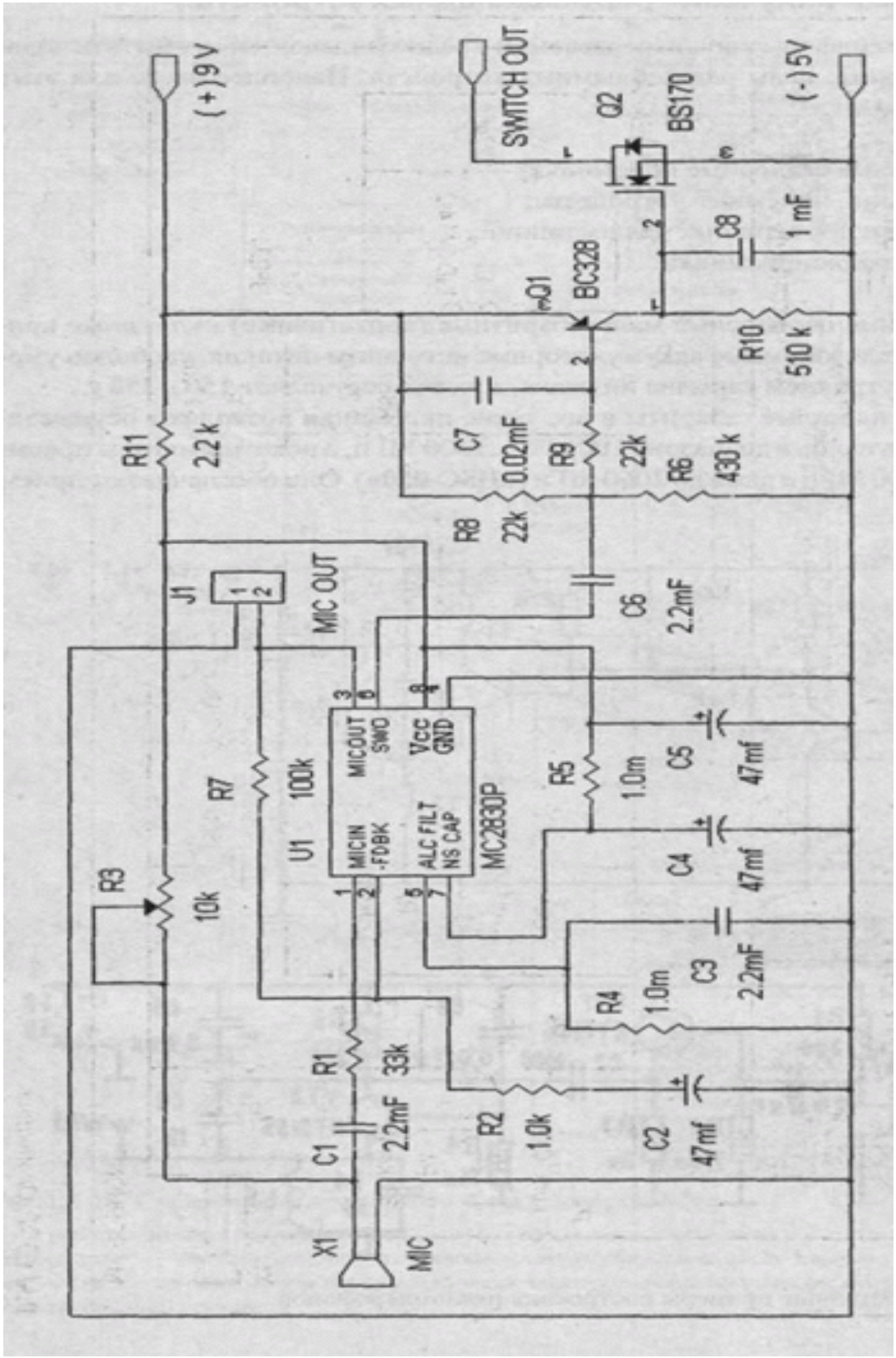


Рис. 10. Принципиальная схема радиомикрофона (начало)

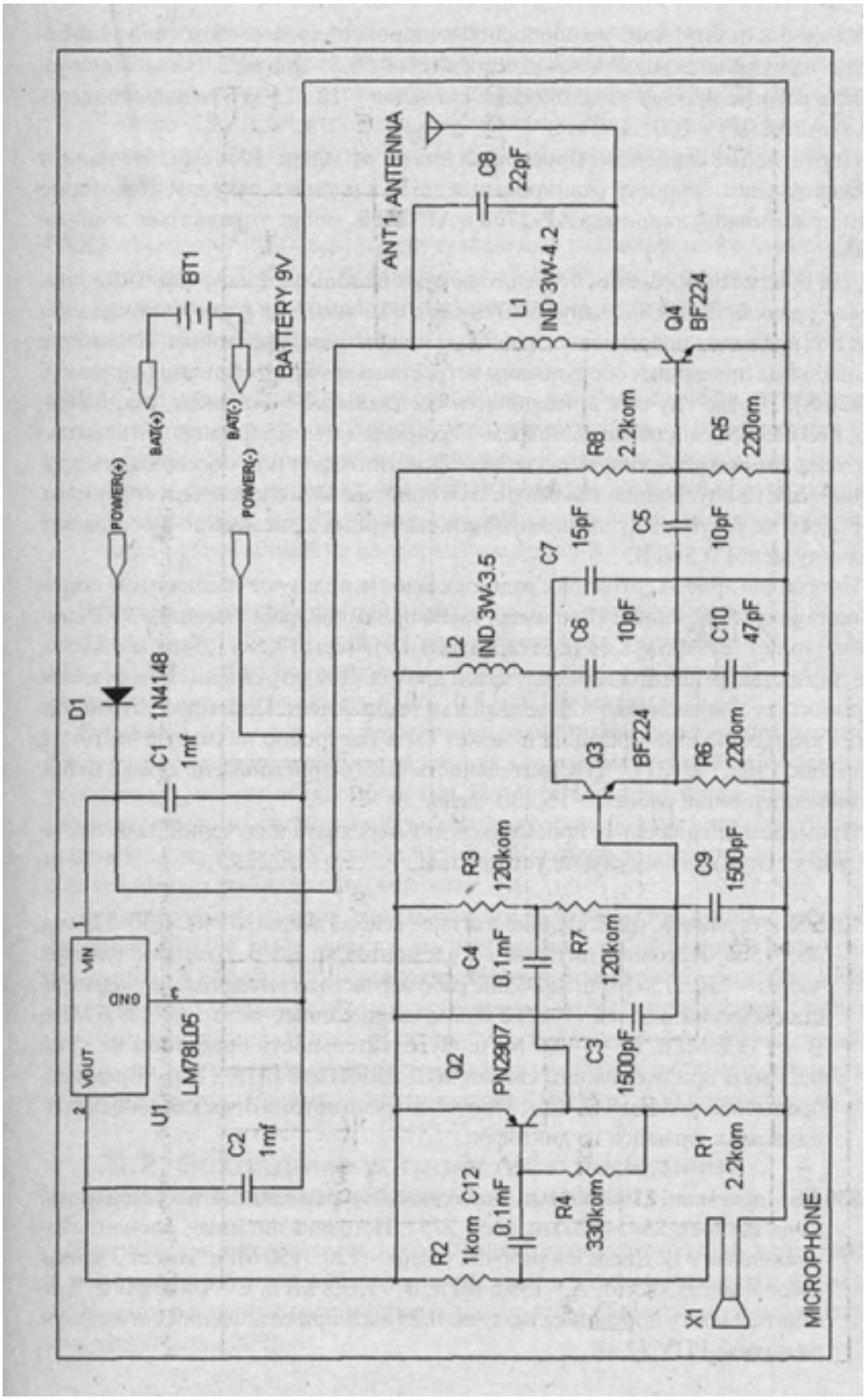


Рис. 10. Принципиальная схема радиомикрофона (окончание)

Они выпускаются как в обычном, так и камуфлированном виде под предметы повседневного обихода или бытовые приемники. Некоторые специальные приемники оборудованы встроенными магнитофонами (например, **РК820-S).** В раде случаев применяются специальные комплексы, как, например, **РК1015-SS,** способные одновременно принимать информацию по нескольким каналам и осуществлять ее запись на магнитофон или

обеспечивать прослушивание на внутренние динамики. Чувствительность специальных приемных устройств не уступает чувствительности сканерных приемников и составляет величину менее 0,5 мкВ.

Иногда для приема сигналов с радиозакладок используют специальные сверхминиатюрные приемники. Например, такой приемник, работающий в УКВ-диапазоне, имеет вес около 1,5 г (с батарейкой) и размеры 17,5х11,5 мм, позволяющие полностью установить его в слуховой проход. Для затруднения обнаружения приемника его окрашивают в телесный или темный цвет. Приемное устройство имеет кварцевую стабилизацию и может быть настроено на любую частоту в диапазоне 138... 190 МГц. Чувствительность такого приемника не хуже 2 мкВ, а время непрерывной работы - 15...30 часов.

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

PK1015-SS - приемник, размещенный в атташе-кейсе. Габариты - 460х330х120 мм, вес - 5 кг. Источник питания - 8 элементов по 1,5 В. Диапазон рабочих частот - 130... 150 МГц. Значение рабочей частоты выводится на жидкокристаллический дисплей. Имеет 3 канала кварцованных частот: А - 139,6 МГц, В - 139,8 МГц, С - 140,0 МГц. Чувствительность приемника не хуже 0,25 мкВ при отношении сигнал/шум на выходе РПУ 12 дБ. Время непрерывной работы - 2 часа. Предусмотрена автоматическая запись принимаемых сигналов на диктофон.

PK830-SS - приемник с габаритами, позволяющими размещать его в стандартной пачке сигарет: 85х54х20 мм, вес - 275 г. Источник питания - элемент с напряжением 9 В. Диапазон рабочих частот - 120... 150 МГц. Имеет 3 канала кварцованных частот: А - 139,6 МГц, В - 139,8 МГц, С - 140,0 МГц. Чувствительность приемника не хуже 0,25 мкВ при отношении сигнал/шум на выходе РПУ 12 дБ.

UXR1 - двухканальный радиоприемник, работающий в диапазоне частот 398...430 МГц. Может одновременно принимать передачи от двух радиомикрофонов с попеременным переключением каналов. Габариты - 48х66х 19 мм, электропитание - литиевая батарея напряжением 6 В, время непрерывной работы - 36-48 часов. Дальность приема сигналов 150-1000 м.

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

UXR5 - четырехканальный радиоприемник - аудиомагнитофон, размещенный в портфеле типа «дипломат». Рабочий диапазон - УВЧ. Оснащен автоматическим управлением и миниатюрным компьютером для опознавания голосов, перехватываемых радиомикрофонами в контролируемых помещениях. В блок входит аудиомагнитофон с автоматическим реверсом, рассчитанный на непрерывную запись в течение 2 часов. Внешний вид некоторых приемных устройств приведен на Рис. 11.

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

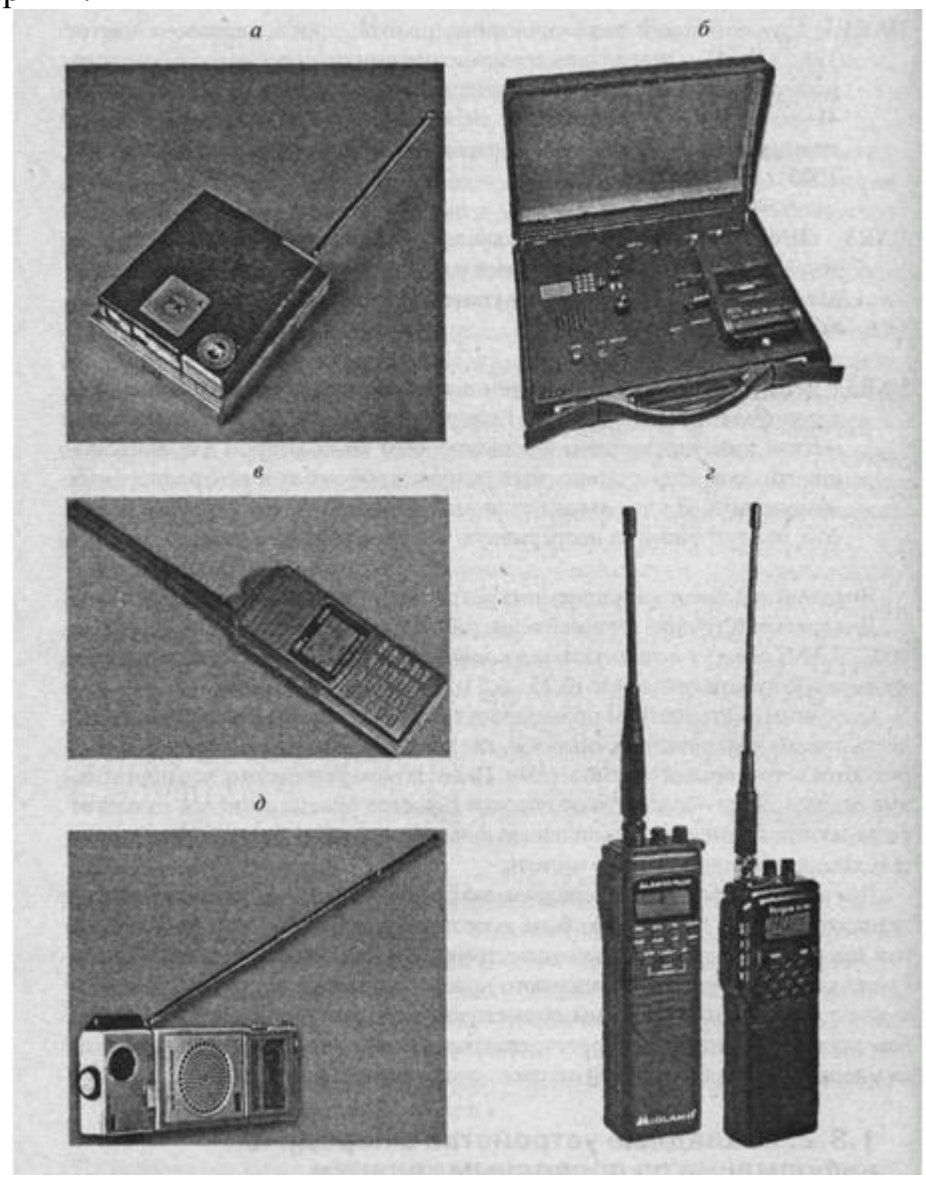


Рис. 11. Внешний вид приемников информации от радиозакладок

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

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

слабого сигнала радиозакладки на мощный сигнал ближайшей стационарной вещательной радиостанции.

2.2.4. Закладные устройства с передачей информации по проводным каналам

Техническая возможность применения токоведущих линий для передачи перехваченной акустической информации практически реализована в целом ряде ЗкУ. Наиболее широкое распространение получили закладки, использующие для этих целей сеть 220 В. Типовая схема организации негласного прослушивания переговоров с задействованием энергосети приведена на Рис. 12.

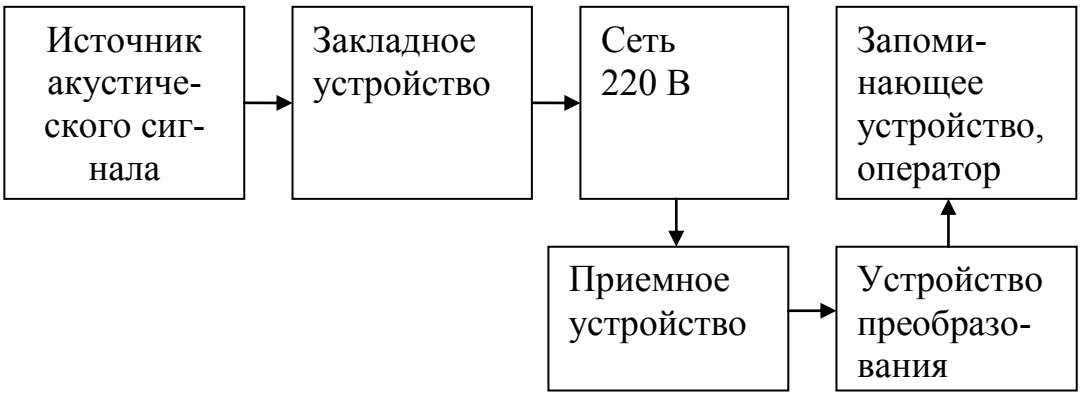


Рис. 12. Схема применения закладного устройства по силовой сети

Подслушивающие устройства устанавливаются в стандартную розетку или любой другой постоянно подключенный к силовой сети электроприбор (тройник, удлинитель, блок питания радиотелефона, факс и др.), расположенный в помещении, в котором ведутся переговоры интересующих лиц. Типовая схема такой закладки приведена на рис. 13.

Чувствительность внедренных микрофонов, как правило, обеспечивает надежную фиксацию голоса человека или группы лиц на удалении до 10 м. Дальность передачи информации лежит в пределах от 300 до 1000 м. Она обеспечивается за счет применения выходного усилителя с мощностью 5...300 мВт и амплитудной или частотной модуляции несущей, специально сформированной в задающем генераторе закладного устройства. Несущая модулируется информационным сигналом, прошедшим предварительное усиление в низкочастотном (НЧ) усилителе, и через высокочастотный (ВЧ) усилитель и специальное согласующее устройство излучается в линию. Частота передаваемого сигнала лежит в диапазоне 50...300 кГц. Выбор данного участка обусловлен тем, что, с одной стороны, на частотах ниже 50 кГц в сетях электропитания относительно высок уровень помех от бытовой техники, промышленного оборудования, лифтов и т. д. С другой - на частотах выше 300 кГц существенно затухание сигнала в линии, и, кроме того, провода начинают работать как антенны, излучающие сигнал в окружающее пространство. Од-

нако в некоторых случаях используются колебания с частотами, достигающими 10 МГц. Электропитание ЗУ осуществляется от той же сети, 220 В. Приемное устройство, расположенное вне пределов контролируемого помещения и подключенное к той же сети, перехватывает информационный сигнал и преобразует его в вид, удобный для прослушивания через головные телефоны, а также запись на магнитофон.

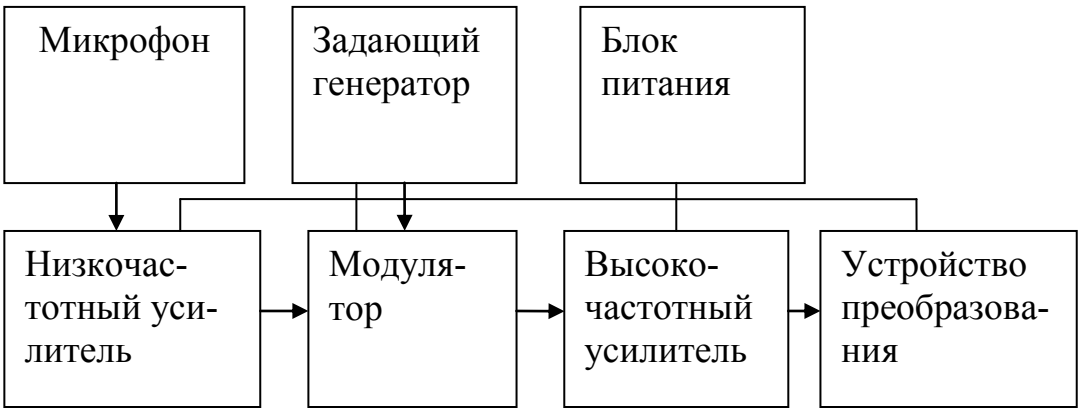


Рис. 13. Структурная схема закладного устройства

Схема приемника приведена на рис. 14. Принимаемый сигнал поступает на ВЧ-усилитель через согласующее устройство, затем детектируется и через НЧ-усилитель подается на головные телефоны или магнитофон. Чувствительность такого устройства, как правило, лежит в пределах от 3 до 100 мкВ, а питание осуществляется от батареек (аккумуляторов).

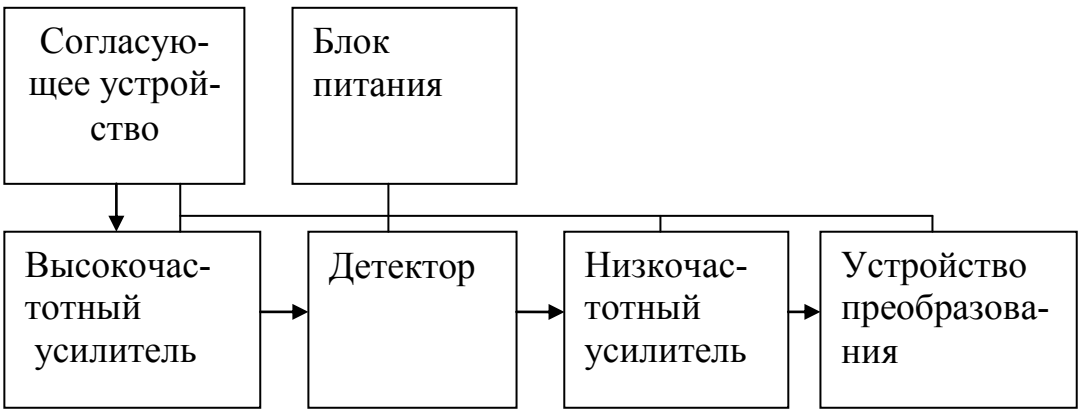


Рис. 14. Структурная схема приемного устройства

В некоторых случаях для одновременного прослушивания нескольких помещений, используются многоканальные системы. При этом ЗкУ работают на различных фиксированных частотах, а оператор выбирает на приемном устройстве канал, необходимый для прослушивания в каждый конкретный момент времени (Рис. 15, а).

В целом устройства контроля акустической информации с передачей по сети 220 В обладают существенными преимуществами перед другими ЗУ. Так, например, по сравнению с радиозакладками - повышенной скрытностью (поскольку невозможно ее обнаружение с помощью радиоприем-

ных устройств), а также практически неограниченным временем непрерывной работы, так как не требуют периодической замены источников питания. По сравнению с обычными про водными микрофонами (Рис. 15, б), использующими собственные проводники для передачи сигнала, - практически невозможно точно выявить место установки приемного оборудования.

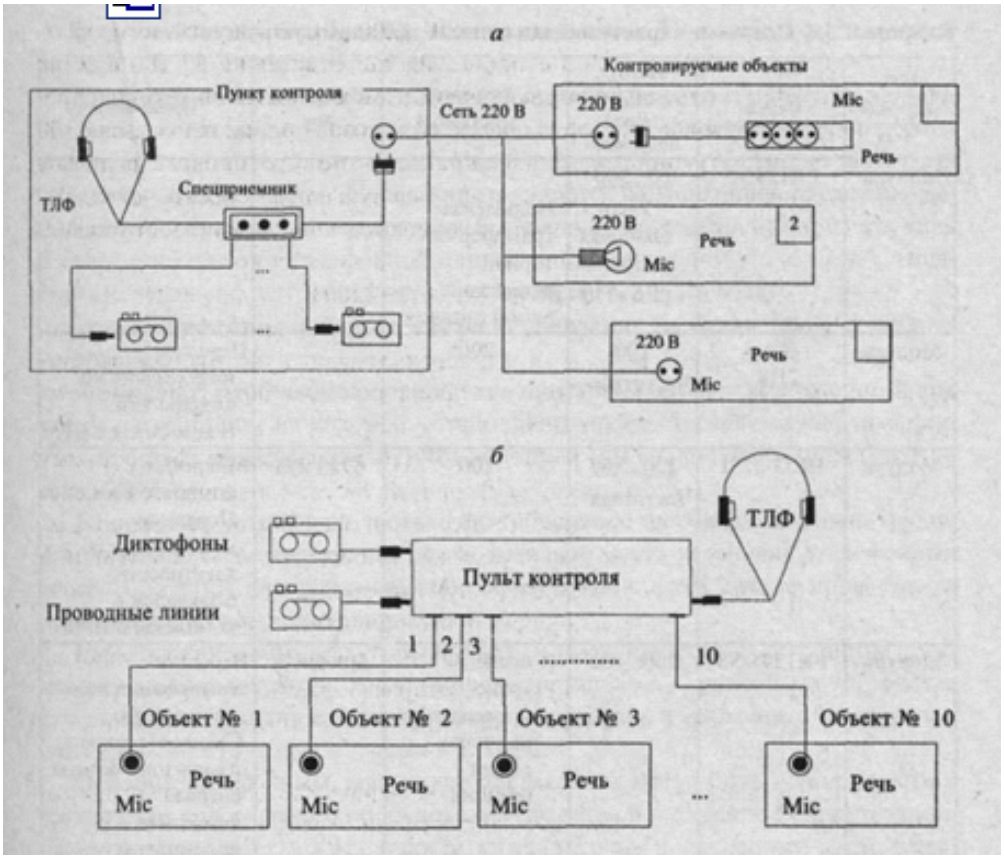


Рис. 15. Многоканальные закладные устройства

Ограничения многоканальных закладных устройств:

- работа возможна только в пределах одной фазы электропроводной сети;
- на качество перехватываемой информации влияют различные сетевые помехи;
- прибор, в который внедрено ЗкУ, может быть случайно отключен от сети переменного тока.

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

Технические характеристики некоторых сетевых ЗкУ с передачей информации по сети 220 В приведены в Приложении табл. П2

Аналогично системам с передачей информации по сети 220 В функционирует и аппаратура акустического контроля с передачей информации по телефонной сети. В состав изделий входят те же блоки, используется тот же частотный диапазон. Отличительной особенностью является блок питания, предназначенный для преобразования напряжения телефонной линии к требуемому уровню. В связи с тем, что от телефонной линии

нельзя потреблять более 2 мА, мощность передающих устройств не может превышать 10... 15 мВт. Однако существуют определенные ограничения на их применение:
- необходимо подключать приемную аппаратуру именно к той телефонной линии, на которой установлено устройство съема информации, что упрощает обнаружение пункта контроля (по сравнению с передачей по сети 220 В);
- устройство достаточно габаритное и его относительно трудно использовать скрытно, так как все возможные места установки (телефонный аппарат, розетки, распределительное оборудование и т. д.) легко проверить, в отличие от системы электропроводки.

Вышеперечисленные факторы привели к тому, что данные устройства практически не используются. Подобно телефонным, для установки закладок могут быть использованы и другие сети слаботочного оборудования (пожарной и охранной сигнализации, радиотрансляции и т. д.). Их недостатки аналогичны приведенным выше, в связи с этим и реальное применение крайне редко.

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

UM104 - сетевая закладка, предназначенная для прослушивания служебных и жилых помещений путем передачи и приема акустической информации по сети переменного тока. Дальность передачи (по проводам) - не менее 30 м; словесная разборчивость (при отсутствии помех) - 90 %; электропитание закладки - сеть 220 В; питание приемника - 4 батареи . Закладка устанавливается вместо стандартной стенной розетки или встраивается в электробытовые приборы. При установке в нишу стенной розетки UM104 полностью выполняет все ее функции и допускает подключение электроприборов мощностью 1,5 кВт. Отличительной способностью спецприемника является подключение к силовой сети только одним проводом, что обеспечивает повышенную безопасность и удобство в эксплуатации. Выбор провода для подключения определяется небольшим экспериментом и по лучшему качеству прослушивания. Контроль переговоров разрабатываемых лиц ведется на головные телефоны.

IPS MCX - акустическая закладка с передачей информации по сети переменного тока. Скрытно устанавливается в одном из бытовых приборов. Диапазон используемых для передачи частот - до 120 кГц; рабочее напряжение 100...260 В переменного тока с частотой 50/60 Гц; диапазон передаваемого акустического сигнала - 300...3500 Гц; модуляция - узко-полосная частотная; габариты - 33х67х21 мм.

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

РК170 - телефонная закладка с рабочей частотой около 100 кГц, вес -

180 г, габариты - 130х30х20 мм. Используется частная модуляция. В комплекте поставляется приемник (вес 750 г). Закладку производитель рекомендует устанавливать либо непосредственно в телефонном аппарате, либо в телефонной розетке.

2.2.5. Направленные микрофоны.

В начале 90-х годов направленные микрофоны вызывали повышенный интерес у организаций и частных лиц, которые занимались вопросами сбора информации с помощью технических средств. Это было связано с тем, что очень немногие люди ранее имели дело с данной техникой, а различные буклеты отечественных и зарубежных фирм рекламировали «универсальное средство получения информации». В технических описаниях приводились фантастические данные о дальности съема информации (до 2000 м) и коэффициентах направленного действия (до 50 дБ) при достаточно скромных габаритах (не более полуметра) и относительно невысокой стоимости (50...800 $). Под впечатлением от таких характеристик у потенциальных клиентов в голове возникали планы безопасного и простого перехвата речевой информации с помощью замечательного направленного микрофона.

Однако результаты попыток применения микрофонов обескураживали. Для того чтобы оценить возможности направленных микрофонов и степень опасности необходимо понять используемые в приборах физические принципы. Ибо без этих знаний невозможно организовать успешную защиту своих секретов от подобных преступных посягательств. В наиболее общем виде любой направленный микрофон можно представить как некоторый комплекс, состоящий из чувствительного элемента (собственно микрофона), осуществляющего акустико-электрическое преобразование, и антенны, обеспечивающей направленные свойства.

Микрофон (от греч. mikros - малый и phone - звук) - это электроакустический прибор для преобразования звуковых колебаний в электрические. В зависимости от принципа действия микрофоны делят на следующие типы:

- порошковые угольные;
- электродинамические;
- электростатические (конденсаторные);
- полупроводниковые;
- пьезоэлектрические, пьезокерамические;
- электромагнитные.

Порошковый угольный микрофон впервые был сконструирован русским изобретателем М. Махальским в 1878 году и позже, независимо от него, П. М. Голубицким в 1883 г. Принцип действия такого микрофона основан на том, что угольная или металлическая мембрана под действием звуковых волн колеблется, изменяя плотность и, следовательно, электрическое сопротивление угольного порошка, находящегося в капсюле и прилегающего к мембране. Вследствие неравномерного механического

давления сила тока, протекающего через микрофон, изменяется и преобразует акустический сигнал в электрический. Однако в интересах съема информации микрофоны данного типа практически не используются из-за их низкой чувствительности и большой неравномерности амплитудно-частотной характеристики.

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

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

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

В электромагнитном микрофоне звуковые волны воздействуют на мембрану, жестко связанную со стальным якорем, находящимся в зазоре постоянного магнита. На небольшом расстоянии вокруг якоря намотана обмотка неподвижной катушки. В результате воздействия акустических волн на такую систему на выводах обмотки появляется ЭДС. Данные изделия так же, как и порошковые угольные микрофоны, не получили широкого распространения из-за большой неравномерности амплитудно-частотной характеристики. Характеристики перечисленных типов микрофонов приведены в Табл. 2

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

борчивость речи) зависит не только от типа микрофона. Важное значение имеют и характеристики электронного блока, состоящего из микрофонного усилителя и головных телефонов. В большинстве же случаев, из экономических соображений, фирмы, поставляющие направленные микрофоны, комплектуют их дешевыми электронными блоками, соответствующими аппаратуре 3-го класса бытовой техники.

Табл. 2.

Характеристики микрофонов

Тип	Диапазон, Гц	Неравномерность воспроизводимых частот, дБ	Осевая чувствительность на частоте 1 кГц, мВм^2/н
Порошковые угольные	300-3400	20	1000
Электродинамические	30-15000	12	1
Конденсаторные	30-15000	5	5
Пьезоэлектрические	100-5000	15	50
Электромагнитные	300-5000	20	5

Поэтому владельцы таких средств зачастую вынуждены сами подбирать акустический усилитель и головные телефоны с требуемыми параметрами. Однако самое главное в направленных микрофонах - это свойства его акустической антенны.

Акустические антенны являются именно теми основополагающими элементами, которые определяют облик и основные характеристики комплексов дистанционного перехвата речевой информации. Назначение их заключается в пространственной селекции - усилении звуков, приходящих по основному направлению, и существенном ослаблении всех остальных акустических сигналов.

В настоящее время разработано несколько модификаций антенн, в соответствии с которыми существует следующая классификация направленных микрофонов, см. Рис. 16.: комбинированные; групповые, в том числе: линейные группы микрофонов; трубчатые приемники органного типа; трубчатые щелевые приемники; фазированные решетки; микрофоны с параболическим рефлектором.

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

Характеристика, или диаграмма направленности - это чувствительность микрофона в зависимости от угла 0 между рабочей осью микрофона и направлением на источник звука. Ее определяют или на раде частот, или в пределах полосы частот. Обычно используют нормированную характеристику направленности $R(\theta)$, то есть зависимость отношения чувствительности E_o измеренной под углом, к осевой (максимальной) чувствительно-

сти $E_{ос}$ $R(\theta) = E_o / E_{oc}$

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

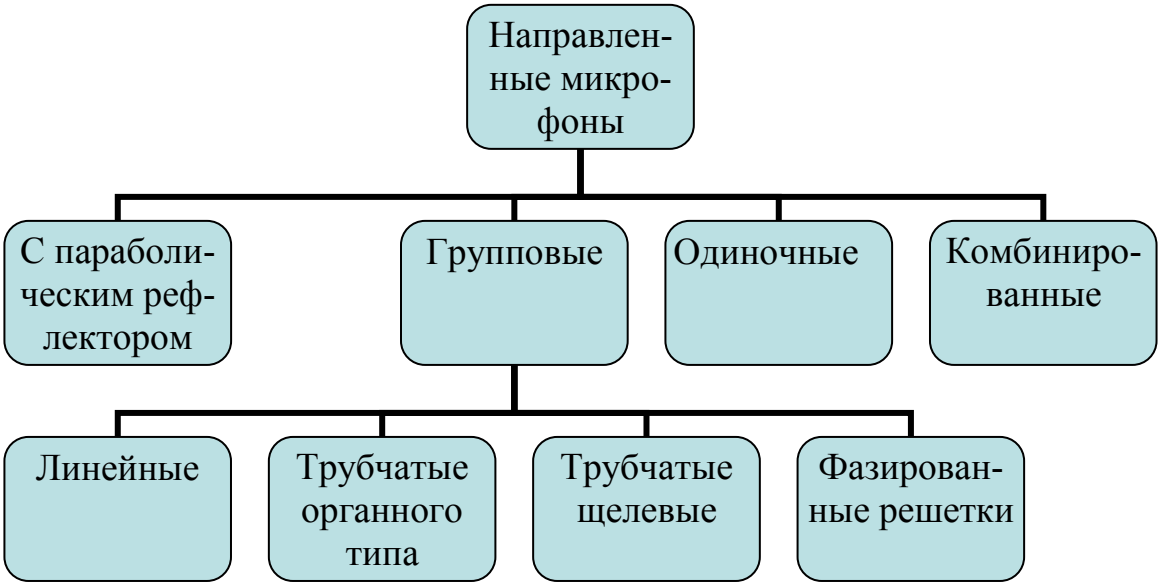


Рис. 16. Направленные микрофоны

Индекс направленности показывает выраженную в децибелах разницу уровней мощности сигналов на выходе микрофона от двух источников звука: одного (например, голоса человека), расположенного на оси, и другого - источника рассеянных звуковых волн (например, шума автотрассы), если оба создают в точке расположения микрофона одинаковое акустическое давление. Иными словами, индекс направленности показывает величину подавления (дискриминации) шума, приходящего с бокового направления, по отношению к сигналу, приходящему с направления, совпадающего с осью микрофона.

Ненаправленный микрофон не подавляет шума, поэтому его индекс направленности равен нулю (0 дБ).

Коэффициент направленного действия показывает выраженную в децибелах степень увеличения уровня сигнала на выходе микрофона при замене ненаправленного микрофона направленным при постоянной величине акустического давления.

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

Простейшая комбинация этих приемников, наиболее часто применяемая на практике, состоит из одного микрофона-приемника давления и одного микрофона-приемника градиента давления, располагаемых как

можно ближе друг к другу (обычно один над другим) и так, чтобы их оси были параллельны.

Изменяя параметры микрофонов, можно получать различные характеристики направленности и соответственно индексы направленности всей системы. Наибольший индекс достигается для случая, когда диаграмма имеет вид гиперкардиоиды (6 дБ).

К групповым акустическим приемникам относятся линейные группы, трубчатые микрофоны и фазированные решетки. Линейная группа приемников (микрофонов) - это несколько микрофонов, обычно располагаемых в ряд по прямой горизонтальной линии так, чтобы их оси были параллельны друг другу, иногда микрофоны располагают по дуге. Электрические выходы акустических приемников последовательно соединяют в специальном смесителе.

Характеристика направленности такой линейной группы из N-элементов определяется как произведение характеристики направленности одиночного приемника на характеристику линейной группы.

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

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

Трубчатый микрофон органного типа так же использует свойства групповых антенн. Такой микрофон имеет в своем составе несколько десятков тонких трубок с длинами от нескольких сантиметров до метра и более. Эти трубки собирают в пучок - длинные по середине, короткие - по наружной поверхности. Концы трубок с одной стороны образуют плоский срез, входящий в предкапсюльный объем. Сам микрофонный капсюль выбирается, как правило, электродинамического или электромагнитного типа (приемника давления) в зависимости от требуемого частотного диапазона. Звуковые волны, приходящие к приемнику по осевому направлению, проходят в трубки и поступают в предкапсюльный объем в одинаковой фазе. Их амплитуды складываются арифметически.

Звуковые волны фонового шума, приходящие под углом 0 к оси, оказываются сдвинутыми по фазе, так как трубки имеют разную длину, поэтому амплитуды этих волн складываются геометрически

Характеристика направленности для такого направленного микрофона определяется из соотношения, аналогичного для линейной группы приемников. Приведенные явления справедливы в случае, если в трубке не

образуются резонансные колебания. С этой целью входные отверстия трубок либо их концы у капсюля закрывают при помощи пробок из пористого поглотителя.

Основным достоинством таких направленных микрофонов является высокий индекс направленности (около 8 дБ, при этом шумы, действующие с боковых направлений, ослабляются по отношению к сигналу почти в 10 раз). Основной недостаток - довольно большие геометрические размеры (максимальная длина трубок около 90 см).

Трубчатый щелевой приемник (иногда его называют приемником бегущей волны) - представляет собой трубку с отверстиями или сплошной осевой прорезью по всей длине.

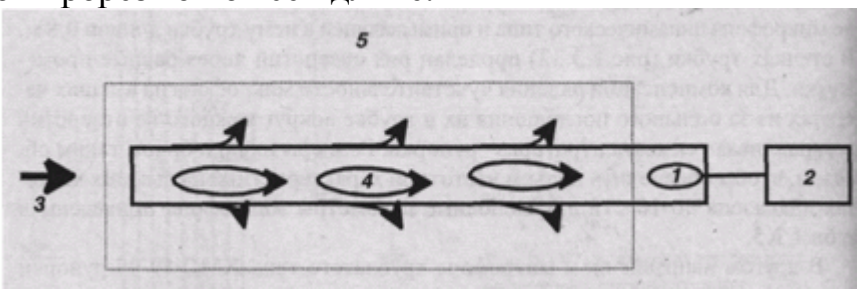


Рис. 17. Трубчатый щелевой приемник

С некоторым приближением такую трубку можно рассматривать как множество трубок разной длины, поэтому трубчатый щелевой микрофон и относят к приемникам группового типа. Если звук приходит по оси, то пути его распространения по трубке и через отверстия одинаковы и составляющие звукового давления от пришедших колебаний синфазны и, следовательно, сумма их, воздействующая на диафрагму микрофонного капсюля, максимальна.

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

Данный тип направленного микрофона получил наибольшее распространение по следующим причинам:

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

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

Отечественный остронаправленный микрофон **МД-74** состоит из собственно микрофона динамического типа и примыкающей к нему трубки длиной 0,8 м. В стенках трубки проделан ряд отверстий через равные промежутки. Для компенсации падения чувствительности микрофона на

высших частотах из-за большого поглощения их в трубке вокруг каждого из отверстий устанавливаются концентраторы. Размеры их подобраны таким образом, чтобы обеспечить подъем частотной характеристики на высших частотах диапазона до 10... 12 дБ. Основные параметры микрофона приведены в табл. 3.

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

Табл. 3.

Характеристики трубчатых щелевых остронаправленных микрофонов

Тип	Диапазон частот, Гц	Неравномерность частотной характеристики, дБ	Чувствительность холостого хода на частоте 1 кГц, мВм ² /н	Размеры	Масса, кг
МД-74	10-10000	8	1.2	Ø71-810	0.5
КМС-19-05	20-20000	8	45	Ø24-850	0.28
КМС-1909	20-20000	8	30	Ø24-203	0.19
МКЕ-802	50-15000	7	13	Ø22-292	0.18

Следует отметить, что многие направленные микрофоны трубчатого типа комплектуются ветрозащитным чехлом, обычно из поролона, благодаря чему снижается чувствительность к помехам от ветровых атмосферных воздействий.

Фазированные решетки обеспечивают синфазное сложение звуковых полей от источника в некотором акустическом сумматоре, на выходе которого расположен микрофон. Если звук приходит с осевого направления, то все сигналы, распространяющиеся по звуководам, будут в фазе, и сложение в акустическом сумматоре даст максимальный результат. Если направление на источник звука не осевое, а под некоторым углом к оси, то сигналы от различных точек приемной плоскости будут разными по фазе и результат их сложения будет меньше. При этом число приемных

точек может достигать нескольких десятков. Очевидно, что подобная решетка является менее громоздкой, чем микрофон органного типа, но она существенно проигрывает в направленных свойствах.

Примером направленного микрофона такого типа является изделие «Шорох». Оно относится к устройствам, предназначенным для прослушивания и записи речевой информации в условиях открытого пространства, в диапазоне частот 100... 10 000 Гц. Предельная паспортная дальность съема информации - 30-40 м при уровнях шума 74...76 дБ и речи 70...74 дБ. Однако в зависимости от шумовой обстановки и уровня информации дальность съема будет изменяться. Микрофон выполнен в виде гибкой пластины размером 320х320 мм, имеющей на внешней поверхности (от оператора) большое число акустических входных отверстий. За счет звуководов и суммирующих устройств образуется фазированная решетка, позволяющая сформировать диаграмму с шириной основного лепестка около 30...40° на частоте 1 кГц. Коэффициент направленного действия составляет около 12 дБ. Микрофон, размещенный в специальном чехле, может устанавливаться на теле оператора, под одеждой в варианте «грудь-спина» (фронт-тыл). На поясе чехла размещен манипулятор, состоящий из усилителя низкой частоты с автоматической регулировкой усиления, источника питания и органов управления: «включено-выключено» с первоначальной установкой уровня полезного сигнала и два выхода на магнитофон и головные телефоны. Функциональные возможности изделия могут расширяться за счет дополнительной установки радиоканала и других сервисных устройств. Конструктивные особенности позволяют легко камуфлировать микрофон под папку, дипломат, картину и т. д. Так как работа в помещении характеризуется наличием большого количества переотраженных сигналов от различных элементов строительных конструкций в виде стен, потолков, колонн, то максимальная эффективность работы такого направленного микрофона достигается в помещениях с объемом более 500 м^3. Рекомендуется избегать использования двух слоев одежды поверх микрофона, один из которых утеплен или выполнен из кожи (кожзаменителя). Полезный сигнал можно записывать без предварительного контроля, но при этом следует помнить, что расстояние до источника звука не должно, более чем 4-5 раз, превышать расстояние, при котором обеспечивается требуемое качество записи, выполненной ненаправленным микрофоном.

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

Принцип действия направленного микрофона с параболическим рефлектором состоит в том, что микрофон размещен в фокусе отражателя параболической формы. Звуковые волны с осевого направления, отража-

ясь от параболического зеркала, суммируются в фазе в фокальной точке. Возникает усиление звукового поля. Чем больше диаметр зеркала, тем большее усиление может обеспечить устройство. Если направление прихода звука не осевое, то сложение отраженных от различных частей параболического зеркала звуковых волн, приходящих в фокус, даст меньший результат, поскольку не все слагаемые будут в фазе. Ослабление тем сильнее, чем больше угол прихода звука по отношению к оси. Создается, таким образом, угловая избирательность по приему. Устройство поставляется в комплекте: блок усиления с системой автоматической регулировки усиления и выходами на наушники и магнитофон.

В качестве примеров направленных микрофонов с параболическим отражателем рассмотрим несколько систем. Портативный параболический приемник **PRO-200** предназначен для дистанционного приема звуковых волн. Обладает высокой чувствительностью и острой диаграммой направленности параболического зеркала. Оборудован дополнительным регулируемым фильтром, позволяющим осуществлять частотную селекцию сигнала по ширине и положению его спектра на оси частот. Паспортная дальность - 1 км. Имеется возможность подключения к магнитофону. Питание - от встроенного аккумулятора или внешнего зарядного устройства от сети 220 В. Диаметр зеркала - 60 и 75 см. Качество приема улучшается с увеличением диаметра, значения коэффициента направленного действия (КНД) антенны в зависимости от диаметра зеркала и частоты принимаемого акустического сигнала приведены в табл. 4.

Табл. 4.

Зависимость коэффициента направленного действия антенны от размера и частоты принимаемого сигнала

Частота, Гц	КНД для Ø зеркала 0.6 м	КНД для Ø зеркала 0.75 м
500	1	11
1000	15	17
5000	19	31
10000	35	37

Другой направленный микрофон **А-2** имеет параболический отражатель диаметром 0.43 м, снабжен усилителем и наушниками. Паспортная дальность действия на открытой местности также заявлена около 1км. Коэффициент усиления электронного блока - не менее 80 дБ. Имеется система автоматической регулировки усиления с динамическим диапазоном входных сигналов 40 дБ. Питание от стандартной батарейки 9 В. Предусмотрен разъем для подключения магнитофона.

Параболические направленные микрофоны **РК375** и **РК390** (производство Германии) имеют следующие параметры. **РК375**: габариты - Ø 600х300 мм, масса - 1,2 кг, коэффициент усиления - 90 дБ, питание - 5 В, автономность - 75 часов.

РК390, соответственно: Ø 130х100 мм, 1,1 кг, 70 дБ, 9 В, 50 часов.

Паспортная дальность - до 50 м.

Особенности оперативного применения направленных микрофонов таковы, что неподготовленный человек не сможет их скрытно использовать, так как необходимо не только правильно расположиться относительно объекта разведки и источников шумов, но при этом и самому не быть обнаруженным. Последнее практически невозможно в случае использования направленных микрофонов с параболическими отражателями из-за их существенных размеров. Специалисты рекомендуют применять такие микрофоны только в условиях ограниченной видимости и при относительно низких уровнях окружающих шумов - ночью, в парках, сельской местности и т. п. При этом честно информируют, что акустический телескоп может не улавливать звуки на большом расстоянии, если он используется недалеко от автомагистралей или в местах с повышенным уровнем фонового шума.

Перспективы развития направленных микрофонов. Конструкция направленных микрофонов непрерывно совершенствуется, так как проблема дистанционной записи речи становится все более актуальной в рамках развития систем негласного съема информации. Однако революционного переворота в данной области техники не предвидится.

Перспективы развития направленных микрофонов:

- адаптивная пространственно-временная фильтрации акустических помех;
- использование нелинейных и параметрических эффектов обработки звуковых сигналов.

Особенности применения направленных микрофонов

Так как на дальность ведения разведки влияют не только параметры микрофонов, но и условия, в которых применяются эти устройства, следует знать некоторые особенности использования направленных микрофонов. К открытой местности обычно относят участки, не имеющие ярко выраженных ограждающих конструкций, которые создают замкнутый объем. Как правило, это улицы, площади, стадионы, дворы, парки, залы летних кафе, пляжи и т. п. К работе на открытых площадках относят и прослушивание разговоров, ведущихся в помещениях, если перехват ведется через открытое окно, форточку или опущенное стекло автомобиля.

Основными ограничениями на ведение негласного съема информации в таких условиях является затухание, которое испытывает сигнал при его распространении, и высокий уровень фоновых шумов.

Величина затухания обусловливается рядом факторов, которые зависят как от характеристик самого звука, так и от свойств среды распространения:

- при распространении в неограниченной среде от источника конечных размеров интенсивность звука убывает обратно пропорционально квадрату пройденного расстояния;
- неоднородности среды вызывают рассеяние звуковых волн, приво-

дящее к ослаблению сигнала;

- на распространение звука в атмосфере влияют турбулентности, распределения температуры и давления, сила и скорость ветра, которые вызывают искривление звуковых лучей, а иногда вообще нарушают передачу звука;

- поглощение звука возрастает пропорционально частоте;

- размещать микрофон следует как можно выше над поверхностью земли, чтобы обеспечить максимальную геометрическую дальность перехвата акустических сигналов.

Высокий уровень акустических шумов - специфика открытых пространств. Для осуществления оценки влияния их на качество фиксации акустической информации используют понятие уровня громкости, под которым понимают уровень равногромкого с мешающим сигналом чистого тона на частоте 1000 Гц, выраженный в децибелах. За единицу уровня принимают один Фон. В табл. 5 /1/ приведены уровни громкости различных шумов в зависимости от дальности источника. Сравнивая приведенные значения с уровнем обычной речи, который составляет 65...75 дБ, делают вывод о степени влияния акустических помех на качество перехвата.

Табл. 5.

Уровни громкости различных источников звука

Источник шума и место его измерения	Уровень громкости, дБ
Автомобильный гудок на расстоянии 8 м	95 - 100
Электропоезд на эстакаде, на расстоянии 6 м	90
Шум в поезде метро во время движения	85 - 90
Автобус на полном ходу, на расстоянии 5м	85 - 88
Трамвай, на расстоянии 10 - 20 м	8 0 - 85
Троллейбус, на расстоянии 5 м	77
Грузовой автомобиль, на расстоянии 5 - 20 м	60 – 75
Легковой автомобиль, на расстоянии 5 – 20 м	50 – 65
Шумная улица без трамвайного движения	60 – 75
Обычный средний шум на улице	55 - 60
Тихая улица	30 - 35
Тихий сад	20
Шумное собрание	65 - 70
Шепот на расстоянии 1 м	20
Разговор на расстоянии 1 м	55 - 70
Коридор	35 – 40
Кафе	50 - 52

Некоторые предельные дальности регистрации приведены в табл. 6. /1/.

Табл. 6.

Предельные дальности акустической регистрации

Звуковые сигналы	Пределы слышимости, м
Шаги человека по грунту	30 – 100
Громкий разговор	200 – 300
Негромкий разговор	100 - 200
Резкая команда голосом, крик	500 - 1500

Из вышесказанного следует, что на дальность фиксации речевой информации на открытом участке местности влияют следующие факторы: направление и сила ветра, температура и влажность воздуха, характер рельефа, наличие строений, растительность, уровни фоновых шумов. Дальность ведения разведки увеличивается, если ветер дует со стороны источника звука, ночью и ранним утром, в пасмурную погоду, особенно после дождя, у водной поверхности, в горах, зимой (при отсутствии снегопада). Звук поглощается (становится слабее) в жаркую солнечную погоду, во время снегопада, дождя, в лесу, кустарнике и на местности с песчаным грунтом, при наличии искусственных и естественных препятствий.

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

Отличительной особенностью применения направленных микрофонов в помещениях является более сложное звуковое поле полезного сигнала, которое представляет из себя суперпозицию составляющей «прямого» звука, созданной звуковыми волнами, не испытавшими ни одного отражения, и составляющих, созданных несколькими отраженными звуковыми волнами. Поле отраженных звуковых волн почти всегда близко к диффузному. Акустические шумы в помещениях так же, как и на открытой местности, существенно ограничивают динамический диапазон принимаемой информации, снижают разборчивость речи. Эти шумы создаются как людьми, так и вибрациями, проникающими в помещение извне (с улицы или из соседних помещений). Уровни шумов, создаваемые людьми, зависят от их количества в помещении, громкости разговоров и т. д. Уровни шумов (вибраций), проникающих снаружи, определяются звукоизоляцией помещения и уровнями внешних шумов. В табл. 7 приведены санитарные нормы допустимых уровней акустических шумов, характерных для различных типов помещений /1/. Приведенные цифры позволяют составить представления об условиях перехвата речевой информации с помощью направленных микрофонов. Здесь уместно еще раз напомнить, что уровень обычной речи на расстоянии 1 м составляет 65...75 дБ.

Табл. 7.

Санитарные нормы уровня шумов в помещениях

Тип помещения	Норма шума, дБ
Для сна и отдыха	35
Для умственной работы	45
В цеху	55

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

2.2.6. Диктофоны

Осуществление негласной звукозаписи является одним из наиболее распространенных приемов промышленного шпионажа. Полученные записи используют для получения односторонних преимуществ в коммерческих сделках, оказания давления на партнеров, шантажа и т. д. Для того чтобы уберечь себя от подобных последствий, необходимо знать основные особенности скрытой звукозаписи, факторы, влияющие на качество фиксации информации, характерные приемы. Эти знания помогут обратить внимание на особенности поведения людей, пытающихся вас записать, правильно выбрать место конфиденциальной встречи, исключить нахождение «случайно забытых» вещей в вашем рабочем кабинете или офисе.

Факторы, влияющие на качество звукозаписи.

Уровень помех в помещении обычно выше уровня прямого звука. При акустическом отношении больше четырех отраженный звук создает недопустимые помехи для регистрации речевой информации.

Пороговое значение расстояния от источника звука, при котором акустическое отношение равно единице, называют радиусом гулкости, так как при большем расстоянии диффузная составляющая становится больше составляющей прямого звука, и в записанном сигнале появляется характерная гулкость.

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

$$S = (E_П + E_{60mc}) / E_m ,$$

где $E_п$ - плотности энергии прямого звука;

$E_{60мс}$ - плотность отраженных звуковых волн, приходящих в данную точку помещения в течение времени t=60 мс;

$E_м$ – общая плотность энергии.

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

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

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

К сожалению, внешние шумы не исчерпывают список помех, возникающих при негласной записи акустической информации. Дело в том, что закамуфлированный в одежде магнитофон записывает все окружающие его шумы, и в первую очередь создаваемые самим оператором, так как он, как правило, ближе всего расположен к микрофону. Так, например, люди дышат, а это значит, что одежда на них постоянно находится в движении - ремень поскрипывает от поднимающейся и опускающейся диафрагмы, пиджак трется о сорочку и т. д. Люди этого не слышат, однако, микрофон, спрятанный в одежде, улавливает все, и записанный разговор будет сопровождать невероятный фоновый шум. Самое большое неудобство для диктофонной записи - беседа на ходу. Здесь «фонит» все: рукава, трущиеся по мере размахивания руками, верхняя одежда, содержимое карманов (всякие ключики, мелочь, бумажки - все бряцает, шуршит и скрипит). Окружающие шумы также будут уловлены и записаны. И если в нормальной жизни мы их не слышим, используя природой данные фильтры, то при воспроизведении записи все будет воссоздано в самом неудобном виде. Рассмотренные факторы являются принципиальными при проведении негласной звукозаписи, и они должны учитываться при выборе места для микрофона звукозаписывающего устройства.

Выбор типа микрофона и места его установки

Многие современные диктофоны позволяют выбирать между встроенным и выносным микрофонами в зависимости от условий ведения звукозаписи. Конечно, встроенный микрофон делает устройство более компактным и эргономичным. Однако его возможности по ведению скрытой фиксации

аудиоинформации существенно ограничены, так как такие микрофоны обладают достаточно скромными характеристиками из-за предельно малых размеров, а их размещение полностью определяется размером и камуфляжем всего записывающего устройства.

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

При размещении выносных акустических приемников операторы, как правило, учитывают следующие три фактора:

1. количество записываемых источников речевых сигналов;
2. пространственная ориентация микрофона;
3. дальность до источника акустического сигнала.

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

Для фиксации диалога подходят как двусторонне, так и односторонне направленные микрофоны. В первом случае микрофон располагают между собеседниками, в последнем - его стараются установить так, чтобы оба объекта оказались симметрично расположенными относительно рабочей оси акустического приемника.

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

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

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

звука менее громкой на фоне других или же придать звучанию большую мягкость и меньшую четкость.

3. Величина расстояния до источника определяется, исходя из свойств помещения, в котором осуществляется аудиозапись, и свойств микрофона и источника. Восприятие источника зависит от того, в каком соотношении находятся расстояние от источника до микрофона и радиус гулкости помещения.

Если расстояние от источника до микрофона меньше радиуса гулкости, то при воспроизведении кажущиеся размеры источника звука больше фактических, а размеры окружающего пространства меньше фактических. При этом создается общее впечатление близости и интимности звучания. При расстоянии микрофона от источника больше радиуса гулкости, наоборот, размеры источника кажутся меньше фактических, а окружающего пространства - больше. Общее впечатление от звучания - объемность, «воздушность», мощность. При расположении микрофона от источника звука на расстоянии, равном радиусу гулкости, качество звучания при воспроизведении является промежуточным по сравнению с описанным выше.

2.3. Средства обеспечения скрытности оперативной звукозаписи

2.3.1. Средства обеспечения скрытной оперативной звукозаписи

Выше отмечалось, что в зависимости от используемой модели диктофон может иметь встроенный или выносной микрофон. Первый существенно уступает последнему по техническим характеристикам, а, кроме того, имеет меньшие возможности по скрытому применению. Поэтому на практике чаще используют выносные акустические приемники. Выносной микрофон может быть закамуфлирован под любой элемент личных вещей. Часто он изготавливается в виде пуговицы и вставляется в петлицу на одежде. А так как пуговицы взаимозаменяемые, то достаточно просто провести общую маскировку из предлагаемого ассортимента. Например, стандартный вариант - белая пуговица на светлой рубашке.

Широко применяются и выносные микрофоны в виде колпачка от авторучки, заколки для галстука и других предметов (как правило, они не вызывают никаких подозрений). Более простые устройства не имеют штатного камуфляжа, а благодаря своим небольшим размерам прячутся под одежду или в различных предметах (книге, папке, портфеле). В зависимости от типа используемого диктофона и расстояния от источника звука микрофоны могут оборудоваться дополнительным усилителем. Как правило, это делается в том случае, если микрофон устанавливается на значительном расстоянии от диктофона.

Необходимо упомянуть о миниатюрных диктофонах, которые используются для скрытной записи. Так, если ранее (в 30-50-е годы) наименьший размер магнитофона позволял разместить его в портфеле или папке, то в настоящее время не составляет труда приобрести в обычном магазине диктофон, который свободно помещается в пачке сигарет. Наиболее часто в

интересах промышленного шпионажа применяются диктофоны типа **SONY-909M, SONY-950, NATIONAL-RNZ-36, OLYMPUS-L400. К** сожалению, часть устройств не снабжена внутренним динамиком, поэтому прослушивание записи в них приходится осуществлять через внешний акустический блок или наушники.

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

У **OLIMPUS-S928** или **SONY-359,** цена которых составляет от 35 до **100** $, качество записи похуже, к тому же изделия такого класса часто не имеют гнезда для подключения выносного микрофона.

В ряде случаев используют и магнитофоны, имеющие увеличенные по сравнению с описанными выше диктофонами габариты. Они, как правило, соответствующим образом маскируются или используются для дистанционной записи, а фиксация информации в них осуществляется на стандартную кассету, как, например, в диктофонах **РК660** и **РК670.** Стандартным вариантом камуфляжа для РК660 и РК670 является книга со специальным вырезом для акустического сигнала.

Все основные типы портативных диктофонов, используемых в интересах промышленного шпионажа, отвечают, как правило, следующим требованиям к техническим характеристикам: диапазон частот 200 - 5000 Гц, коэффициент детонации (коэффициент колебания скорости ленты) - до 4 %, остаточный уровень шумов - 30 дБ, коэффициент гармоник - до 10 %, разборчивость слогов - 60...80 % при доверительной вероятности не хуже 0,9. Некоторые марки современных диктофонов и их технические возможности приведены в Приложении табл. П3, а внешний вид - на Рис. 18.

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

Некоторые диктофоны имеют неприятные особенности управления - выключаться с характерным щелчком выстреливаемых кнопок или после окончания кассеты включать обратную перемотку, что также может вылиться в нежелательные последствия. Бывают экземпляры с программируемым управлением и таймером, автоматически включающиеся на воспроизведение в самый неподходящий момент (поэтому если во время разговора у вашего собеседника в кармане, что-то щелкнуло, то будьте готовы к тому, что вся предыдущая беседа уже на пленке).

Другой важной проблемой является емкость записи. Поэтому человек, осуществляющий скрытую аудиозапись, вынужден постоянно следить за временем беседы для того, чтобы не выйти за кассетное время. Это ино-

гда весьма неудобно. Для увеличения времени записи в некоторых диктофонах, как отмечалось выше, используется пониженная скорость лентопротяжного механизма (меньше 1,2 см/с), но качество записи при этом существенно ухудшается и иногда даже становится проблематично идентифицировать разговор.

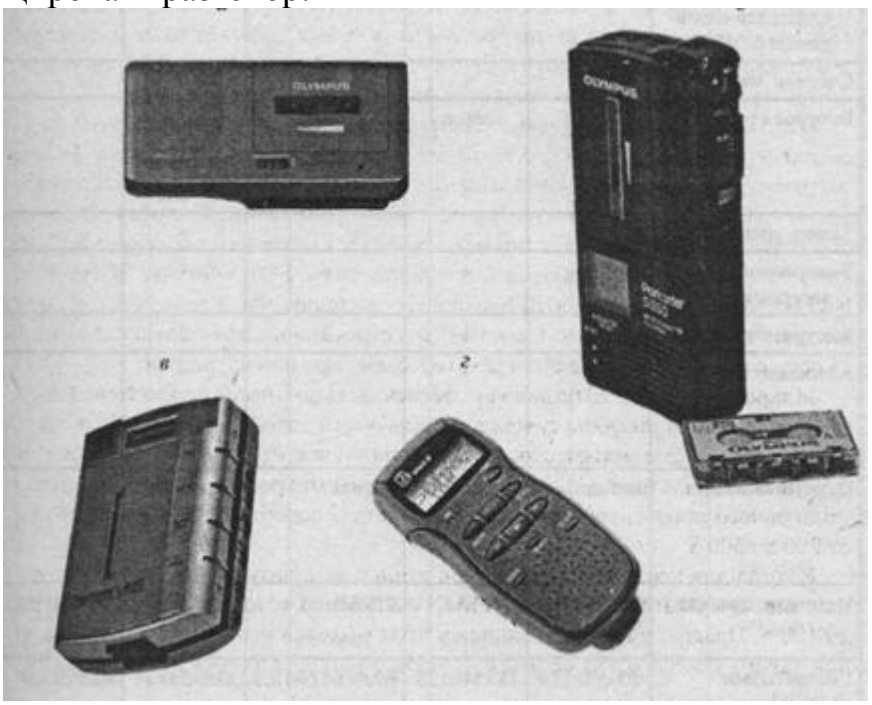


Рис. 18. Внешний вид диктофонов: а – OLYMPUS-L250; б – OLYMPUS - 950; в - OLYMPUS-L400; г – цифровой диктофон – VR-5000

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

Главный недостаток – очень высокая цена, которая может достигать нескольких тысяч долларов. Другой путь - использование магнитофонов с электронной записью звука. Например, диктофон **Edic** способен непрерывно вести фиксацию акустических сигналов в течение 1...2 суток, сохраняя последние 20-40 мин записи. Диктофон незаменим для звуковой регистрации неожиданных ситуаций, так как нет необходимости нажимать кнопку «Пуск» при внезапном интересе к какой-либо информации, она автоматически запишется, и будет храниться до 40 мин пока не «затрется» новой записью. Единственное неудобство для оператора – надо не забыть нажать на «Стоп» после окончания интересующего разговора. Небольшие габаритные размеры (105x55x14 мм) позволяют легко камуфлировать диктофон. В нем нет движущихся частей, поэтому его применение сложно обнаружить. Комплектуется выносным микрофоном и зарядным устройством для встроенных аккумуляторов.

Более современными вариантами являются малогабаритные цифро-

вые стереофонические диктофоны NT-1 и NT-2 фирмы SONY.

Табл. 8.

Характеристики профессиональных кассетных магнитофонов

Характеристики	UHER CR-1600	UHER CR-1601	MARANTZ PMD-201	MARANTZ PMD-221
Скорость движения ленты, см/с	4.7; 1.2	4.7; 2.4; 1.2	4.7; 2.4	4.7; 2.4
Диапазон частот, Гц :				
- для скорости 4.7 см/с	300-16000	300-16000	40-14000	40-15000
- для скорости 2.4 см/с			40-8000	40-8500
- для скорости 1.2 см/с	600-3400	600-3400		
Отношение сигнал/шум	70	70	57	57
Длительность перемотки	90	90		
Количество головок	2	3	2	3
Режим работы	стерео	моно		
Размеры, мм			228x51x165	228x51x165
Масса, кг			1.3	1.3

Главное достоинство данных устройств - наличие специальных бесшумных кнопок и высокое качество записи. Дополнительные возможности создает встроенный календарь и часы, автоматически регистрирующие и сохраняющие время начала и конца записи.

Для увеличения времени непрерывной записи используют реверсивные системы. Однако и здесь не каждая модель может быть использована, так как при переключении записи на реверс некоторые диктофоны (а их, к сожалению, большинство) издают довольно громкий щелчок, о чем говорилось выше. Иногда для экономии ресурсов используют функцию включения по голосу акустомат. Но здесь, как и у закладного устройства, «съедается» начало первой фразы. Если порог срабатывания выставлен некорректно, то возможен пропуск целых предложений.

Для экономии пленки в ряде случаев используется система дистанционного включения. В простейшем случае она представляет собой переключатель, соединенный проводом с соответствующим разъемом на диктофоне, а при отсутствии специального разъема используется доработанный вход по питанию. Система внешнего включения должна содер-

жать переключатель с четкой фиксацией положения, чтобы в стрессовых ситуациях оператор был уверен, что его диктофон действительно работает. Иногда используют специальные системы включения, например, в виде зажима для авторучки. В случае, когда авторучка находится в зажиме, расположенном во внутреннем кармане, диктофон выключен, а когда она извлечена - производится запись.

Некоторого преимущества при использовании диктофонов позволяет достичь дистанционного включения по радиоканалу. Данная техника предназначена для применения устройств аудиозаписи в качестве закладки. Запуск диктофона производится специальной командой, передаваемой радиопередатчиком. Например, устройство дистанционного управления РК1670 имеет передатчик мощностью 1 Вт и дальность действия 500 м. Габариты приемника команд - 25х58х18 мм, вес - всего 55 г. Подключается приемник к соответствующему разъему магнитофона. Существенно увеличить время непрерывной звукозаписи позволяет использование диктофонов с записью на жесткий проволочный носитель, изготовленный из специальных сплавов. Их память может простираться на сутки и более. Однако в будущем они, видимо, не найдут широкого применения для вышеуказанных целей. Это связано в первую очередь с такими недостатками, как трудность соединения проволоки при монтаже и обрывах, появление паразитной амплитудной модуляции сигнала из-за скручивания носителя, неудовлетворительная передача верхних частот, довольно высокая стоимость, сильный износ головок.

Перспективным по-прежнему остается применение цифровых диктофонов. Тем более, в последнее время появились диктофоны нового типа - с записью в память персональной ЭВМ. Например, цифровая система регистрации переговоров **«Аудиокод».** Данная система предназначена для записи информации, ее сжатия (компрессии), хранения с автоматическим удалением устаревших материалов и прослушивания информации. Область фиксируемых звуковых частот канала «запись-воспроизведение» лежит в диапазоне 300...3000 Гц. Система защищена от несанкционированного доступа. Обеспечивается одновременная регистрация переговоров по 4 каналам с автоматической или ручной регулировкой уровня записи в каждом канале, реализована функция «эхо» (прослушивание записываемых каналов). Включение записи осуществляется по уровню входного сигнала или после нажатия клавиши. Кроме того, в диктофоне предусмотрен мгновенный доступ к любой записи базы данных, быстрый поиск по номеру канала и времени регистрации, прослушивание любой записи без прерывания процесса регистрации, воспроизведение с любого места, быстрый переход к любому участку фонограммы.

Для обеспечения цифровой записи в различных марках диктофонов используются различные форматы записи. К наиболее известным относятся следующие. **DAT (Digital Audio Tape)** - формат цифровой магнитной записи звука на специальную DAT-кассету, время непрерывной работы ко-

торой достигает двух часов, а в режиме Long Play (LP) - четырех часов. Запись ведется вращающимися головками, как в видеомагнитофонах, а магнитная лента движется со скоростью всего 8,15 мм/с.

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

DCC (Digital Compact Cassete) - цифровая компакт-кассета (изобретение фирмы Philips), выпущенная на рынок в 1992 году. Основным достоинством DCC-системы является полная совместимость с обычными компакт-кассетами. Цифровая звукозапись ведется с помощью стационарной многодорожечной головки при стандартной скорости протяжки ленты, при этом исходный звуковой сигнал подвергается многократному сжатию с помощью адаптивного алгоритма, учитывающего психологические особенности восприятия звука человеком. Стоимость первых образцов DCC-магнитофонов также оказалась высокой, а качество звука довольно низким, и это решило их судьбу - они не нашли широкого применения. Качество звучания впоследствии удалось существенно улучшить, однако доверие к новой системе было подорвано. Сейчас фирма Philips производит DCC-магнитофоны, в том числе и портативные, которые можно приобрести в магазинах по цене от 700$. Несомненный интерес представляет возможность воспроизводить на этих аппаратах записи, сделанные на компакт-кассетах обычным способом. Однако ограниченное распространение этого формата затрудняет его внедрение в практику.

MD (Mini Disc) - мини-диск - разработан фирмой Sony. Конструктивно он напоминает 3,5-дюймовую компьютерную дискету диаметром 64 мм. Материал, из которого изготовлен диск, меняет свои оптические свойства под воздействием магнитного поля. Запись на минидиск осуществляется магнитной головкой, при этом поверхность диска в зоне действия магнитного поля разогревается лучом лазера. Считывание информации про-

исходит также с помощью лазера, но меньшей мощности. Таким образом, информация сохраняется на диске даже в случае воздействия сильных магнитных полей и появляется возможность многократной (до 1 млн. раз) перезаписи. На мини-диск можно записать стереозвук продолжительностью до 74 мин, а некоторые модели мини-дисковых аппаратов позволяют вести монофоническую запись в течение 148 мин.

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

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

NT (Non Tracking) - «бездорожечный» принцип записи на специальную микро- кассету - разработан и реализован фирмой Sony в диктофонах NT-1 и 1 NT-2. В них запись производится вращающимися со скоростью 3000 об/мин головками на ленту шириной 2,5 мм, которая движется со скоростью 6,35 мм/с. Это обеспечивает запись стереозвука в диапазоне 10 - 14 000 Гц при соотношении «сигнал/шум» 80 дБ. Цифровой звуковой сигнал записывается без сжатия. Продолжительность записи составляет 60, 90 и 120 минут в зависимости от типа микрокассеты. Диктофон весит 147 г, имеет габариты 113x23x55 мм. К недостаткам диктофонов следует отнести их высокую стоимость (порядка 2000 $).

Для улучшения разборчивости речи, полученной в результате скрытой звукозаписи, используют различные «очищающие» фильтры. Они

особенно эффективны, если фиксация информации осуществлялась на фоне мощных, но сосредоточенных по спектру помех или специфически «окрашенных» шумов. В простейшем случае можно использовать широко известные эквалайзеры. Однако часто этот прием не помогает, поэтому применяют специально разработанные устройства. Например, цифровой нелинейный адаптивный фильтр **АФ-512** специально предназначен для обработки зашумленных речевых сигналов в реальном масштабе времени. Его рабочая полоса лежит в пределах от 200 до 5000 Гц, а коэффициент нелинейных искажений не превышает 0,5 %, габариты - 300х200х80 мм. При обработке записей на фоне сосредоточенных помех фильтр позволяет увеличить разборчивость речи в 1,5... 5 раз. Правда, фильтр недостаточно эффективен, если помехой будут быстрая музыка, шум или речь. Более совершенными являются специальные программно-аппаратные комплексы очистки речи, например «Золушка-97». Это двухканальное цифровое устройство шумоочистки речевых сигналов. Оно предназначено: для очистки «живого» звука и звукозаписей; для повышения разборчивости и качества речи в условиях низкого качества каналов связи; для выделения источника звука в условиях «шумного» производства.

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

2.3.2. Устройства высокочастотного навязывания

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

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

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

Принцип организации съема информации, основанный на зондировании, показан на Рис.19.

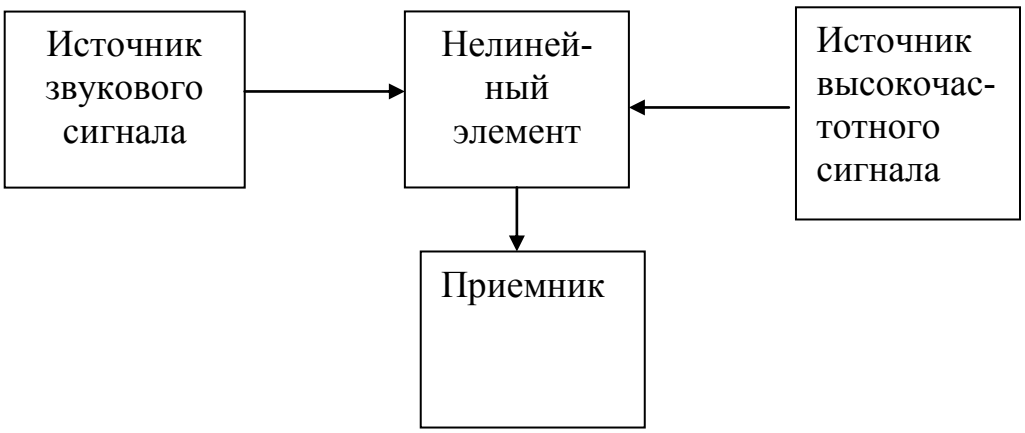


Рис. 19. Принцип организации съема информации путем высокочастотного навязывания

Недостатки - как правило, малая дальность действия и высокие уровни облучающих сигналов, наносящие вред здоровью людей. Данные обстоятельства существенно снижают ценность ВЧ-зондирования. Однако определенные методы, о которых будет рассказано в дальнейшем, получили достаточно широкое распространение. Общее представление о многообразии методов такого перехвата дает Рис. 20.

2.3.3. Устройства для перехвата речевой информации в проводных каналах

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

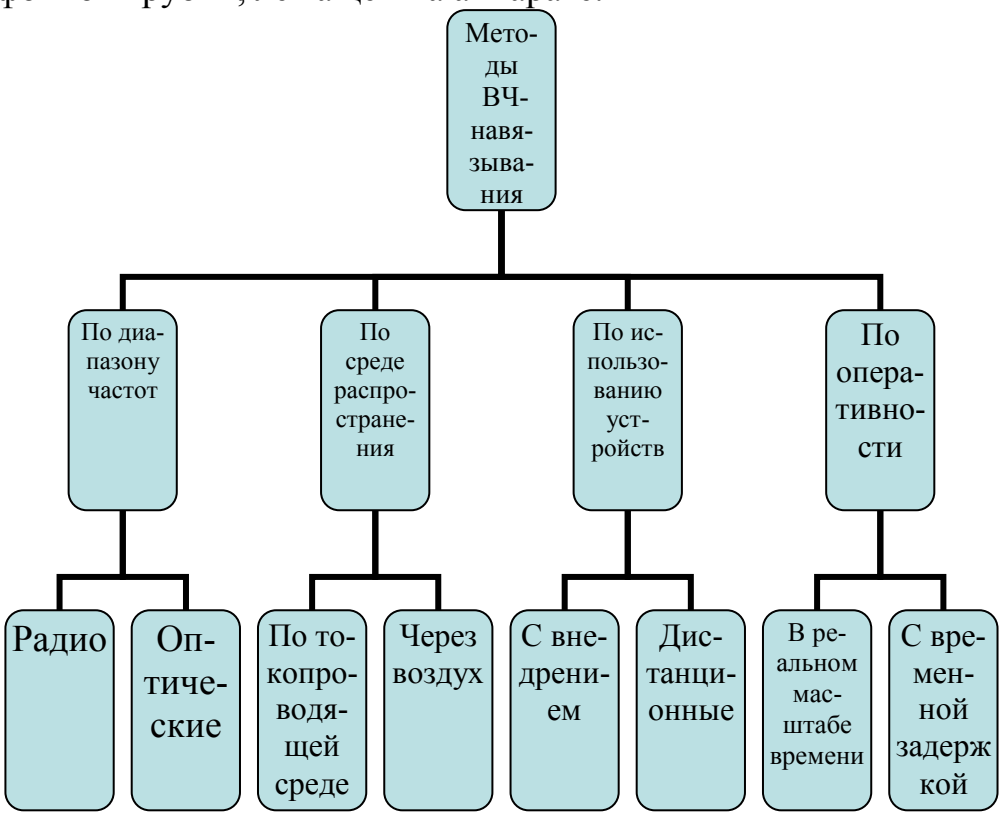


Рис. 20. Классификация методов перехвата аудиоинформации с использованием высокочастотного навязывания

Принцип реализации метода заключается в том, что в телефонную линию относительно общего корпуса (в качестве которого, например, используют контур заземления или трубы парового отопления) на один из проводов подают ВЧ-колебания от специального генератора-передатчика (ПРД), см. Рис. 21.

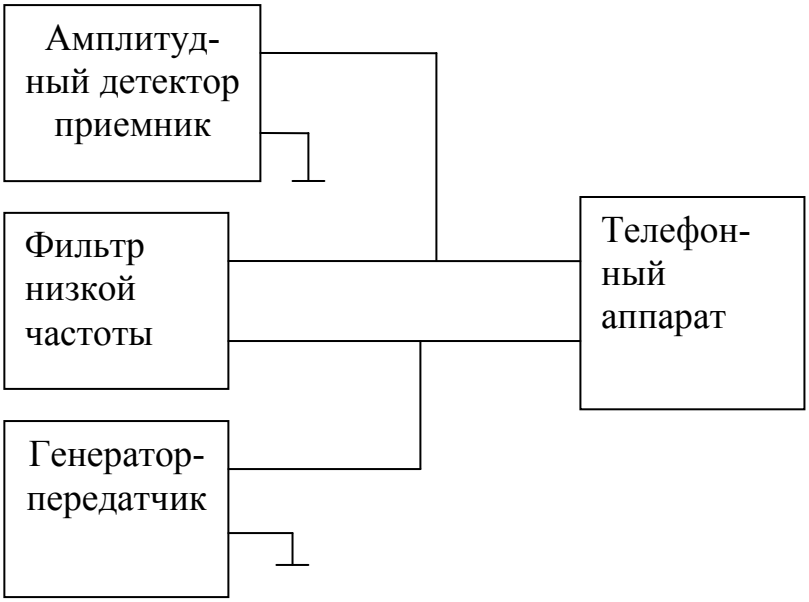


Рис. 21. Принцип перехвата речевой информации в проводных каналах телефонии

Через элементы схемы телефонного аппарата (ТА), даже если трубка не «снята», они поступают на микрофон и модулируются речью ничего не подозревающих собеседников.

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

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

При воздействии ВЧ-излучения на телефонный аппарат нелинейные процессы происходят в целом ряде элементов его электрической схемы. Однако наиболее сильно они проявляются именно в микрофоне, сопротивление которого изменяется по закону случайно воздействующего акустического сигнала, что и приводит к амплитудной модуляции несущей. Для гарантированного возникновения указанного эффекта уровень зондирующего сигнала в микрофонной цепи должен быть не меньше 150 мВ, а

выходное сопротивление генератора должно быть выше, чем у микрофона, в 5-10 раз. Частота зондирующего сигнала должна лежать в диапазоне 30 кГц...20 МГц. Чаще ее выбирают примерно равной 1 МГц, так как при этом обеспечиваются наилучшие условия распространения.

Схема устройства, реализующего вышеописанный метод, приведена на Рис. 21. В ней умышленно отсутствуют номиналы элементов, что не позволяет реализовать ее на практике. Дальность действия подобных устройств в реальных условиях не превышает нескольких десятков метров. В перспективе в области использования проводных каналов, вероятно, будут осваиваться способы зондирования не только телефонных аппаратов, но и других устройств, в том числе по цепям питания, заземления и т. д.

Перехват речевой информации с использованием радиоканала

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

Так, постоянный представитель США при ООН Генри Кэбот Лодж на одном из заседаний Совета Безопасности продемонстрировал в разобранном виде подслушивающее устройство, выполненное в виде гипсового орла - герба Соединенных Штатов Америки. Этот герб был подарен американскому дипломату - послу Соединенных Штатов Америки в Москве Аверелллу Гарриману в 1945 году и провисел на стене кабинета в общей сложности при четырех послах. Только в начале 50-х годов специалисты по обнаружению скрытых электронных средств нашли вмонтированное в герб подслушивающее устройство.

Инициатор создания программы ЦРУ по разработке миниатюрных средств оперативной техники Питер Карлоу вспоминает, что «мы нашли его, но долго не знали принцип действия. В гербе находилось пассивное устройство, похожее на головастика с маленьким хвостом». Таким образом, долгое время советское руководство имело возможность получать актуальную, очень важную оперативную информацию, что давало нам определенные преимущества в прогнозировании и осуществлении мировой политики в сложный период «холодной войны». Имеются данные о том, что, даже зная, что в кабинете посла находится подслушивающее устройство, специалисты обнаружили его только тогда, когда вынесли из кабинета практически всю мебель. В наших разведывательных кругах ходили тогда слухи, что первые подозрение появились у американцев после одной из речей Н. С. Хрущева, когда в результате анализа сведений, высказанных им, специалисты пришли к выводу, что источник утечки информации находится в посольстве США в Москве. Опубликование информации о необычном закладном устройстве явилось сенсационным еще и потому, что США было заявлено об отсутствии у них аналогичной спецтехники. Она

явилась для них полной неожиданностью. Также сообщалось, что Соединенные Штаты приступили к разработке подобных систем съема информации. И действительно через много лет американцы создали у себя аналогичный вид техники съема информации, который и внедрили в советское посольство за рубежом.

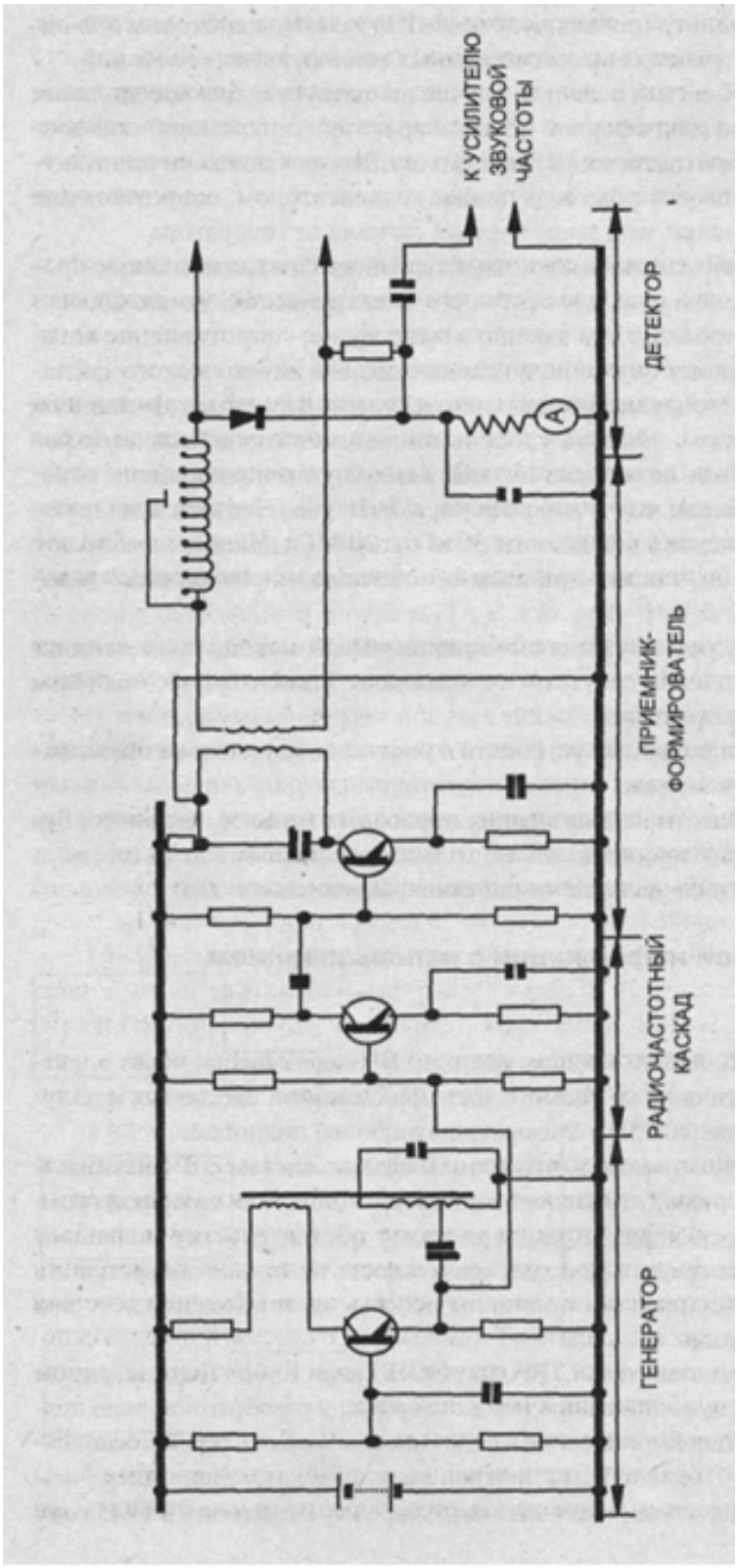


Рис. 22. Схема высокочастотного устройства перехвата речевой информации через телефонный аппарат

Автором и ведущим руководителем проекта первого пассивного закладного устройства был выдающийся изобретатель Лев Сергеевич Термен. Большой Энциклопедический Словарь уделил ему несколько строк. Родился в 1896 году. Советский физик. Музыкант. В 1920 году изобрел электромузыкальный инструмент «Терменвокс». В 1931-1938 годах - директор акционерного общества по производству электромузыкальных инструментов в США. С 1966 года - научный сотрудник кафедры МГУ. Известно, что Л. С. Термен лично демонстрировал В. И. Ленину свой инструмент, основанный на изменении тона звука генератора при поднесении рук к двум антеннам. В начале 30-х годов Термен после поездки остался в Америке, где основал акционерное общество. Помимо изготовления музыкальных инструментов он участвовал в оборудовании границы между США и Мексикой системой охранной сигнализации для регистрации незаконного пересечения границы нелегалами-мексиканцами. Принцип действия сигнализации такой же, как и аппарата «Терменвокс», емкостной, то есть основывался на регистрации изменений электрической емкости провода, натянутого вдоль границы, при приближении к нему человека. Когда Термен перед войной приехал туристом в СССР, он, по приказу Берии, был арестован и отправлен в организацию, подобную той, которая была описана А. И. Солженицыным в романе «В круге первом» под названием «шарашка». В эти годы (в середине 40-х) Л. С. Термен и создал свой шедевр, см. Рис. 23, которым до сих пор не устают восхищаться специалисты. Основой устройства является цилиндрический объемный резонатор, на дне которого налит небольшой слой масла.

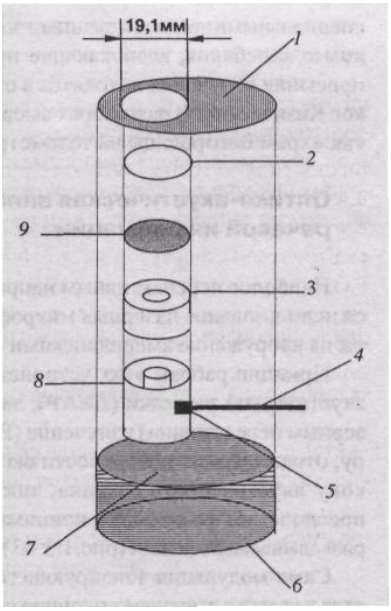


Рис. 23. Пассивный радиомикрофон: 1 - верхняя пластмассовая крышка; 2 - ферритовое кольцо; 3 - изолятор; 4 - антенна (четвертьволновой вибратор); 5 - согласующий конденсатор; б - корпус; 7 - жидкость; 8 - медный цилиндр (индуктивность); 9 - металлическая диафрагма

Верхняя часть закрыта крышкой из пластмассы, являющейся радио-

прозрачной для радиоволн, но препятствующей проникновению акустических колебаний. В крышке имеется отверстие, через него внутренний объем резонатора сообщается с воздухом помещения, в котором ведутся переговоры. В указанное отверстие вставлена металлическая втулка, снабженная четвертьволновым вибратором, настроенным на частоту 330 МГц. Размеры резонатора и уровень жидкости подобраны таким образом, чтобы вся система резонировала на внешнее излучение с частотой 330 МГц. При этом собственный четвертьволновый вибратор внутри резонатора создает внешнее поле переизлучения. При ведении разговоров вблизи резонатора на поверхности масла появляются микроколебания, вызывающие изменение добротности и резонансной частоты резонатора. Этих изменений достаточно, чтобы влиять на характеристики переизлученного поля, создаваемого внутренним вибратором. Сигнал становится модулированным по амплитуде и фазе акустическими колебаниями. Работать такой радиомикрофон может только тогда, когда он облучается мощным источником на частоте резонатора, то есть 330 МГц. Главным достоинством такого радиомикрофона является невозможность его обнаружения известными средствами поиска радиозакладок при отсутствии внешнего облучения. Наряду с пассивными закладками, аналогичными выше описанной, для съема информации используются и полуактивные закладки, называемые аудио-транспондерами; (ответчиками; Audiotransponder). К таким закладкам относятся, например, **S1M-ATP-16**, **SIM-ATP-40** (Hildenbrand-Elektronik), **PK500** (PK-Electronic) и некоторые другие.

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

Современные закладные устройства, реализующие вышеописанные принципы, имеют различные габариты и форму. Самые маленькие из них напоминают пластмассовую рыболовную блесну. Об их достаточно широком использовании говорит тот факт, что в 60-е годы американцы жаловались на постоянное облучение ВЧ-сигналами их представительства в СССР с целью активизации встроенных резонаторов.

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

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

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

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

Выводы по главе:

1. Перспективы развития направленных микрофонов:
- адаптивная пространственно-временная фильтрации акустических помех;
- использование нелинейных и параметрических эффектов обработки звуковых сигналов.

2. Качество перехвата аудиоинформации с помощью ВЧ-навязывания зависит от ряда факторов:
- характеристик и пространственного положения источника акустического сигнала;
- наличия в контролируемом помещении нелинейного элемента (устройства), параметры которого (геометрические размеры, положение в пространстве, индуктивность, емкость, сопротивление и т. д.) изменяются по закону акустического сигнала;
- характеристик внешнего источника, облучающего данный элемент;
- типа приемника отраженного сигнала.

Вопросы для самоконтроля:

Вопрос 1. Какие факторы учитываются при размещении выносных акустических?

Вопрос 2. Приведите ограничения многоканальных закладных устройств?

Вопрос 3. Приведите классификацию закладных устройств.

Методические рекомендации.

Изучив материал главы, ответьте на вопросы. При возникновении трудностей обратитесь к материалам для закрепления знаний в конце пособия.

Для углубленного изучения воспользуйтесь литературой:

основной: 1 – 3; дополнительной: 5 – 6 и повторите основные определения, приведенные в конце пособия.

ГЛАВА 3. СРЕДСТВА ОПТИКО-АКУСТИЧЕСКОГО ПЕРЕХВАТА РЕЧЕВОЙ ИНФОРМАЦИИ

3.1. Оптико-акустическая аппаратура перехвата речевой информаци

3.1.1. Устройства оптико-акустического перехвата информации.

Наиболее перспективным направлением в области ВЧ-навязывания является использование лазерных микрофонов, первые образцы которых были приняты на вооружение американскими спецслужбами еще в 60-е годы. Принцип работы этих устройств, получивших название лазерные системы акустической разведки (ЛСАР), заключается в следующем. Генерируемое лазерным передатчиком излучение (ВЧ-сигнал) распространяется через атмосферу, отражается от поверхности оконного стекла, модулируется при этом по закону акустического сигнала, также воздействующего на стекло, повторно преодолевает атмосферу и принимается фотоприемником, восстанавливающим разведываемый сигнал, см. Рис. 24.

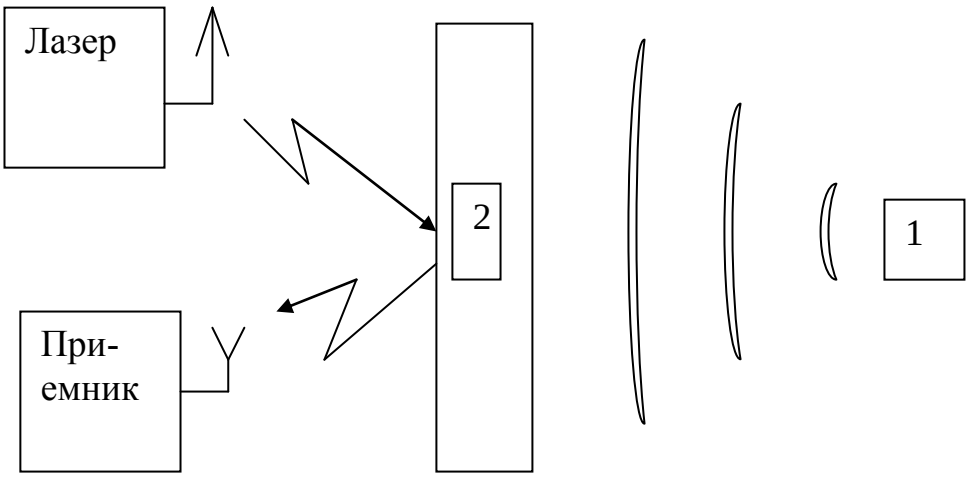


Рис. 24. Принцип работы оптико-акустическая аппаратура перехвата речевой информации: 1 - источник сигнала; 2 – оконное стекло

Сама модуляция зондирующего сигнала на нелинейном элементе, в качестве которого выступает оконное стекло может быть представлен в следующем виде:

1. Звуковая волна, генерируемая источником акустического сигнала, падая на границу раздела воздух-стекло, вызывает отклонения поверхности стекла от исходного положения. Отклонения приводят к дифракции света, отражающегося от этой границы. Отклонения границы от стационарного состояния представляют собой бегущую вдоль стекла «поверхностную» волну с амплитудой, пропорциональной амплитуде смещений среды в поле звуковой волны.

2. Отраженный от возмущенной поверхности свет содержит сдвинутые по частоте дифракционные компоненты. Если поперечный размер па-

дающего пучка лазерного излучения значительно превышают длину «поверхностной» волны, то отраженный свет представляет собой совокупность дифрагирующих пучков, распространяющихся по различным направлениям.

В результате в отраженных пучках присутствуют три вида модуляции оптического излучения. Во-первых, частотная модуляция, вызванная эффектом Доплера, вследствие колебательных движений оконного стекла под воздействием акустических сигналов. Во-вторых, фазовая модуляция, вызванная наличием в отраженном сигнале как зеркально-отраженного, так и дифракционных компонентов. Результат суперпозиции последних приводит к тому, что если поперечные размеры падающего оптического пучка малы по сравнению с длиной «поверхностной» волны, то в отраженном сигнале будет доминировать дифракционный пучок нулевого порядка. В этом случае и окажется, что фаза световой волны будет промодулирована во времени с частотой звукового сигнала.

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

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

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

3.1.2. Примером современных лазерных систем перехвата информации

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

ный блок компенсации помех, а также треноги поставляются в комплекте устройства. Вся аппаратура размещена в небольшом чемодане. Электропитание - от батареи.

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

Характеристики некоторых видов ЛСАР приведены в Приложении табл. П4, а внешний вид - на Рис. 25.

Рис. 25. Внешний вид лазерной системы акустической разведки

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

Дальнейшее развитие лазерных систем, вероятнее всего, пойдет по пути уменьшения массогабаритных характеристик устройств за счет ис-

пользования современных полупроводниковых лазеров, оптических устройств и средств первичной обработки сигналов с использованием ЭВМ.

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

1. аппаратура, использующая принцип ВЧ-навязывания,- реальное средство несанкционированного получения речевой информации;
2. эффективность ее применения зависит от следующих факторов:

- уровня речи;
- расстояния от пункта контроля до объекта;
- технических характеристик аппаратуры и средств вторичной обработки перехваченных сигналов;
- погодных условий;
- степени подготовки лиц, использующих технические средства разведки.

3.2. Оптические средства добывания конфиденциальной информации.

3.2.1. Оптико-механические приборы.

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

Однако мудрая природа, дав людям такой важный для восприятия окружающего мира прибор, существенно ограничила его возможности. Так, основными характеристиками человеческого глаза являются следующие: - мгновенное угловое поле зрения: в горизонтальной плоскости составляет 65...95°; в вертикальной плоскости - 60...72°;

- расстояние наилучшего зрения - 250 мм;
- область спектральной чувствительности лежит в диапазоне 0,37...0,72 мкм;
- максимальная восприимчивость для дневных условий соответствует темно-зеленому излучению с длиной волны 0,54 мкм (поэтому на зеленом цвете глаз «отдыхает»), а в сумеречное время - излучению с длиной волны 0,507 мкм - голубой цвет.

Естественно и вечное стремление людей расширить границы своего зрения. Люди старались улучшить все характеристики зрения и создали огромное количество оптических приборов:

- для увеличения дальности наблюдения: зрительные трубы, бинокли и телескопы;

- для расширения области спектральной чувствительности: приборы ночного видения;

- для расширения поля зрения: перескопы, системы телевизионного наблюдения;

- для фиксации изображения: фотоаппараты кино- и видеокамеры.

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

Принцип действия таких приборов основан на том свойстве, что один и тот же предмет виден под большим углом при меньшей дальности. Достоинством системы Кеплера является то, что в плоскости изображения может быть установлена сетка (шкала). Она позволяет решать измерительные задачи по определению дальности до объекта наблюдения, в то время как другие оптические системы не могут быть использованы для этих целей.

Для ведения скрытного наблюдения необходимо тщательно выбирать позицию с учетом местных условий и окружающего ландшафта. Хорошо для этих целей подходит густая листва деревьев, различные строения, места складирования крупногабаритных предметов. Однако в ряде случаев, оказывается, затруднительно выбрать удобное место, и наблюдение приходится вести из-за угла, через препятствие и т. п. В этом случае хорошую услугу могут оказать артиллерийские панорамы или другие оптические системы перископического типа, имеющие достаточно малые геометрические размеры входного объектива и изменяющие направление распространения оптических лучей. Простейший перископ может быть изготовлен своими силами с использованием всего двух параллельно расположенных зеркал.

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

ектив оптического прибора. Она предотвращает прямое попадание световых лучей на объектив и существенно ослабляет переотражение лучей за счет внутренних колец. В качестве примера современного оптико-механического прибора можно рассмотреть бинокль британской фирмы BCB International – габариты: 9.5x7x4 см, масса 200 г., линза диаметром 21 мм имеет мгновенный угол зрения 7^0 и 8 кратное увеличение, что дает возможность наблюдать за участком местности шириной 130 м на дальности 1000 м.

3.2.2. Приборы ночного видения.

Иногда возникают ситуации. Когда необходимо вести наблюдение в условиях плохой освещенности. Для этого предназначены приборы ночного видения. Их основные достоинства:

- возможность наблюдения в условиях слабой освещенность;
- меньшее по сравнению с видимой областью спектра затухание электромагнитных волн ИК-диапазона в осадках.

К недостаткам приборов следует отнести:

• значительно худшую разрешающую способность, связанную с большой длиной волны (человека, например, можно опознать только по силуэту, так как черты лица не распознаются);

• нечувствительность человеческого глаза к ИК-излучению.

Для того чтобы объединить достоинства оптико-механических приборов и ИК-приборов и уменьшить недостатки последних приборы ночного видения строятся по схеме, изображенной на Рис. 26.

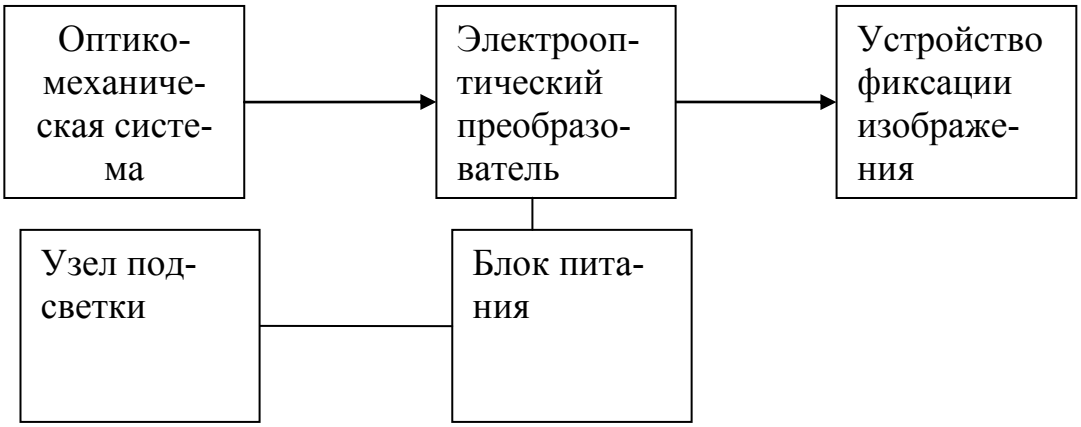


Рис. 26. Структурная схема прибора ночного видения

Оптико-механическая система аналогична рассмотренным выше оптико-механическим приборам, и именно она определяет такие характеристики прибора, как мгновенный угол поля зрения и кратность увеличения. Электрооптический преобразователь преобразует ИК-излучение в видимое, выводя его на небольшой встроенный экран. Эта часть устройства принципиально не работает без источника электрического питания, что можно отнести к еще одному из недостатков приборов ночного видения. В качестве

устройства фиксации изображения обычно выступает человеческий глаз или фотоаппарат.

Приборы ночного видения могут работать как в пассивном, так и в активном режиме. Пассивный режим применяется при наличии собственного излучения объекта наблюдения и в условиях слабого рассеянного излучения случайных искусственных или естественных источников, уровень которого превышает 10^{-5} лк. Активный режим используется в условиях полного отсутствия освещения. Он сопровождается применением источника подсветки объекта наблюдения. Таким источником может быть лазер, например полупроводниковый или на стекле с неодимом, или специальный ИК-прожектор. Прожекторы с мощностью излучения до 100-120 Вт функционируют, как правило, от автономных блоков питания с напряжением питания 12 В. Диапазон расстояний, подсвечиваемых такими прожекторами, варьируется в диапазоне 10-110 м, в зависимости от мощности источника и ширины луча, вид последнего формируется специальными насадками.

Технические характеристики ряда приборов ночного видения и источников подсветки приведены ниже, а внешний вид некоторых из них - на рис. 27 и 28.

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

РК1260-S - прибор ночного видения, предназначенный для получения фотоснимков объектов, находящихся на расстоянии до 10 км. Используется обычная фотопленка 35 мм.

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

РК305 - прибор ночного видения активного типа, предназначенный для наблюдения объектов в условиях полного отсутствия освещенности. Имеет объектив с фокусным расстоянием 135 мм и светосилой объектива F 2,8. ИК-прожектор имеет мощность 35 Вт и обеспечивает дальность наблюдения до 350 м. Собственный источник питания с напряжением 8 В обеспечивает время непрерывной работы 1,5 часа. Габариты прибора - 250x280x80 мм, вес - 1,3 кг.

Dedal-220 - монокулярный прибор ночного видения с угловым полем зрения прибора 28° в вертикальной и горизонтальной области. Диаметр объектива - 37 мм, светосила — F 1,0, кратность увеличения - 1,3. Усиление яркости изображения, создаваемое прибором, достигает 30 000. Габарит-

ные размеры - 122x58x58, вес - 8 кг. Время непрерывной работы - 40 часов.

Dedal-040 - прибор ночного видения, выпускаемый как в монокулярном, так и бинокулярном исполнении. Угловое поле зрения прибора в зависимости от конструктивного исполнения лежит в диапазоне 14°... 17°. Диаметр объектива - 85-100 мм, светосила - F 1,5...F 2,0, кратность увеличения - 1,9...3,2. Усиление яркости изображения, создаваемое прибором, достигает 50 000. Габаритные размеры монокуляра - 210x76x93, бинокуляра - 325x76x103 мм, вес, соответственно, 1,12 и 1,52 кг. Время непрерывной работы - 50 часов.

Рис. 27. Приборы ночного видения: а – монокуляр DEDAL-0410; б - монокуляр RETRON RN MO2; в - бинокуляр RETRON RN BO3 ; г – активный ночной наблюдательный прибор с лазерной подсветкой ; д – очки ночного видения OR11

Spylux - прибор ночного видения индивидуального применения. Заключен в прочный и компактный корпус, дает высококонтрастное изображение с

хорошим разрешением при низких уровнях освещенности. Прибор имеет окуляр с регулированием фокусировки, кнопку включения-выключения и держатель объектива типа С с адаптером, дающим возможность менять объектив в соответствии с условиями наблюдения. Стандартно прибор поставляется с объективом диаметром 75 мм и светосилой F 1,4. Масса прибора - 0,5 кг, напряжение питания - 2,0...5,0 В, потребляемый ток - 16 мА.

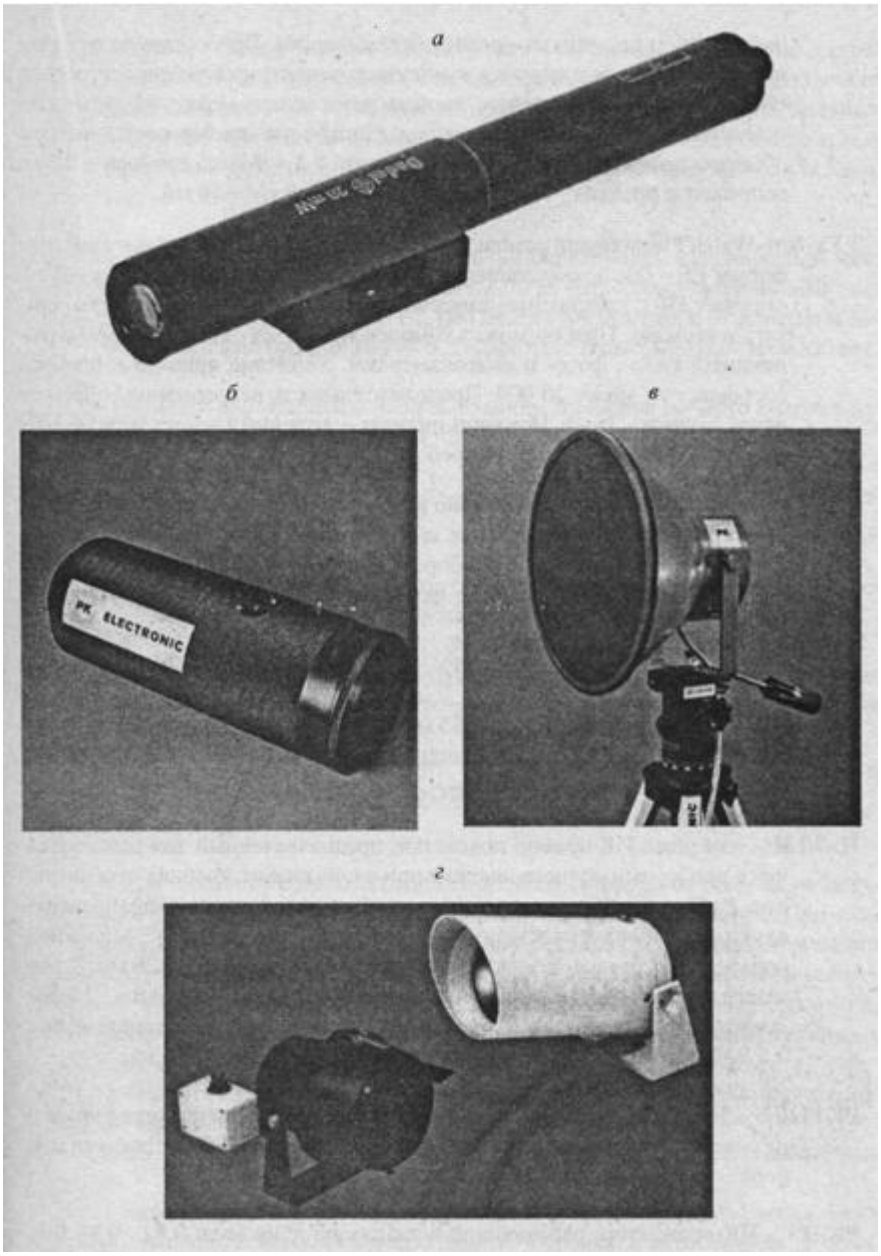


Рис. 28. Источники подсветки: а – лазерный источник излучения фирмы DEDAL; б - ИК - лазерный осветительный прибор РК765; в - ИК - прожектор РК325; г – ИК - прожектор фирмы Dennard

EEV Black Watch - прибор, специально разработанный для скрытного фотографирования и видеонаблюдения. Усиление яркости изображения, создаваемое прибором, достигает 2000000, что позволяет получать высококачественные фотографии в самых неблагоприятных условиях.

3.2.3. Источники подсветки приборов ночного видения.

РК765 - ИК-лазер с длиной волны 0,85 мкм и мощностью излучения в импульсе 180 мВт. Имеет форму цилиндра диаметром 65 мм и длиной 200 мм, напряжение питания - 12 В.

IL-7/LR - лазерный ИК-прибор подсветки, предназначенный для использования с приборами ночного видения при очень низких уровнях освещенности. Расходимость пучка регулируется от интенсивного карандашного пучка для точечной подсветки до пучка с расходимостью 40°. Масса прибора - 130 г с батареей электропитания, габариты - 63х50х20 мм. Длина волны излучения - 0,83 мкм, минимальная выходная мощность - 15 мВт. Электропитание - батарея литиевых элементов типа АА с напряжением 3,5 В. Продолжительность непрерывной работы – 5 - 20 часов.

РК1420-S - ИК-прожектор, предназначенный для подсветки фотографируемого объекта ИК-лучами. Дальность подсветки - 10-100 м. Диаметр прибора - 130 мм, длина - 240 мм, вес - 720 г.

РК325 - ИК-прожектор, работающий в диапазоне длин волн 0,82...0,98 мкм. Мощность - 110 Вт, дальность подсветки достигает 500 м. Напряжение питания - 220/110/12 В. Габариты: диаметр - 260 мм, длина - 200 мм. Вес - 2 кг.

Minilight 500 - миниатюрный ИК-излучатель на основе галогенной лампы. В зависимости от модификации мощность лампы может быть 20 или 50 Вт. Напряжение питания - 12 В. ИК-фильтр, предназначенный для задержки видимого света, пропускает излучение с длиной волны 0,84 мкм. Размеры источника излучения - 65х65х115 мм, масса - 350 г.

AVSIR-1/48V - светодиодный ИК-излучатель с длиной волны излучения 0,88 мкм. Минимальная дальность подсветки - 70 м, расходимость пучка - 30°, потребляемая мощность - 48 Вт. Питание осуществляется от источника постоянного напряжения 10-14 В. Габаритные размеры - 160х160х100 мм.

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

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

3.3. Средства для проведения фотосъемки.

3.3.1. Средства для проведения фотосъемки

Важным элементом промышленного шпионажа является получение документов, подтверждающих тот или иной вид деятельности конкурентов.

При этом фотоматериалы могут быть незаменимы при решении задач документального подтверждения конфиденциальных встреч, факта посещения объектом наблюдения определенных мест, а также при анализе особенностей малознакомой, труднодоступной местности или при решении задач копирования текстовых документов, рисунков, схем, чертежей в условиях дефицита времени. В зависимости от решаемых задач различают два вида фотосъемки: съемку объекта наблюдения и съемку документов: съемка объекта наблюдения и съемка документов.

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

- подбор объектива;
- определение точки производства фотосъемки.

Выбор времени экспозиции и степени открытия диафрагмы решаются достаточно просто при наличии фотоэкспонометра, определяющего величину светового потока, отраженного объектом и местными предметами. Прибор выдает несколько пар цифр, оптимальных для той чувствительности пленки, которая установлена в фотоаппарате. Например,

Время экспозиции, с	1/15	1/30	1/60	1/125	1/250	1/500
Диафрагменное число, к	16	11	8	5.6	4	2.8

любая комбинация из приведенных цифр (от 1/15 -16 до 1/500 - 2,8) обеспечит один и тот же уровень светового потока, воздействующего на фотопленку. Однако конкретная пара должна выбираться, исходя из условий и задач съемки. Так, при съемке движущихся объектов время экспозиции должно выбираться как можно меньше (например, 1/250 или 1/500 с) для того, чтобы уменьшить «смаз» изображения, вызванный перемещением объекта в момент съемки. При этом, как видно из приведенной ниже таблицы, степень открытия диафрагмы будет максимальна (диафрагменное число 4 или 2,8, соответственно). В свою очередь, это приведет к уменьшению глубины резкости изображения. Например, при съемке объективом Гелиос-44М, см. Табл. 9. с расстояния R=10 м и к=2,8 обеспечивается приемлемая резкость изображений только в интервале дальностей от 8 м до 15 м. Все предметы и объекты, находящиеся за пределами этого интервала будут выглядеть расплывчатыми (нечеткими). Глубина резкости изображения будет тем выше, чем больше значение диафрагменного числа к. Важное значение для получения высококачественных снимков имеет правильный выбор объектива. Так, если необходимо получить детальный снимок объекта, находящегося на значительном рас-

стоянии, то следует применять специальные длиннофокусные объективы, например, «Уран», «Таир» или «Телемар».

Табл. 9.

Характеристики фотографических объективов

Тип	Диаметр апертуры, мм	Светосила	Фокусное расстояние, мм	Угол поля зрения, град
Гелиос-44М	29	F2	58	31
Уран - 9	100	F2,5	250	54
Уран – 12	200	F2,5	500	38
Уран - 24	167	F3	500	46
Таир - 30	67	F4,5	300	22
Телемар - 17	64	F6.3	400	30

Они позволяют обеспечить хорошую распознаваемость изображенного объекта при съемке с расстояния, достигающего величины, примерно равной половине фокусного расстояния оптической системы объектива, выраженного в метрах. Так как объективы с фокусным расстоянием f=400 мм и более оказываются достаточно громоздкими, то их часто строят по специальным многолинзовым схемам, позволяющим существенно уменьшить продольные габариты, примерно до значения L =0,2 f.

Однако рассмотренные выше объективы имеют малый угол поля зрения, а в ряде случаев возникает необходимость получения общего панорамного изображения какой-либо территории. Для этих целей следует применять специальные широкоугольные или сверхширокоугольные объективы с угловыми полями от 90° до 180°. Примеры таких объективов приведены в табл. 10.

Табл. 10.

Характеристики фотографических объективов

Тип	Диаметр апертуры, мм	Светосила	Фокусное расстояние, мм	Угол поля зрения, град
Русар - 29	8.8	F9	70	120
Родина - 26	6.7	F8.2	55	133
Орион - 20		F4.5		130

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

Определение точки съемки производится на основе комплексного

анализа решаемой задачи, местных условий, возможностей аппаратуры и наличия естественных укрытий. Рекомендуются два следующих правила:

1. при проведении фотосъемки из помещения (или автомобиля) с закрытыми окнами стекла последних должны быть тщательно вымыты;
2. опасным демаскирующим признаком скрытой фотосъемки может быть появление солнечных бликов на стеклах объектива.

Съемка объекта наблюдения может производиться и с малых расстояний, не превышающих нескольких метров. В этом случае целесообразно маскировать аппарат под одеждой, в сумке, папке или в другом малогабаритном предмете, который можно, не вызывая подозрений, держать в руках.

Естественно, что и фотоаппарат должен отвечать решаемым задачам, поэтому он должен быть наделен следующими функциями, см. Рис 29 /1/:

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

Этим требованиям отвечают современные широко распространенные в продаже аппараты. Съемку можно производить как через специально проделанные в предметах камуфляжа отверстия (в сумке, папке), так и непосредственно через ткань легкой одежды (хлопок, шелк, ситец). Демаскирующими признаками описанной съемки являются достаточно громкий щелчок фотоспуска и характерный звук работы мотора при перемотке пленки.

Человеческая память обладает совершенно уникальным свойством со временем забывать то, что в нее попадает. Эта защитная функция организма спасает наш мозг от переполнения ненужными знаниями, освобождая место для новой полезной информации. К сожалению, участи забывания не избегают и полезные сведения, что побудило в свое время людей изобрести письменность. Записями в том или ином виде пользуются все, в том числе и ваши конкуренты, а получение этих записей или иных документов на бумажном носителе может иметь для вас стратегическое значение. Лучше всего, конечно, скрытно сделать копии этих документов, воспользовавшись, например сканером, факсом или ксероксом. Однако, вероятнее всего, этих удобных и полезных вещей в нужный момент под рукой у вас не окажется, и вы будете ограничены во времени. На выручку в такой ситуации может прийти старый хорошо зарекомендовавший себя способ - репродукционная фотосъемка документов.

Для ее производства пригоден практически любой фотоаппарат, позволяющий установить специальный репродукционный объектив, предназначенный для копирования документов. Особенностью этих объективов является конструкция, позволяющая снимать документы с предельно малого расстояния (>1 см), в то время как обычные короткофокусные объективы ограничивают минимальную дальность величиной 0,5- 0,6 м, а при такой дистанции изображение получается мелким и трудно распознавае-

мым. Некоторые типы репродукционных объективов отечественного производства представлены в табл. 11./1/.

Табл. 11.

Характеристики фотографических объективов

Тип	Диаметр апертуры, мм	Светосила	Фокусное расстояние, мм	Угол поля зрения, град
Гелиос - 91	9	F4.5	40	19
Эра – 5	7	F3.5	25	26
Эра - 7	38	F2.8	105	11

Следует отметить, что для указанных целей хорошо подходит уже упомянутый фотоаппарат «Зенит», так как он имеет зеркальную систему визирования (что важно для получения хорошей резкости изображения) и позволяет копировать документы не только с использованием репродукционных объективов, но и с помощью обычных короткофокусных, например, «Гелиос-44М». Однако в этом случае необходимы специальные дополнительные кольца, устанавливаемые между фотоаппаратом и объективом. К сожалению, выбор объектива не исчерпывает особенностей репродукционной съемки. Важное значение играет и подбор чувствительности фотопленки. С одной стороны, она должна быть достаточной для получения снимка в условиях естественной освещенности, а с другой - предельно малой. Так как, чем ниже чувствительность, тем меньше размер «зерна» фоточувствительного слоя и, следовательно, выше разрешение пленки (меньше размер фиксируемых деталей). Лучше всего для этих целей подходит фотопленка с чувствительностью от 8 до 22 единиц.

3.3.2. Цифровые фотоаппараты

Цифровые аппараты - digital cameras фиксирующие изображение не на фотопленку, а в память, в виде, удобном для хранения, просмотра и обработки на персональном компьютере (форматы BMP, JPEG, TIFF). Объем внутренней памяти аппарата может выбираться и наращиваться. Перенос необходимых кадров на персональный компьютер осуществляется по специальному кабелю.

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

Основные технические характеристики цифровых аппаратов фирм Philips и Panasonic приведены в табл. 12./1/.

Более подробно технические характеристики ряда аппаратов, предназначенных для негласной фотосъемки, приведены ниже, а внешний вид некоторых из них показан на Рис. 29, 30./1/.

РК420 - специальная фотокамера, вмонтированная в электронные часы с жидкокристаллическим дисплеем (ЖКД), секундомером и будильником. Диаметр часов - 34 мм, толщина - 10 мм, вес - 70 г. Фотопленка

представлена в виде кассеты из 7 кадров. В каждом кадре пленка имеет свою чувствительность в диапазоне от 15 DIN (ASA 25) до 22 DIN (ASA 125) для обеспечения съемки в различных условиях освещенности. Фиксированное фокусное расстояние обеспечивает диапазон дальностей производства фотосъемки от 1 м до бесконечности. Негатив диаметром 5,5 мм позволяет получать фотоснимки хорошего качества размером 9х9 см.

РК415 - мини-фотокамера для репродукционной съемки и съемки на расстоянии на дальностях от 1м до бесконечности. Фиксированное фокусное

Рис. 29. Фотоаппараты для негласной фиксации информации: а – аппарат Minox; б - камера Ф-21; в – фотоаппарат «Киев-30»; г – фотоаппарат в ручных часах; д – фотоаппарат в зажигалке; е – фотоаппарат в книге

РК1780 - стандартная автомобильная антенна с 5-мм встроенным объективом, снабжена поворотным устройством вокруг вертикальной оси. Изображение фиксируется на фотоаппарат с автоматической регулировкой фокусного расстояния и времени экспозиции.

РК1780-S - то же устройство, но снабженное видеокамерой **РК5105** для прямой видеозаписи наблюдаемого изображения либо передачи его на

дальность до 3 км. Мощность передатчика видеосигнала - 1,5 или 10 Вт.

Табл. 12

Характеристики цифровых аппаратов

Характеристики	Philips ESP-2	Panasonic KXL-600
Габариты	128x34x72,6	134x69x25
Вес	230	182
Размер приемной матрицы, дюйм	1/4	1/4
Число чувствительных элементов, пикселей	350000	360000
Светосила объектива	F3,8	F2,8
Фокусное расстояние	4	5.2
Время срабатывания электронного затвора, с	1/5 – 1/8000	1/15 – 1/4000
Дальность съемки, м	0.6 -	1.0-
Количество снимков, шт	25	48

РК11930 или **РК1935** - специальные устройства для приема видеосигналов. Первый имеет размер экрана по диагонали - 23 мм, габариты - 83х 167х49 мм, вес - 460 г и работает от **автономного** источника питания, второй имеет экран с диагональю 50 мм, габариты - 190х470х412 мм, вес - 4,4 кг и питается от сети 110/220 В.

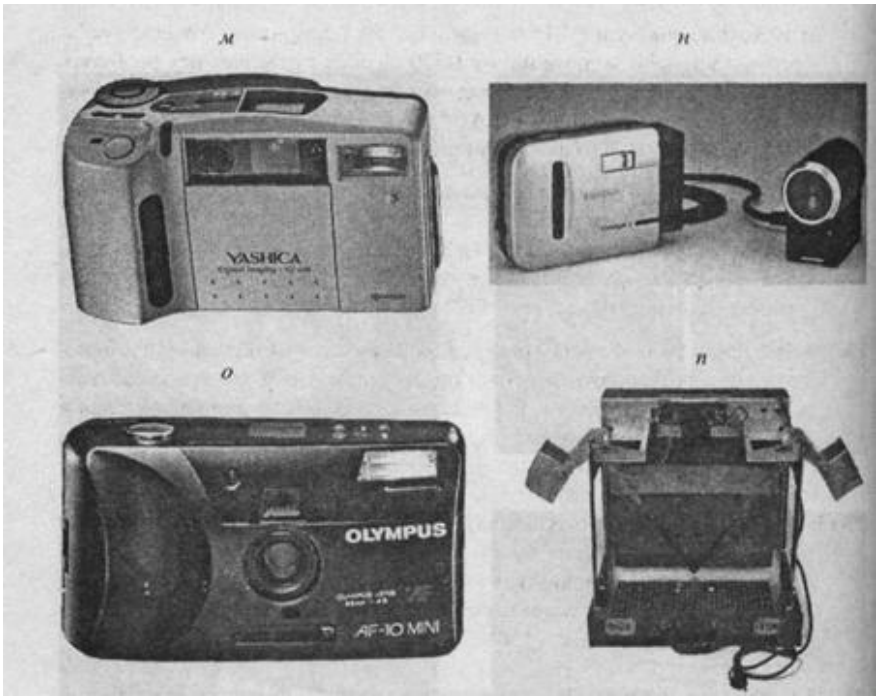


Рис. 30. Цифровые фотоаппараты: m – цифровая камера КС-600 фирмы Yashica; н - цифровая камера Dimage Y; о – цифровая камера AF- 10 Mini; п – цифровая камера в атташе-кейсе с фотоаппаратом фирмы Pentax

РК1700 - устройство для чтения, фотографирования или снятия на видеокамеру **PKS10S** текстов (писем), запечатанных в конверты. Представляет собой специальный эндоскоп длиной 170 мм фиксированным фокусным расстоянием и углом зрения 70°, его диаметр равен 1,7 мм. Устройство вводится в нераспечатанный конверт и перемещается вдоль текста, который можно прочесть, например, на экране монитора. В устройство входит и специальный источник подсветки **РК1765** с напряжением питания 220 В и мощностью **1**50 Вт.

РК1705 - прибор для прямого наблюдения, фотографирования или снятия на видеокамеру **РК5105.** Жесткий эндоскоп длиной 245 мм, диаметром 6 мм вставляется в отверстие в стене. Вес прибора 320 г, угол зрения 80°. Дальность наблюдения - от 0,5 м до бесконечности. Модель **РК1780-S** содержит встроенный аудиомикрофон и усилитель с коэффициентом усиления 20 000 раз, напряжением питания 9 В и частотным диапазоном 300-3000 Гц. Размеры усилителя - 54х80х20 мм. Он позволяет прослушивать помещение с помощью головных телефонов.

3.4. Технические средства получения видеоинформации.

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

Однако по своей структуре телевизионные камеры более сложны, чем рассмотренные выше приборы ночного видения. Это связано с необходимостью разложения получаемого изображения на составные части для их передачи к месту регистрации и последующего восстановления передаваемого изображения. В общем случае структурная схема телевизионной камеры имеет вид, показанный на Рис. 31.

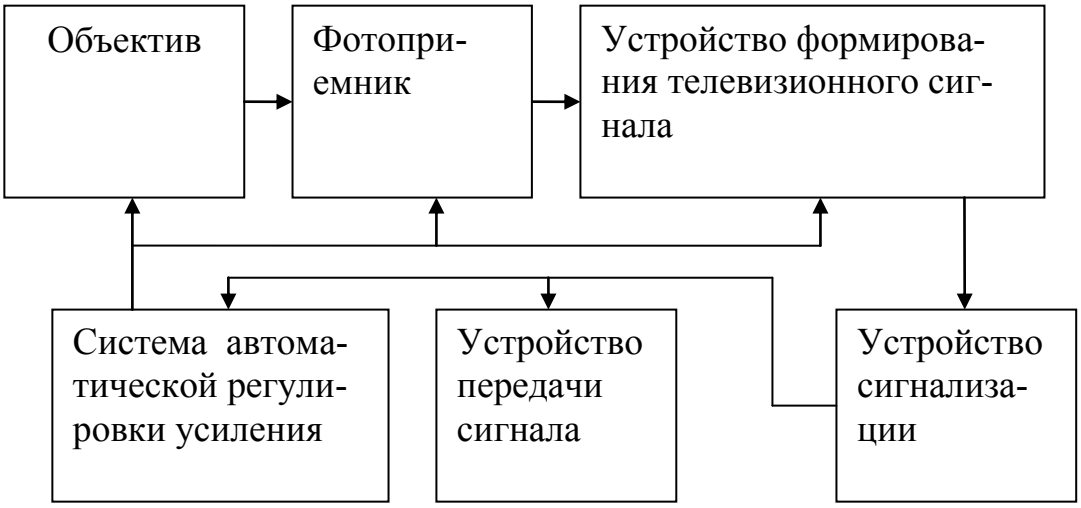


Рис. 31. Структура телевизионной камеры

Здесь объектив играет такую же роль, как и в рассмотренных выше оптических приборах, но конструкция его может быть сложнее из-за необ-

ходимости решения задачи автоматической регулировки диафрагмы в зависимости от уровня освещенности объекта наблюдения.

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

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

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

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

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

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

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

Мгновенный угол поля зрения полностью определяется конструкцией оптической системы. Его значения для различных типов объективов приведены в Табл. 13 /1, 2/.

Разрешающая способность включает в себя два понятия: разрешающую способность объектива и разрешающую способность фотоприемника. Разрешающая способность объектива - это тот предел, к которому стремится любая система фиксации изображения. Она зависит от диаметра D, входного зрачка объектива и расстояния R от телекамеры до объекта

наблюдения и соответствует минимальному линейному разносу двух точек на объекте, при котором они воспринимаются еще раздельно.

Табл. 13.

Характеристики объективов телевизионных камер

Тип объектива	Диаметр апертуры, мм	Светосила объектива	Фокусное расстояние, мм	Угол поля зрения, град	Установочная резьба
iVi-1.0	14	F 1.8	3.6	110	M12
iVi-2.0	13	F1.8	4.1	90	M12
iVi-3.0	3.4	F1.8	6.6	50	M12
iVi-4.0	4.6	F1.6	7.7	40	M12
iVi-7.0	1.2	F2.8	3.5	110	M12
iVi-10	6.5	F2.8	19.5	16	M12
HS3 166-X	3.7	F1.6 - 64			CS
HS4 166-X	4.2	F1.6 - 64			CS
HS614-HX	2.6	F1.6 - 300			CS

Разрешающая способность фотоприемника хуже (больше) разрешающей способности объектива, поэтому ее величина и определяет разрешение телевизионной системы в целом. Она зависит от числа чувствительных элементов ПЗС-матрицы (пикселей), из выходных сигналов которых складывается изображение. Их число обычно лежит в пределах от 270 000 до 440 000. Чем больше число пикселей в матрице, тем больше дискретных точек образует изображение, тем выше его четкость и качество. Однако на практике часто пользуются не понятием «число чувствительных элементов матрицы», а однозначно связанной с ней характеристике - максимальному количеству переходов от черного к белому и обратно. Она называется числом телевизионных линий и указывается, как правило, только по горизонтали. Некоторые фирмы в технических характеристиках на свои телевизионные камеры дополнительно указывают размер матрицы оптического приемника. В большинстве представляемых на российском рынке камерах используются датчики изображения (матрицы) с размером: 1 дюйм; 2/3 дюйма; 1/2 дюйма; 1/3 дюйма; 1/4 дюйма. Последние, как правило, применяются только в сверхминиатюрных камерах, используемых для скрытого наблюдения.

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

I - камеры, которые могут работать только при нормальном дневном освещении (при уровне освещенности E = 50 лк).

II - камеры, способные работать при низкой освещенности вплоть до наступления сумерек (E = 4 лк).

III - камеры, предназначенные для работы при лунном свете, соответствующем уровню освещенности от четверти луны в безоблачную ночь (Е = 0,1 - 0,4лк).
IV - камеры, способные работать при уровне освещенности, создаваемой безлунным звездным небом в безоблачную ночь (Е = 0.007...0,002 лк).
V - камеры, предназначенные для работы с дополнительными источниками ИК-излучения в условиях полного отсутствия видимого излучения.

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

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

$$E \geq E_0 \cdot R \cdot K,$$

где E_o - общий уровень освещенности в зоне нахождения объекта наблюдения [лк];

R - Коэффициент отражения объекта наблюдения;

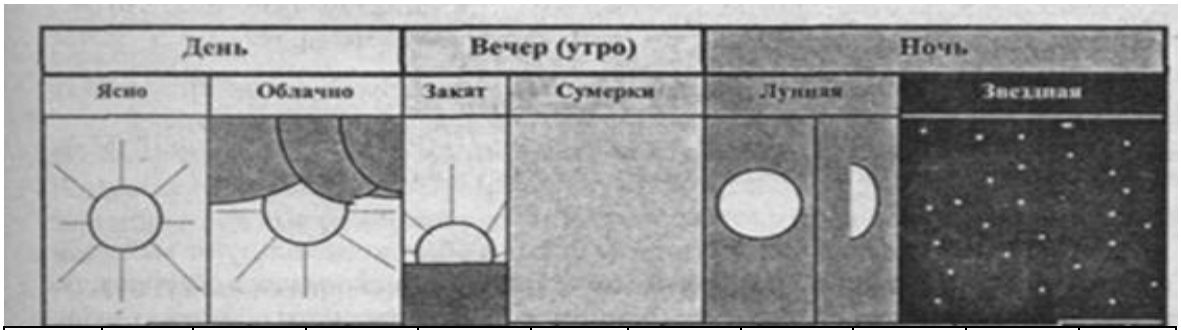
К - коэффициент пропускания объектива камеры.

Значения параметров R и К приведены в табл. 14 и 15 /1 и 2/, соответственно, а типовая зависимость уровня освещенности E_o (лк) от времени суток и состояния атмосферы - на рис. 32/1/.

Табл. 14.

Коэффициенты отражения различных поверхностей

Поверхность	Коэффициент отражения
Кожа человека	0.15 - 0.25
Ткань серого цвета	0.2 – 0.6
Ткань желтло-коричневого цвета	0.3 – 0.4
Ткань желтого цвета	0.6 – 0.75
Ткань белого цвета	0.8 – 0.9



5	4	3	2	1	0	-1	-2	-3	-4	-5

Рис. 32 Зависимость уровня освещенности от времени суток и состояния атмосферы

Табл. 15.

Коэффициенты пропускания объективов телевизионных камер

Светосила объектива	Относительное отверстие объектива	Коэффициент пропускания
F 0.8	1/0.8	0.31
F0.95	1/0.95	0.2
F1.2	1/1.2	0.14
F1.4	1/1.4	0.1
F2.0	1/2.0	0.05
F2.8	1/2.8	0.025
F4.0	1/4	0.0125
F5.6	1/5.6	0.00625
F8.0	1/8	0.003125

Для скрытой телевизионной (видео) съемки обычно используют малогабаритные камеры, которые могут быть выполнены как в обычном, так и закамуфлированном исполнении (например, в виде дверного «глазка»); существует целое семейство бескорпусных видеокамер. Для осуществления наблюдения вышеперечисленные устройства устанавливают в элементы конструкций зданий, предметы интерьера или прячут под одежду.

Важным достоинством указанной камеры является наличие специального передатчика телевизионного сигнала **JR-500,** позволяющего передавать изображение и звук на расстояние до 500 м. Передатчик работает в диапазоне дециметровых волн, имеет габариты 120x120x25 мм и массу 200 г. Питание - от элемента с напряжением 12 В. Предусмотрено закрытие передаваемой информации. Так, например, телевизионная камера **JT-241s** штатно оснащается следующими предметами камуфляжа:

•элементы интерьера: картина, мебель, цветочная ваза, статуэтка, светильник, электророзетка;

•одежда и ее элементы: куртка, костюм, заколка для галстука, пуговица, пряжка ремня;

•носимые предметы: кейс, сумка, радиоприемник, магнитофон.

Дополнительно камера оснащается выносным проводным микрофоном **JM-004** и оптико-волоконными жгутами для вынесения объектива, прожектором инфракрасной подсветки, диктофоном и видеомагнитофоном. В зависимости от комплектации камера может использоваться как носимое средство либо как закладное устройство.

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

Для приема телевизионных и аудиосигналов от передатчика **JR-500**

применяется специальный приемник **JD-500,** обеспечивающий уверенный прием на указанной дальности - до 500 м. Основные технические характеристики телевизионной камеры JT-241s, а также некоторых других приведены в Приложении Табл. П5.

Выводы по главе:

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

2. Применение съема путем высокочастотного навязывания возможно только при тщательной предварительной подготовке. Использование аппаратуры ВЧ-навязывания в проводных каналах имеет хорошую перспективу из-за сравнительной простоты и дешевизны, известных методов. Использование лазерных систем в техническом плане не имеет серьезных проблем, и в обозримом будущем они станут обычным средством несанкционированного получения речевой информации не только спецслужб.

Вопросы для самоконтроля:

Вопрос 1. Перечислите пять классов телевизионных камер.
Вопрос 2. Приведите основные характеристики объективов.
Вопрос 3. Приведите основные характеристики видеокамер.
Вопрос 4. Чем отличаются цифровые фотоаппараты.
Вопрос 5. Перечислите основные функции фотоаппарата.

Методические рекомендации.

Изучив материал главы, ответьте на вопросы. При возникновении трудностей обратитесь к материалам для закрепления знаний в конце пособия.

Для углубленного изучения воспользуйтесь литературой:

основной: 1 – 2; дополнительной: 4 – 6 и повторите основные определения, приведенные в конце пособия.

ГЛАВА 4. СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

Информационная безопасность страны является составной частью ее национальной безопасности и призвана обеспечить «информационный» суверенитет государства и способствовать успешному проведению экономических преобразований, укреплению политической стабильности общества. Это связано с обеспечением защищенности системы формирования информационных ресурсов и созданием необходимого уровня защищенности применяемых технологий, использующего, в том числе современные системы и средства.

Решение этих задач возможно только на основе создания системы комплексной защиты информации и правильной организации ее функционирования. Именно такая система способна реализовать непрерывность процесса защиты информации, создать эффективные механизмы защиты и обеспечить их надежную работу.

Государственная система защиты информации должна обеспечивать решение ряда задач, основными из которых являются:

1. разработка общей технической политики и концепции обеспечения безопасности информации;
2. разработка законодательно-правового обеспечения безопасности информации;
3. разработка концепции деятельности органов государственного управления по отдельным вопросам защиты информации;
4. разработка нормативно-технических и организационно-распорядительных документов;
5. сертификация технических и программных средств по требованиям безопасности.
6. лицензирование деятельности по оказанию услуг в сфере безопасности информации;
7. контроль за выполнением законодательства и требуемых мер в области безопасности информации;
8. подготовка квалифицированных кадров в сфере защиты информации;
9. проведение важнейших научно-исследовательских и опытно-конструкторских работ в области защиты информации;
10. информационное обеспечение по вопросам защиты информации;
11. защита прав собственников (владельцев, пользователей) информации.

Система должна включать:

- органы управления;
- органы межотраслевой координации;
- центры безопасности;
- научно-исследовательские организации;
- центры подготовки кадров;
- органы сертификации, лицензирования, экспертизы и контроля;

- сервисные организации и службы, действующие на основании лицензий;
- службы безопасности информации у потребителей.

Система защиты информации должна удовлетворять следующим требованиям:
- обеспечивать безопасность информации, средств информатизации, щиту интересов участников информационных отношений;
- быть, по возможности, прозрачной для участников информационного обмена, не создавать им излишних неудобств, связанных с дополнительными процедурами проверки, надзора, контроля за доступом и т.д.;
- реализовывать различные методы управления: жесткие (административные) и мягкие (рекомендательного характера).

Защита государственного информационного ресурса (обеспечение государственной тайны) осуществляется с применением административно-директивных методов, реализуемых в форме государственного заказа, системы стандартов качества, а также ответственности производителя перед государством.

Директивные формы управления реализуются в виде, во-первых, обязательных для выполнения норм, требований и инструкций, во-вторых, независимой системы контроля (надзора) и, в-третьих, системы ответственности за допущенные нарушения. В государственном секторе ответственность за обеспечение установленных требований по защите информации возлагается на руководителей предприятий, организаций и учреждений, эксплуатирующих объев защиты.

В независимом секторе экономики, не связанном с обеспечением государственной тайны, возможны только формы управления органами защиты формации путем рекомендательного использования нормативных, методических и организационно-распорядительных документов, применение разработанной и испытанной в интересах госсектора техники, программных и других средств. Основой функционирования системы защиты информации в этом случае является личный выбор собственником информации степени ее защищённости и механизмов защиты. При этом определяющими факторами является риск участников информационных отношений и их личная ответственность за принятые меры по защите конфиденциальной информации.

Основными целями защиты информации на объектах защиты являются предотвращение проявления и нейтрализация преднамеренных и непреднамеренных источников угроз безопасности информации. В соответствии с этим процесс защиты информации должен обеспечить поддержание ее целостности и конфиденциальности. При этом под целостностью информации следует понимать ее неизменность (физическую целостность) и непротиворечивость (логическую целостность) в процессе хранения и обработки. Конфиденциальность информации предполагает ее доступность только для тех лиц, которые имеют на это соответствующие полномочия.

Целостность информации тесно связана с понятием надежности как технических, так и программных средств, реализующих процессы накопления, хранения и обработки информации.

Из анализа угроз безопасности информации, целей и задач ее защиты следует, что достичь максимального (требуемого) уровня защищенности можно только за счет комплексного использования существующих методов и средств защиты. Комплексность является одним из принципов, которые должны быть положены в основу разработки как, концепции защиты информации, так и конкретных систем защиты.

Цели защиты информации на объектах могут быть достигнуты при проведении работ по следующим направлениям:

- определению охраняемых сведений об объектах защиты;
- выявлению и устранению (ослаблению) демаскирующих признаков, раскрывающих охраняемые сведения;
- оценке возможностей и степени опасности технических средств разведки;
- выявлению возможных технических каналов утечки информации;
- анализу возможностей и опасности несанкционированного доступа к информационным объектам;
- анализу опасности уничтожения или искажения информации с помощью программно-технических воздействий на объекты защиты;
- разработке и реализации организационных, технических, программных и других средств и методов защиты информации от всех возможных угроз;
- созданию комплексной системы защиты;
- организации и проведению контроля состояния и эффективности системы защиты информации;
- обеспечению устойчивого управления процессом функционирования системы защиты информации.

На объектах защиты процесс комплексной защиты информации должен осуществляться непрерывно на всех этапах их жизненного цикла. Реализация непрерывного процесса защиты информации возможна только на основе системно-концептуального подхода и промышленного производства средств защиты, а создание механизмов защиты и обеспечение их надежного функционирования и высокой эффективности может быть осуществлена только специалистами высокой квалификации в области защиты информации.

Необходимые для создания и поддержания эффективного функционирования системы защиты информации виды обеспечения включают законодательно-правовое, организационно-техническое и страховое обеспечение.

Законодательно-правовое обеспечение включает систему законодательно-правовых актов, устанавливающих правовой статус субъектов правоотношений, субъектов и объектов защиты, формы и способы защиты. Система законодательно-правовых актов и разработанных на их базе нормативных и организационно-распорядительных документов должна обес-

печить организацию эффективного надзора за их исполнением со стороны правоохранительных органов и реализацию мер судебной защиты.

Организационно-техническое обеспечение представляет собой комплекс взаимокоординируемых организационных мероприятий, технических, программных и других мер, реализующих все практические механизмы защиты.

Страховое обеспечение предназначено для защиты собственника информации или средств информатизации как от традиционных угроз (краж, стихийных бедствий и т.д.), так и от угроз, возникающих в ходе информатизации общества (утечка, уничтожение, блокирование и т.п.). Важным является вопрос защиты от промышленного шпионажа, а также страхование риска. Особенностью страховых методов обеспечения защиты является их эффективное действие в независимом секторе экономики, где административные методы управления и особенно контроля малоприемлемы.

Основой для практической деятельности по реализации основных направлений и работ по защите информации в ТСОИ являются нормативно-методические документы, регламентирующие эту деятельность. Нормативно-методическую базу для проведения работ по защите информации в составляют:

- государственные стандарты;
- модели;
- общие требования, общие технические требования, тактико-технические требования, и другие документы общегосударственного значения;
- нормы, методики и инструкции;
- эксплуатационно-техническая документация;
- учебно-методическая и научная литература.

ГОСТами вводится единая терминология в области защиты информации, а также определяются виды и методы испытаний технических и программных средств обработки и защиты, виды, комплектность и обозначения документов.

Модели содержат обобщенные сведения о состоянии, возможностях, тактико-технических и эксплуатационно-технических характеристиках, способах применения, тенденциях и перспективах развития технических средств различного назначения. Такие модели, как правило, охватывают определенные направления: средства разведки, средства промышленного шпионажа, технические средства защиты информации, программные средства защиты и т.д. и разрабатываются ведомственными научно-исследовательскими организациями и учреждениями, а также межведомственными органами. Они широко используются при решении конкретных научных, научно-исследовательских и практических инженерных задач в области защиты информации.

Нормативные документы (нормы) определяют конкретные количественные требования к противодействию техническим средствам разведки, требования к эффективности защиты объектов от утечки информации по

техническим каналам и т.п. Методики и инструкции определяют организацию и порядок категорирования объектов защиты, измерения и расчета различных количественных показателей, проведения испытаний объектов и средств защиты, оценки опасности технических средств разведки, контроля эффективности методов и средств защиты информации, проведения специсследований, спецпроверок, аттестации объектов информатики и т.п.

Нормы, методики и инструкции разрабатываются в министерствах и ведомствах и широко используются в повседневной работе при проектировании, создании и эксплуатации объектов и средств защиты информации.

Эксплуатационно-техническая документация (технические описания технических средств, инструкции по эксплуатации, схемы электрические принципиальные и т.д.) содержат сведения о составе, характеристиках, устройстве, условиях и правилах эксплуатации конкретных технических средств и систем обработки и защиты информации.

При решении различных задач в области защиты информации могут быть дополнительно использованы учебно-методическая и научная литература, открытия, изобретения, рацпредложения и т.п. Эти источники информации не регламентируют деятельность в области защиты информации, но могут оказаться полезными в решении многих конкретных задач.

При разработке и создании системы комплексной защиты информации для конкретного объекта защиты основное внимание должно быть уделено ее оптимальности. Оптимальность системы защиты заключается в следующем: система должна обеспечить требуемый уровень защиты информации при минимальном расходовании ресурсов (финансовых, технических, информационных и др.) на ее создание, организацию и обеспечение функционирования или при заданном объеме ресурсов обеспечить максимально возможный уровень защищенности информации.

При оптимизации системы защиты ключевым исходным моментом является формирование полного множества функций защиты, так как надлежащим распределение ресурсов в осуществлении каждой функции можно оказывать воздействие на уровень защищенности информации, создавая таким образом, объективные предпосылки для разработки оптимальной системы защиты. Общеизвестно, что полное множество составляют семь функций защиты:

1. создание таких условий, при которых угрозы безопасности информации не могли бы проявляться;
2. предупреждение появления угроз, даже если для этого есть объективные предпосылки;
3. обнаружение появления угроз;
4. предупреждение воздействия появившихся угроз на защищаемую информацию;
5. обнаружение воздействия угроз на защищаемую информацию;
6. локализация воздействия угроз на информацию;

7. ликвидация последствий воздействия угроз.

Решение задачи оптимизации систем защиты включает:

1. Проводится анализ структурного построения и принципов функционирования объекта защиты с целью определения уязвимых элементов, которые влияют на безопасность объекта.

2. Определяются и анализируются возможные угрозы выделенным элементам и формируется перечень требований к системе защиты.

3. На основе опыта создания систем защиты информации определяются наиболее подходящие варианты набора средств и мер защиты, использованием которых может быть реализована каждая из функций защиты, и для этих вариантов методами экспертных оценок определяются показатели эффективности составленных вариантов.

4. На основе технико-экономических оценок средств и мер защиты определяются размеры ресурсов, необходимых для практического использования различных средств и мероприятий

5. Решается задача синтеза оптимальной системы защиты информации методами статистического моделирования.

Следует иметь в виду, что разработка системы комплексной защиты информации предусматривает варианты и процедуры перехода степени защиты в соответствии с прогнозируемым уровнем опасности.

Выводы по главе:

1. Необходимым условием разработки системы защиты информации является соблюдение следующих принципов:

- учет требований защиты информации при построении объекта защиты и разработке технологии автоматизированной обработки информации;
- комплексность использования средств и методов защиты;
- обеспечение непрерывности процесса защиты;
- обеспечение периодического контроля правильности функционирования всех подсистем защиты.

Вопросы для самоконтроля:

Вопрос 1. В каком виде реализуются директивные формы управления?

Вопрос 2. Каковы процедуры оптимизации системы защиты?

Вопрос 3. Перечислите семь функций защиты.

Методические рекомендации.

Изучив материал главы, ответьте на вопросы. При возникновении трудностей обратитесь к материалам для закрепления знаний в конце пособия. Для углубленного изучения воспользуйтесь литературой:

основной: 1 – 3; дополнительной: 6 и повторите основные определения, приведенные в конце пособия.

ГЛАВА 5. ТЕХНИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

5.1. Защита телефонных аппаратов и линий связи

Одним из основных каналов утечки информации является телефонный аппарат и линия связи, его с автоматической телефонной станцией (АТС). Для специалиста, работающего в области шпионажа с применением технических средств контроля, наибольший интерес представляют комплексы средств, позволяющие получать информацию из интересующих помещений без необходимости физического присутствия в них. Телефонный аппарат представляет в этом плане множество возможностей. Рассмотрим три схемы решения этой задачи.

1. Телефонный аппарат содержит систему передачи информации, т.е. внутри установлена специальная аппаратура. Например, телефонные аппараты с электронными номеронабирателями уже имеют канал утечки информации в виде паразитного высокочастотного излучения в широкой полосе частот, промодулированного звуковым сигналом.

2. Используются определенные недостатки конструкций телефонных аппаратов для получения информации.

3. Производится внешнее воздействие на телефонный аппарат, при котором возникает канал утечки.

5.1.1. Защита звонковой цепи

При разговоре в помещении акустические колебания воздействуют на маятник звонка, соединенного с электромагнитного реле. Под воздействием звуковых сигналов якорь совершает микроколебания, что, в свою очередь, вызывает колебание якорных пластин в электромагнитном поле катушек, что приводит к появлению микротоков, промодулированных звуком. Амплитуда ЭДС, наводимая в линии, для некоторых типов телефонных аппаратов может достигать нескольких милливольт. Для приема используется низкочастотный усилитель с частотным диапазоном 300-3500 Гц, который подключается к абонентской линии.

Для защиты от такого канала утечки информации используется схема, представленная на Рис. 33.

Два кремниевых диода VD1 и VD2 включены встречно-параллельно в цепь звонка телефонного аппарата B1. Они образуют зону нечувствительности для микро-ЭДС. Это объясняется тем, что в интервале 0 - 0,65 В диод обладает большим внутренним сопротивлением.

Поэтому низкочастотные токи, наводимые в схеме аппарата, не пройдут в линию. В тоже время звуковой сигнал абонента и напряжение вызова свободно "проходят" через диоды, так как их амплитуда превышает порог открывания диодов VD1, VD2. Резистор R1 является дополнительным шумящим элементом. Подобная схема, включенная последовательно в линию связи, подавляет микро-ЭДС катушки на 40-50 дБ. В схеме можно использовать диоды Д226, КД105, КД102 и резистор 5к1.

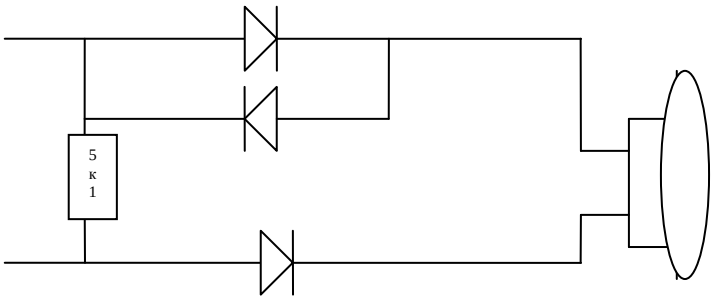


Рис. 33 Схема защиты звонковой цепи

5.1.2. Защита микрофонной цепи

Этот вариант получения информации связан с явлением высокочастотного навязывания. При этом относительно общего корпуса на один провод подается высокочастотное колебание (частотой более 150 кГц). Через элементы схемы телефонного аппарата, даже если трубка не снята, высокочастотные колебания поступают на микрофон, где и модулируются звуковыми колебаниями. Прием информации производится относительно общего корпуса через второй провод линии. Амплитудный детектор позволяет выделить низкочастотную огибающую для дальнейшего усиления и записи. Схема защиты телефонного аппарата от этого метода съема информации представлена на Рис. 34.

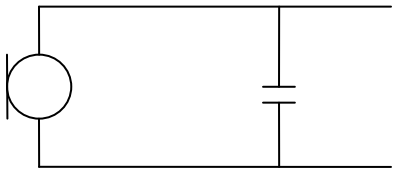


Рис. 34 Схема защиты звонковой цепи

Так как модулирующим элементом является микрофон Ml телефонного аппарата, то для его защиты достаточно подключить параллельно микрофону Ml конденсатор емкостью 0,01- 0,05 мкФ. При этом конденсатор шунтирует по высокой частоте микрофонный капсуль Ml. Глубина модуляции высокочастотных колебаний уменьшается более чем 10000 раз, что делает практически невозможной дальнейшую демодуляцию.

5.1.3. Комплексная схема защиты

Эта схема представляет собой сочетание приведенных ранее двух схем. Кроме конденсаторов и резисторов, схема, представленная на Рис. 35, содержит катушки индуктивности. Диоды, включенные встречно-параллельно, защищают звонковую цепь телефона. Конденсаторы и катушки образуют Г-образные фильтры для подавления напряжений высокой частоты. Данное устройство не защищает пользователя от непосредственного подслушивания, путем прямого подключения в линию. Кроме рассмотренной схемы существует и ряд других, которые по своим характеристикам близки к рассмотренным.

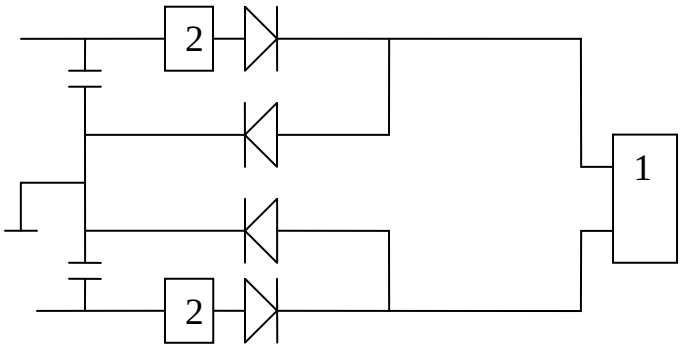


Рис. 35 Комплексная схема защиты: 1 - телефонный аппарат, 2 – катушка индуктивности 5мГн

5.1.4. Защита линий связи

1. Анализатор телефонной линии является простейшим индикатором наличия подслушивающих устройств. Оно устанавливается на предварительно проверенной телефонной линии. Питание осуществляется от телефонной линии. При наличии любых несанкционированных подключений различных устройств, питающихся от телефонной линии, выдается сигнал тревоги - светодиод. Схема такого устройства приведена на Рис. 36.

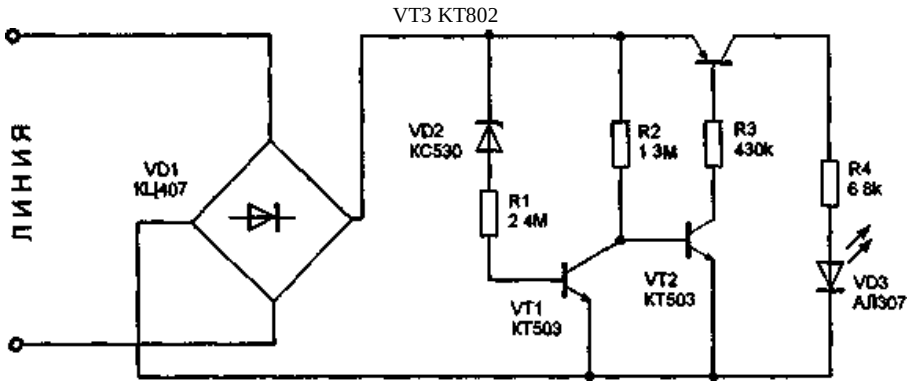


Рис. 36 Анализатор телефонной линии

Устройство состоит из анализатора линии, собранного на стабилитроне VD2 типа КС530 и транзисторе VT1 типа КТ503, и усилителя тока, собранного на транзисторах VT2 и VT3 типа КТ503 и КТ502, соответственно. К выходу усилителя через ограничительный резистор R4 подключен светодиод VD3 типа АЛ307. Выпрямительный мост VD1 типа КЦ407 обеспечивает требуемую полярность питания устройства независимо от подключения его к телефонной сети. Стабилитрон VD2 открывается, и в базу транзистора VT1 подается через ограничительный резистор R1 управляющий ток. Открытый и насыщенный транзистор VT1 шунтирует вход каскада на транзисторе VT2, поэтому усилитель тока закрыт и светодиод VD3 погашен. При подключении в линию посторонних устройств, напряжение в линии падает и ток, протекающий через стабилитрон VD2 уменьшается (вплоть до закрытия последнего). Транзистор VT1 закрывается, а в базу транзистора VT2 через резистор R2 подается управляющий ток. Усилитель открывается и светодиод VD3 включается.

2. **Индикатор линии на микросхеме** приведен на Рис. 37.

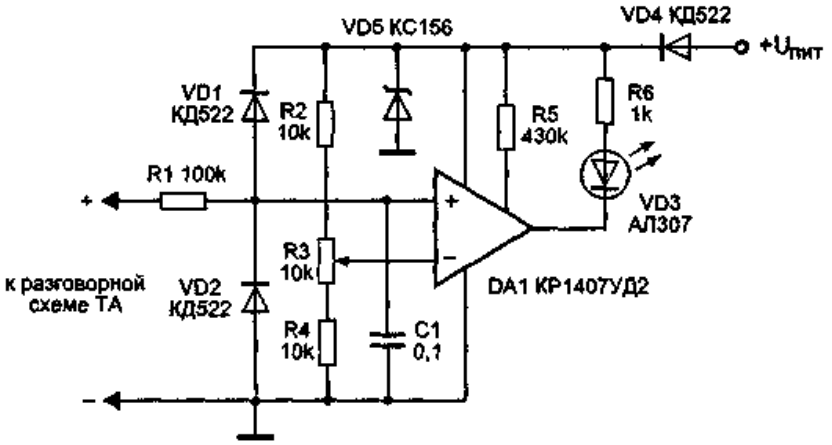


Рис. 37 Анализатор телефонной линии на микросхеме

Индикатор устанавливается в корпус телефонного аппарата и питается от телефонной линии. Он индицирует несанкционированное подключение к линии в момент ведения разговора, т. е. когда трубка снята с рычага телефона. Основу схемы составляет операционный усилитель DA1 типа КР1407УД2, включенный по схеме компаратора напряжений. При снятии телефонной трубки напряжение с линии подается на рассматриваемое устройство через диод VD4 типа КД522, образующий со стабилитроном VD5 типа КС 156 параметрический стабилизатор напряжения. Одновременно напряжение поступает через резистор R1 на вход компаратора DA1. На инвертирующий вход последнего подается опорное напряжение, снимаемое с движка подстроечного резистора R3. При уменьшении входного напряжения до уровня меньшего, чем опорное напряжение, на выходе компаратора DA1 появляется уровень логического нуля, что вызывает включение светодиода VD3 типа АЛ307. Диоды VD1 и VD2 совместно с резистором R1 ограничивают напряжение на входе DA1 на уровнях, выходящих за пределы питающих напряжений - не более, чем на 0,7 В (на величину прямого падения напряжения на диодах VD1, VD2). Конденсатор C1 защищает схему от высокочастотных наводок в линии. Резистор R5 устанавливает режим работы микросхемы DA1. В устройстве использованы резисторы типа МЛТ-0,125. Диоды VD1, VD2, VD4 - любые кремниевые. Стабилитрон VD5 - любой на напряжение стабилизации 4,7-7,0 В. Микросхему DA1 можно заменить на любой операционный усилитель с током потребления не более 5 мА. Устройство настраивают по методике: 1. сняв трубку телефонного аппарата и установив разговорное соединение, подстройкой резистора R3 добиваются погашения светодиода VD3. Медленно, изменяя сопротивление резистора R3, находят положение движка последнего, при котором устройство срабатывает. Затем немного поворачивают движок резистора R3 в обратную сторону. Свето-

диод снова гаснет, прибор настроен. Он будет реагировать как на параллельное подключение к линии, так и на последовательное подключение. Необходимо соблюдать полярность включения прибора!

3. **Активный индикатор состояния линии.** Принципиальная схема такого устройства представлена на Рис. 38.

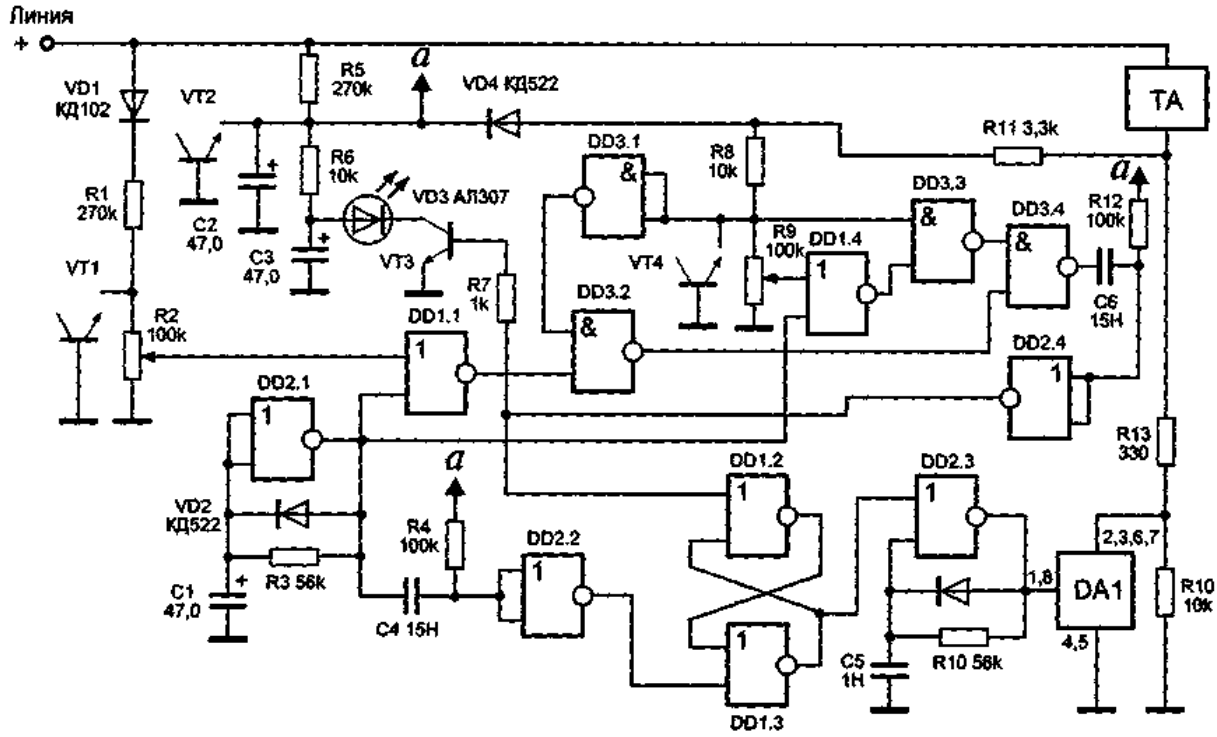


Рис. 38 Активный анализатор телефонной линии на микросхемах

Данное устройство, не только выявляет подключение дополнительной нагрузки, но и при срабатывании системы сигнализации переводит устройство в активный режим работы. Этот режим позволяет блокировать многие радиоретрансляционные устройства и приборы, предназначенные для автоматической записи телефонных переговоров. Устройство собрано на 4-х микросхемах и 4-х транзисторах. Исходное состояние: трубка телефонного аппарата опущена. Питание устройства осуществляется от телефонной линии через ограничительный резистор R5. Конденсатор C2 заряжается через резистор R5 до напряжения стабилизации стабилитрона, выполненного на транзисторе VT2. С конденсатора C2 напряжение величиной 7-8 В поступает на устройство для питания микросхем (точка "а"). От источника питания через резистор R6 заряжается конденсатор C3. Резисторы R6, R7, конденсатор C3, светодиод VD3 и транзистор VT3 образуют схему индикации устройства. Напряжение линии через диод VD1 типа КД102 поступает на делитель напряжения, образованный резисторами R1 и R2. Напряжение на резисторе R2 ограничивается транзистором VT1, включенным по схеме стабилитрона до напряжения питания, что необходимо для защиты входов микросхем от высшего напряжения. С движка подстроечного резистора R2 напряжение высокого уровня посту-

пает на вход элемента DD1.1 микросхемы К561ЛЕ5, запрещая проход импульсов с генератора, выполненного на элементе DD2.1 микросхемы К561ТЛ1. Этот генератор выполнен на основе триггера Шмидта. При заряде и разряде конденсатора С1 на выходе генератора появляются прямоугольные импульсы. Поскольку заряд конденсатора С1 происходит через диод VD2 типа КД522, а разряд - через резистор R3, то на выходе элемента DD2.1 имеют место короткие положительные импульсы с частотой следования 1- 0,5 Гц. Первый же импульс, пройдя через дифференцирующую цепочку С4, R4 и элемент DD2.2, устанавливает триггер, собранный на элементах DD2.1, DD1.3, в положение, когда на входе элемента DD2.3 низкий уровень напряжения. Генератор, собранный на DD2.3, выключен и на выводах 1, 8 микросхемы DA1 типа КР1014КТ1 присутствует высокий уровень. Одновременно импульсы с DD2.1 поступают на элементы DD1.1 и DD1.4. Через DD1.1 импульсы не проходят, т. к. с резистора R2 поступает высокий уровень. Нулевой уровень, снимаемый с резистора R9 подается на входы элементов DD3.1 и вход DD3.3 микросхемы К561ЛА7. Поэтому импульсы, проходящие через DD1.4, не проходят на DD3.4. Следовательно, на выходе DD2.4 присутствует логический нуль, и транзистор VT3 закрыт. С движка резистора R2 снимается напряжение логической единицы, достаточное для переключения элемента DD1.1, выполняющего функцию управляемого компаратора с чувствительностью в десятки милливольт. Если к линии подключается дополнительная нагрузка сопротивлением менее 100 кОм, то напряжение в линии уменьшится на некоторую величину. Одновременно уменьшается и напряжение на резистора R2. Это приводит к появлению на входе DD1.1 напряжения, воспринимаемого микросхемой как уровень логического нуля. Этот уровень разрешает прохождение импульсов от DD2.1 через DD1.1. Поскольку на выходе DD3.1 высокой уровень, то импульсы проходят через ключ DD3.2. При этом на выходе DD3.3 тоже высокий уровень и эти импульсы проходят и через ключ DD3.4. Продифференцированные импульсы цепочкой С6, R12 и элементом DD2.4 поступают на базу транзистора VT3. Транзистор открывается, и конденсатор С3 быстро разряжается через открытый транзистор VT3 и светодиод VD3, который ярко вспыхивает с частотой 0,5- 1 Гц. В перерывах между импульсами конденсатор С3 подзаряжается через резистор R6. Так как оценка состояния линии происходит под управлением импульсов с генератора DD2.1, то некоторое изменение напряжения в линии в момент заряда конденсатора С3 на работе устройства не сказывается. Рассмотрим случай, когда телефонная трубка снята. При этом сопротивление телефонного аппарата включается между плюсовым проводом линии и резисторами R11 и R13. Напряжение в линии уменьшается до 5 - 25 В, т. к. нагрузкой линии будут телефонный аппарат, Резистор R13 и резистор R14, зашунтированный малым (около 10 Ом) сопротивлением микросхемы DA1. Напряжение, снимаемое с резистора R13, обеспечивает пи-

тание устройства через диод VD4 типа КД522. При этом напряжение высокого уровня с точки соединения резисторов R8, R9 поступает на элементы DD3.3 и DD3.1. Низким уровнем закрывается ключ DD3.2. С движка резистора R9 снимается напряжение логической единицы, близкое к напряжению переключения компаратора DD1.4. Допустим, что к линии подключается (или была подключена) дополнительная параллельная или последовательная нагрузка, которая приводит к уменьшению напряжения в линии. При этом напряжение на движке резистора R9 принимает уровень, расцениваемый микросхемой, как уровень логического нуля. При этом импульсы с DD2.1 проходят через DD1.4, DD3.3 и DD3.4. После дифференцирующей цепочки С6, R12 и элемента DD2.4 они поступают на базу транзистора VT3, включая световую индикацию. Одновременно, первый же импульс переводит триггер DDl.2 и DDl.3 в состояние, разрешающее работу генератора на элементе DD2.3. С выхода генератора короткие импульсы частотой 12-20 кГц поступают на ключ, выполненный на микросхеме DA1. Ключ начинает закрываться и открываться с частотой генератора. При этом сигнал в линии модулируется этой частотой. Это вызывает расширение спектра сигнала, излучаемого радиоретранслятором, подключенным в линию. Одновременно напряжение в линии увеличивается до 35-45 В. Это связано с тем, что последовательно с резистором R13 включается резистор R14, ранее шунтированный ключом DA1. Повышение напряжения в линии до такого уровня позволяет нейтрализовать автоматические записывающие устройства, срабатывающие по уровню напряжения в линии. Для того, чтобы работа этого генератора не мешала анализу состояния линии, он периодически отключается путем переключения триггера DD1.2, DD1.3 на момент оценки состояния линии. Если в процессе оценки состояния линии принимается решение о том, что линия свободна от посторонних подключений, то схема автоматически устанавливается в исходное состояние и переходит в ждущий режим с периодической проверкой состояния линии. Резисторы используются типа МЛТ-0,125. Диод VD1 можно заменить на КД105, Д226. Транзисторы можно заменить на КТ3102, КТ503. Микросхемы можно использовать из серий 564 и 1561. Конденсаторы Cl, С2 и СЗ должны быть с минимальным током утечки. При настройке устройства устанавливается частота генераторов 0,5-1 Гц и 12-20 кГц резисторами R3 и R10, соответственно. При включенном генераторе DD2.3 резистором R14 устанавливается уровень напряжения в линии, равный 35-45 В, при котором еще не происходит рассоединения линии. Исходные уровни срабатывания рассматриваемого устройства устанавливаются резисторами R2 и R9. Прибор необходимо подключать к линии с соблюдением полярности!

4. **Блокиратор параллельного телефона.** Во многих офисах и квартирах телефонные аппараты подключают параллельно к одной линии. Поэтому разговор между двумя абонентами легко может прослушать и тре-

тий. Чтобы исключить такую возможность используют устройство, обычно именуемое блокиратором. Схема блокиратора приведена на рис. 39. Допустим, что снята трубка с телефонного аппарата ТА2. В цепи задействованного аппарата ТА2, напряжение линии 60 В пробивает динистор VS2 типа КН102А и оно падает до 5-15 В.

Этого напряжения недостаточно для пробоя динисторов VS1, VS3 или VS4 в цепях параллельных аппаратов. Последние оказываются практически отключенными от линии очень большим сопротивлением закрытых динисторов. Это будет продолжаться до тех пор, пока первый из снявших трубку не положит ее на рычаги. Эта же схема позволит избавиться и от такого недостатка, связанного с параллельным включением аппаратов, как "подзванивание" их при наборе номера. Устройство не нуждается в настройке. При подключении необходимо соблюдать полярность напряжения питания.

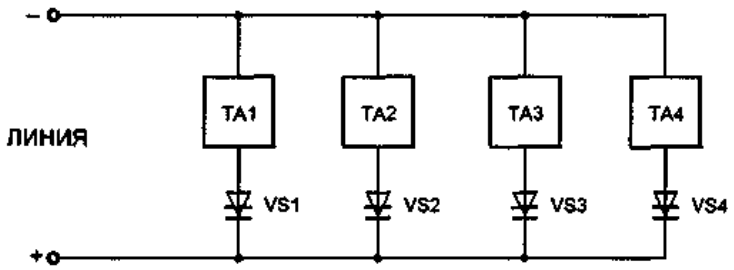


Рис. 39. Блокиратор параллельного телефона

Аналогичное устройство по принципу действия можно собрать на другой элементной базе по схеме приведенной на Рис. 40. Устройство содержит два аналога динисторов. Диоды и тиристоры могут быть с допустимым напряжением не менее 100 В и рассчитанными на ток до 0,1 А. Стабилитроны VD1 и VD3 могут быть на напряжение стабилизации 5,6 - 20 В.

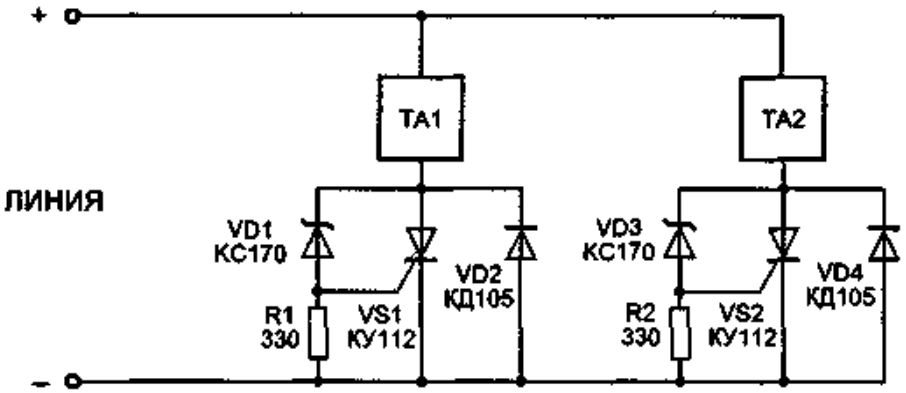


Рис. 40. Блокиратор параллельного телефона

5.2. Средства активной защиты телефонных переговоров

5.2.1. Скремблеры

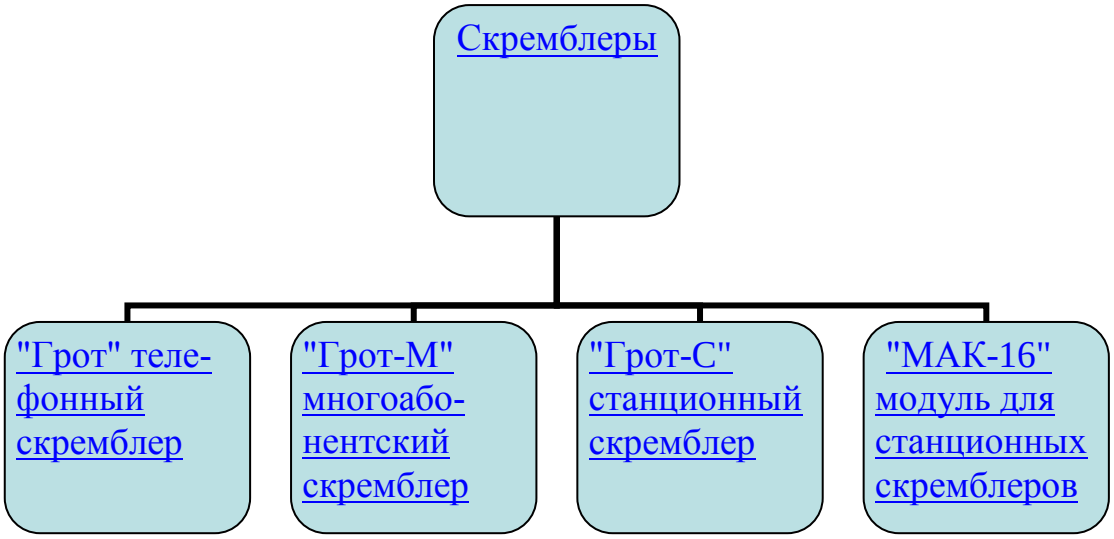


Рис. 41. Классификация скремблеров

5.2.2. Система «Грот»

Предназначен для шифрования речевого сигнала и защиты факсимильных сообщений, передаваемых по телефонной сети общего применения, см. Рис. 42.

Рис. 42. Внешний вид скремблера «Грот»

Система «Грот» может использоваться как для закрытия всего тракта от абонента до абонента при работе с любым другим скремблером серии ГРОТ или SCR-M1.2., так и для защиты абонентского участка телефонного тракта в паре с «Грот-С».

Характеристики:

- напряжение постоянного тока в абонентской линии: от 30 до 60 В;
- высокая помехоустойчивость при работе в канале связи;
- автоматическая адаптация к телефонному аппарату абонента, абонентской линии, нелинейности трактов АТС;
- устойчивость работы в реальных телефонных каналах России и стран СНГ, включая междугородные и международные с радиорелейными вставками и любыми видами уплотнения;
- совместимость с любым типом телефонного и факсимильного аппарата, с мини-АТС любого типа, имеющей аналоговый выход;

- работа в линиях, оборудованных системами уплотнения и используемых для охранной сигнализации.

Пользовательские свойства:

- высокая степень эхокомпенсации;
- низкий уровень шумов в телефонной трубке;
- высокое качество восстановленной речи;
- речевая поддержка режимов работы;
- энергонезависимая память индивидуальных ключей-идентификаторов;
- упрощенный алгоритм ввода индивидуальных ключей-идентификаторов за счет использования электронного блокнота индивидуальных ключей;

Шифрование:

- метод шифрования - мозаичный: частотные и временные перестановки;
- метод открытого распределения ключей, позволяющий работать без ручного набора ключей;
- общее количество ключевых комбинаций $2*10^{18}$;
- возможность введения дополнительного 7-ми значного ключа для идентификации абонента;
- высокая степень криптографической защиты за счет наличия дополнительных мастер-ключей, которые устанавливаются по желанию Заказчика;

Технические характеристики:

- потребляемая мощность: не более 2,5 Вт;
- питание: от сетевого адаптера или внешних батарей 9-12 В;
- габариты: 115х200х30 мм; вес: не более 0,8 кг.

Электрические параметры скремблеров Грот по стыку с телефонной линией: - напряжение постоянного тока в абонентской линии: от 30 до 60 В;

- модуль входного электрического сопротивления в разговорном режиме в режиме закрытой связи в диапазоне частот от 300 Гц до 3,4 кГц: от 500 до 750 Ом;
- модуль входного электрического сопротивления в режиме ожидания вызова в диапазоне частот от 300 Гц до 3,4 кГц: от 12 до 15 кОм;
- напряжение постоянного тока на разъеме ЛИНИЯ в режиме закрытой связи при токе в линии от 20 до 25 мА: от 6 до 13 В;
- диапазон частот по уровню 3 дБ в режиме закрытой связи: от 300 Гц до 2,7 кГц.

5.2.3. Устройство активной защиты телефонных переговоров

Предназначено для защиты телефонных переговоров на участке линии от абонента до ГАТС. Принцип действия прибора основан на маскировке спектра речи широкополосной шумовой помехой и компенсации постоянного напряжения линии. Прибор формирует синфазную и дифференциаль-

ную шумовую помеху как при «положенной», так и при «поднятой» трубке защищаемого телефонного аппарата. Прибор предназначен для эксплуатации, как на городских, так и на местных телефонных линиях, см. Рис. 44 .

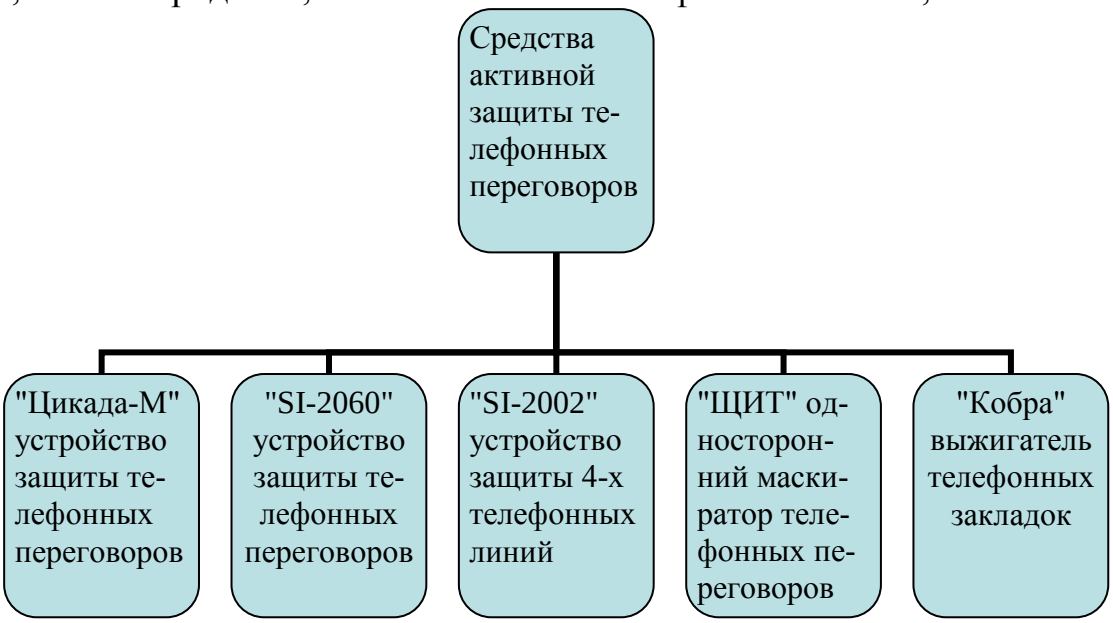


Рис. 43. Классификация средств активной защиты телефонных переговоров

Рис. 44. Устройство активной защиты телефонных переговоров

Прибор обеспечивает эффективное противодействие следующим средствам несанкционированного съема информации: - телефонным радиопередатчикам с питанием от линии и с внешним питанием, включенным в линию последовательно, параллельно или через индуктивные датчики;

- аппаратуре магнитной записи, подключаемой к линии через контактные адаптеры или индуктивные датчики;
- микрофонам и радиомикрофонам с питанием от линии и аналогичной аппаратуре (в том числе, параллельным ТА), использующей линию в качестве канала передачи информации или в качестве источника электропитания;
- аппаратуре «ВЧ-навязывания».

Технические характеристики:

- подавление устройств последовательного съема;

- подавление устройств параллельного съема;
- блокирование устройств съема с питанием от ТЛ;
- сигнализация использования параллельных ТА;
- габариты: 155 х 60 х 200 мм.

Среди средств активной защиты телефонных переговоров особое место занимает устройство «Кобра» - выжигатель телефонных закладок, с документацией которого можно познакомиться на сайте «Аском» /4/.

5.3. Защита информации от утечки по виброакустическому каналу

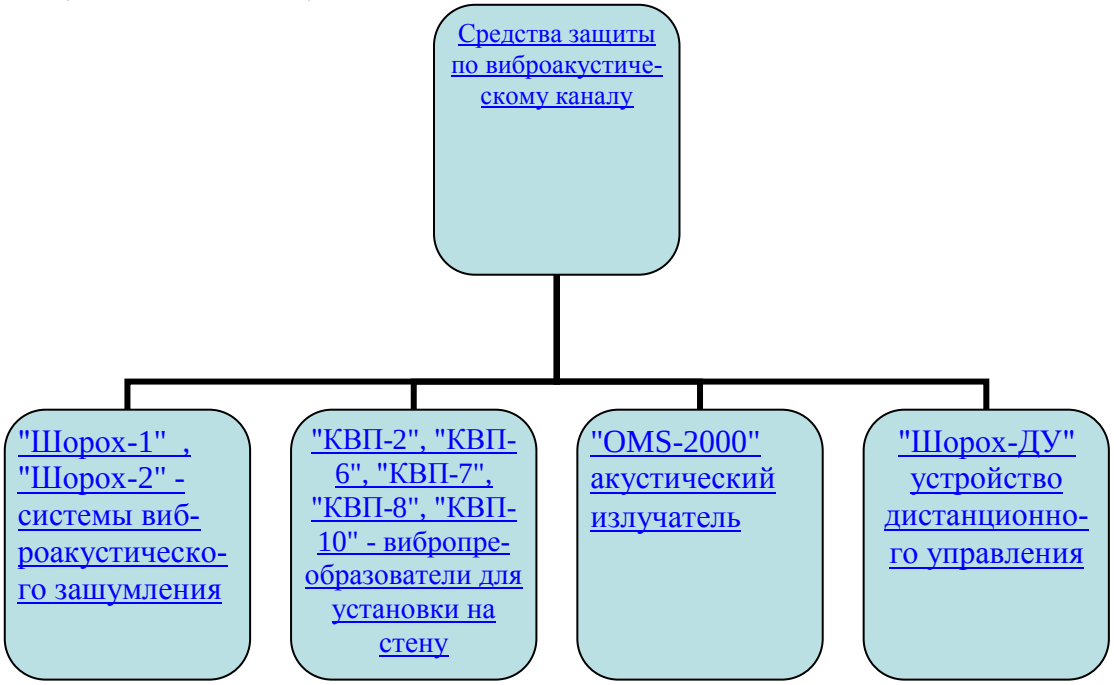


Рис. 45. Классификация средств защиты по виброакустическому каналу

5.3.1. Система виброакустического зашумления помещения.

Система виброакустического зашумления помещения Шорох-**2** /4/ предназначена для защиты выделенных помещений по виброакустическому каналу. Достоинствами системы является высокий КПД и низкий уровень паразитного акустического зашумления. Пятиполосный эквалайзер позволяет оптимальным образом сформировать спектр сигнала помехи и выполнить требования по защите помещения при обеспечении максимальной комфортности переговоров. Более высокий радиус действия вибропреобразователей позволяет выполнить требования по защите помещений применяя меньшее количество преобразователей, см. Рис. 46. Состав системы:

- Генератор сигнала помехи ГШВА-1.
- Вибропреобразователь на стену КВП-2.
- Вибропреобразователь на стену КВП-6.
- Вибропреобразователь на стену КВП-8.
- Вибропреобразователь на оконное стекло КВП-7.
- Вибропреобразователь скрытой установки в стену КВП-10.

- OMS-2000 акустический излучатель.

Рис. 46. Система виброакустического зашумления помещения Шорох-**2**

Технические характеристики:

- вид сигнала помехи: аналоговый шум с нормальным распределением плотности вероятности мгновенных значений;
- диапазон генерируемых частот: 175-5600 Гц;
- пятиполосный октавный эквалайзер с глубиной регулировки по полосам ±20 дБ;
- глубина регулировки уровня сигнала помехи: не менее 40 дБ;
- раздельная регулировка уровней акустической и виброакустической помехи;
- применяемые типы вибропреобразователей: КВП-2, КВП-6 , КВП-8 (стеновые) и КВП-7 (оконный);
- эффективный радиус действия КВП-2, КВП-6, КВП-8 на перекрытии толщиной 0,25 м: 6 ±1 м;
- эффективный радиус действия КВП-7 на стекле толщиной 4 мм: 1,5 ±0,5 м;
- к генератору одновременно могут подключаться вибропреобразователи КВП-2 - 24 шт., КВП-7 - 16 шт. и акустические колонки (8 Ом) - 16 шт;
- максимальная суммарная выходная мощность: «Шорох-2» - 19 Вт;
- габариты блока генератора: «Шорох-2» - 280х270х120 мм; вес: не более 6 кг ;
- габариты и масса вибропреобразователей: КВП-2: Ø40х30 мм; вес: 250 г; КВП-6: Ø50х39 мм; вес: 550 г; КВП-7: Ø30х10 мм; вес: 20 г; КВП-8: Ø40х36 мм; вес: 300 г.

5.3.2. Система оценки защищенности выделенных помещений по виброакустическому каналу

Система оценки защищенности выделенных помещений по виброакустическому каналу "ШЕПОТ" предназначена для измерений акустических и виброакустических параметров ограждающих и инженерных конструкций выделенных помещений. Полностью реализует методику Гостехкомиссии России. Система построена на базе прецизионного интегрирующего шумомера Larson&Davis модели 824, дополненного необходимыми элементами, обеспечивающими проведение измерений в автоматическом ре-

жиме. Основным отличием данной системы см. Рис. 47. является наличие двух измерительных каналов, позволяющих выполнять измерения в полностью автоматическом режиме, включая оценку эффективности систем активной защиты (САЗ). А также возможность выполнения измерений (при наличии беспроводных каналов передачи) при размещении датчиков (микрофонов и/или акселерометра) за строительными конструкциями и в других помещениях.

Рис. 47. Система оценки защищенности выделенных помещений по виброакустическому каналу "ШЕПОТ"

Большинство компонентов системы поставляются с автономным или универсальным электропитанием, остальные (усилитель - генератор) могут поставляться с автономным электропитанием опционно. При проведении измерений микрофоны и акселерометр могут быть отнесены на значительное расстояние от коммутатора (до 1000 м при измерениях на частотах не выше 5 кГц). Длины соединительных кабелей оговариваются при поставке. Все элементы системы, включая датчики (микрофоны, акселерометр), измерительный интерфейс, имеют калибровочные сертификаты и свидетельства о поверке. Входящий в состав системы шумомер Larson&Davis тип 824 введён в Госреестр измерительных приборов. Система полностью реализует методику Гостехкомиссии России по проведению акустических и вибрационных замеров ограждающих и инженерных конструкций, позволяя получить готовые результаты расчёта, которые включаются в состав типового протокола измерений. Измерения в каждой октавной полосе производятся непрерывно в течение заданного оператором промежутка

времени с усреднением результата, что практически полностью исключает искажения результатов случайными громкими звуками или вибрациями (минимум 240 замеров). При измерении фоновых значений акустического или вибрационного сигнала в комплексе реализовано выявление минимальных значений за период измерения, что соответствует методическим требованиям к такого рода измерениям. Результаты замеров и расчётов могут быть сохранены в виде файлов на жёстком диске управляющего компьютера и использованы для последующего применения. Предусмотрен экспорт результатов в формате "EXCEL 97/2000". Сохранённые результаты измерения и расчётов могут быть загружены в управляющую программу вновь для внесения оператором изменений с последующим перерасчётом. Это позволяет оперативно оценить количественно необходимые изменения в виброакустических параметрах объекта для выполнения условий защищённости. Дополнительно система может быть использована для контроля уровня зашумлённости помещений, уровня вибраций различных конструкций и т. д. Интерфейс управляющей программы позволяет оператору произвольно устанавливать все варьируемые параметры измерений, выбирать режимы, проводить измерения в полностью автоматическом или полуавтоматическом режимах. Управляющий компьютер подключается к измерительной системе через стандартные COM (RS 232) и LPT порты. Все необходимые измерения производятся системой в автоматическом режиме, включая управление акустическим тест-сигналом и переключение датчиков. Задачей оператора является только правильное размещение датчиков комплекса (микрофонов, акселерометра и акустического излучателя) и ручное включение (при необходимости) системы акустического или виброакустического зашумления по команде комплекса. Расчёт значений защищённости помещения по окончании цикла измерений выполняется также автоматически. Программный модуль расчёта результатов позволяет ручное занесение данных оператором и перерасчёт значений после их занесения или коррекции. Измерения могут проводится при достаточном удалении датчиков от комплекса, поскольку длина соединительных кабелей может достигать сотен метров, что позволяет выполнить весь цикл исследований без переноса самого комплекса в любом помещении. Наличие у всех составляющих комплекса автономного электропитания увеличивает его мобильность и расширяет сферу применения.

Построение программного обеспечения позволяет с минимальными доработками адаптировать его к другой модели шумомера, имеющего управление по стыку Rs232. Новое в системе «ШЁПОТ».

- В функционал системы введена задача расчёта параметров защищённости с учётом требований МВТР.
- Улучшено формирование отчёта (таблиц результатов измерений) в формате MS Word;

- Вывод таблиц в отчёте, по желанию пользователя, либо в формате, сконструированном в ЦБИ «МАСКОМ», либо в формате, предусмотренном НМД АРР;
- Поддержка вывода отчёта, по выбору пользователя в форматах:
текстовом; MS Word 97/98; MS Word 2000/2003
- Изменён и значительно упрощен для пользователя интерфейс процедуры «Калибровка» в части привязки характеристик обоих измерительных микрофонов и акселерометра друг к другу и к «нулевым» уровням отсчёта;
- Упрощено «ручноё» управления элементами комплекса за счёт ввода этих функций непосредственно в интерфейс программы;
- Появилась возможность копировать контрольные точки с выбором тех параметров, которые необходимо перенести в копию;
- Логическая оценка уровня защищённости (параметра защищённости) в контрольной точке теперь выполняется не по одному, а по любому их 3-х, выбираемых пользователем, уровням оценки;
- Выбор типа измерения («Акустика» или «Виброакустика») осуществляется не только для каждой точки, но и для группы контрольных точек;
- Включена возможность сохранения всех предварительных установок работы комплекса (включая параметры калибровки) в файл и выбора этого файла при загрузке;
- Полностью осуществлён перевод системы на работу с интерфейсом USB (с сохранением возможности использования и LPT интерфейса связи);
- С учётом опыта эксплуатации в функционирование комплекса введены изменения, позволяющие контролировать условия измерения в конкретной контрольной точке и предупреждать оператора, если эти условия не гарантируют корректности измерения с точки зрения действующих метрологических ГОСТ;
- Значительно повышена надёжность акустического излучателя;
- Радиоканалы, входящие в состав комплекса, усовершенствованы и могут теперь комплектоваться внешними антеннами, что резко увеличило гарантированную дальность их работы;

5.4. Защита информации от утечки по оптическому каналу

Для скрытности проведения перехвата речевых сообщений из помещений могут быть использованы устройства, в которых передача информации осуществляется в оптическом диапазоне. Чаще всего используется невидимый для простого глаза инфракрасный диапазон излучения. Наиболее сложными и дорогостоящими средствами дистанционного перехвата речи из помещений являются лазерные устройства. Принцип их действия заключается в посылке зондирующего луча в направлении источника звука и приеме этого луча после отражения от каких-либо предметов, например, оконных стекол, зеркал и т. д. Эти предметы вибрируют под действием окружающих звуков и модулируют своими колебаниями лазерный луч. Приняв отраженный от них луч можно восстановить мо-

дулирующие колебание. Исходя из этого, рассмотрим один из достаточно простых, но очень эффективных способов защиты от лазерных устройств. Он заключается в том, чтобы с помощью специальных устройств сделать амплитуду вибрации стекла много большей, чем вызванную голосом человека. При этом на приемной стороне возникают трудности в детектировании речевого сигнала. Ниже приведены схемы и описания некоторых устройств.

5.4.1. Простейшие модуляторы оконного стекла

Этот модулятор прост в изготовлении, содержит минимальное количество деталей и не требует налаживания. Он позволяет передавать стеклу колебания частотой 50 Гц. И в этом заключается его недостаток, так как с помощью современных средств обработки сигналов, возможно, вырезать эту частоту из спектра речевого сигнала. Принципиальная схема устройства приведена на Рис. 48. В качестве модулятора с частотой 50 Гц используется обычное мало габаритное реле постоянного тока Р1. Питается реле Р1 от сети переменного тока частотой 50 Гц и напряжением 220 В через понижающий трансформатор Т1. На выводы обмотки реле Р1 подается напряжение с вторичной обмотки трансформатора Т1 немного ниже порога срабатывания. В качестве трансформатора используется любой, желательно малогабаритный, понижающий трансформатор. Напряжение на обмотке II выбирается в зависимости от используемого реле. Реле Р1 может быть типа РЭС22, РЭС9 и им подобные. Корпус реле приклеивается к стеклу клеем "Момент" или аналогичным.

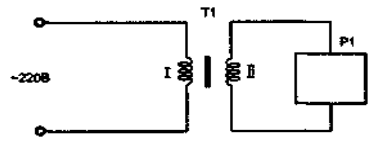


Рис. 48. Модулятор оконного стекла с трансформатором

Если подходящего трансформатора подобрать не удалось, то можно воспользоваться бестрансформаторной схемой устройства приведенной на Рис. 49. Конденсатор С1 гасит излишек напряжения, он подбирается под определенную нагрузку. Его можно разместить прямо в штепсельной вилке.

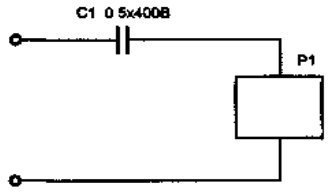


Рис. 49. Модулятор оконного стекла

5.4.2. Модулятор на одной микросхеме

Этот модулятор питается от сети переменного тока напряжением 220 В. Принципиальная схема модулятора приведена на Рис. 50.

Напряжение сети гасится резисторами R1 и R2 и выпрямляется диодом VD1 типа КД102А. Конденсатор С1 уменьшает пульсации выпрямленного напряжения. Модулятор выполнен на одной микросхеме К561ЛЕ5. По своему схемному построению он напоминает генератор качающей частоты или частотный модулятор. На элементах DD1.3 и DD1.4 собран управляющий генератор низкой частоты. С его выхода прямоугольные импульсы поступают на интегрирующую цепочку R5C4. При этом конденсатор С4 то заряжается через резистор R5, то разряжается через него. Поэтому на конденсаторе С4 получается напряжение треугольной формы, которое используется для управления генератором на элементах DD1.1, DD1.2. Этот генератор собран по схеме симметричного мультивибратора. Конденсаторы С2 и С3 поочередно заряжаются через резисторы R3 и R4 от источника треугольного напряжения. Поэтому на выходе генератора будет иметь место сигнал, частота которого "плавает" в области звуковых частот речевого диапазона. Поскольку питание генератора не стабилизировано, то это приводит к усложнению характера генерируемых сигналов.

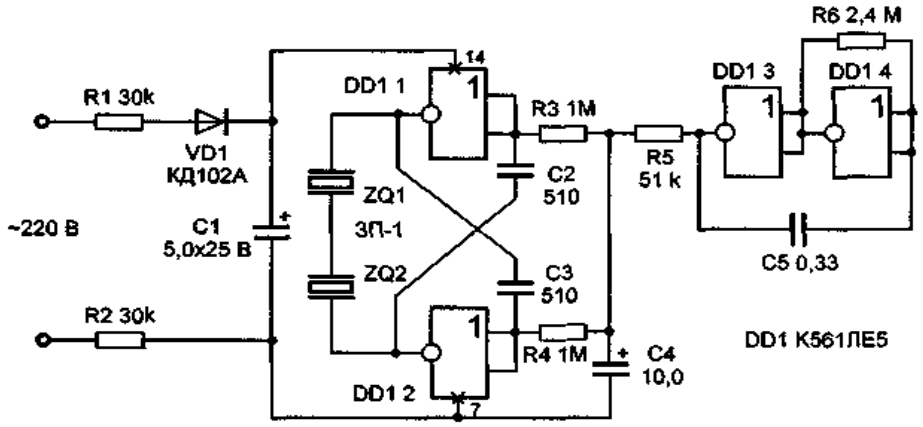


Рис. 50. Модулятор на одной микросхеме

Нагрузкой генератора служат пьезокерамические излучатели ZQ1 и ZQ2 типа ЗП-1. Микросхему DD1 можно заменить на К561ЛА7 или на К561ЛН1, К561ЛН2, либо на микросхемы серий 564, 1561. Излучатели ZQ1 и ZQ2 могут быть любыми, их количество может быть от одного до четырех. Они могут быть соединены последовательно или параллельно-последовательно.

5.4.3. Модулятор стекла на микросхемах

Принципиальная схема устройства приведена на Рис. 51. Данное устройство вызывает вибрацию стекла с различной частотой, тем самым, устраняя основной недостаток простейшего модулятора. Оно выполнено на

двух цифровых схемах 561 серии. В качестве вибропреобразователя используется пьезокерамический преобразователь.

Модулятор собран на микросхемах К561ЛН2 и К561ИЕ8. Генератор тактовых импульсов собран на элементах DD1.1, DD1.2, резисторе R1 и конденсаторе C1 по схеме несимметричного мультивибратора. С выхода генератора тактовые импульсы поступают на вход счетчика DD2 типа К561ИЕ8. Эта микросхема имеет встроенный дешифратор, поэтому напряжение высокого уровня поочередно появляется на выходах счетчика в соответствии с количеством пришедших импульсов. Допустим, что после прихода очередного тактового импульса уровень логической единицы появился на выходе 2 микросхемы DD2 (выв. 4).

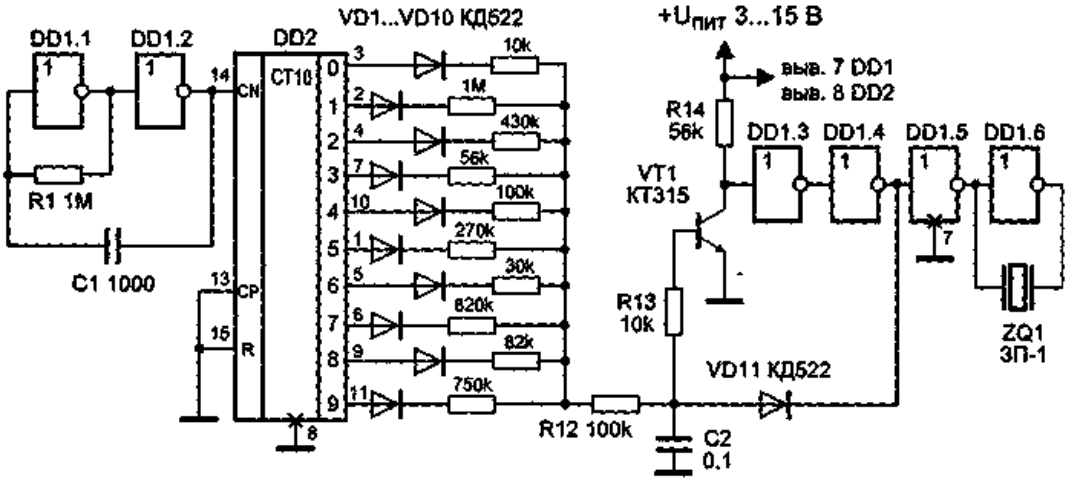


Рис. 51. Модулятор на микросхемах

На остальных выходах присутствует уровень логического нуля. Положительное напряжение начинает заряжать конденсатор C2 по цепи VD3, R4, R12. При достижении на конденсаторе C2 напряжения, достаточного для открывания транзистора VT1 типа КТ315, последний открывается, и на выходе элемента DD1.4 появляется уровень логического нуля. Конденсатор C2 быстро разряжается через диод VD11 типа КД522. Транзистор VT1 закрывается, и процесс заряда конденсатора C2 возобновляется по той же зарядной цепи. С приходом очередного тактового импульса уровень положительного напряжения появляется только на выходе 3 (выв. 7). Теперь конденсатор C2 заряжается по цепи VD4, R5, R12. Так как суммарное сопротивление этой цепи меньше, чем сопротивление цепи VD3, R4, R12, то заряд конденсатора C2 до напряжения открывания происходит быстрее. Частота импульсов на выходе этого управляемого генератора увеличивается. Прямоугольные импульсы поступают на вибропреобразователь ZQ1, выполненный на основе пьезокерамического преобразователя. Микросхемы DD1 и DD2 можно заменить на аналогичные - серий 176, 564, 1561. Резисторы - типа

МЛТ-0,125. Сопротивления резисторов R2-R11 могут быть любыми из интервала 10 кОм — 1 МОм. Резисторы одинакового номинала лучше не использовать. Диоды VD1—VD11 могут быть любыми, например, КД521, Д9, Д18, КД510 и др. Транзистор VT1 можно заменить на КТ3102. Пьезокерамический преобразователь ZQ1 может быть любой, от игрушек или телефонных аппаратов. Питание устройства осуществляется от батарейки типа "Крона". Вибродатчик ZQ1 приклеивается на стекло клеем типа "Момент". Сигнал к нему подводится по проводам от элемента DD1.6. Настройка заключается в установке частоты тактового генератора подбором конденсатора C1 или резистора R1. Частота тактовых импульсов выбирается около 2-3 Гц.

Количество генерируемых частот можно увеличить, если вместо микросхемы DD2 К561ИЕ8 использовать широко распространенную микросхему К561ИЕ10. Эта микросхема содержит два двоичных четырехразрядных счетчика. К выходам счетчиков подключаются резисторы R2-R9, их сопротивления могут быть также от 10 кОм до 1 МОм. Диоды VD1-VD10 из схемы исключаются. При подаче тактовых импульсов на вход СТ микросхемы DD2.1 в точке соединения резисторов R2—R12 появляется, изменяющееся ступенчато, напряжение. Число градаций напряжения, а, следовательно, и число частот, можно варьировать путем использования определенного количества разрядов счетчика DD2.

5.4.4. Генераторы акустического шума

Акустические генераторы шума используются для зашумления акустического диапазона в помещениях и в линиях связи, а также для оценки акустических свойств помещений. Под "шумом" в узком смысле этого слова часто понимают, так называемый, белый шум, характеризующийся тем, что его амплитудный спектр распределен по нормальному закону, а спектральная плотность мощности постоянна для всех частот. В более широком смысле под шумом, по ассоциации с акустикой, понимают помехи, представляющие собой смесь случайных и кратковременных периодических процессов. Кроме белого шума выделяют такие разновидности шума, как фликкер-шум и импульсный шум. В генераторах шума используется белый шум, так как даже современными способами обработки сигналов этот шум плохо отфильтровывается. Ниже приводятся несколько схем различных генераторов шума.

1. **Генератор белого шума.** Самым простым методом получения белого шума является использование шумящих электронных элементов (ламп, транзисторов, различных диодов) с усилением напряжения шума. Принципиальная схема несложного генератора шума приведена на рис. 52. Источником шума является стабилитрон VD1 типа КС168, работающий в режиме лавинного пробоя при очень малом токе. Сила тока через стабилитрон VD1 составляет всего лишь около 100 мкА. Шум, как полезный сигнал, снимается с катода стабилитрона VD1 и через конденса-

тор С1 поступает на инвертирующий вход операционного усилителя DA1 типа КР140УД1208. На вход этого усилителя поступает напряжение смещения, равное половине напряжения питания с делителя напряжения, выполненного на резисторах R2 и R3. Режим работы микросхемы определяется резистором R5, а коэффициент усиления - резистором R4.

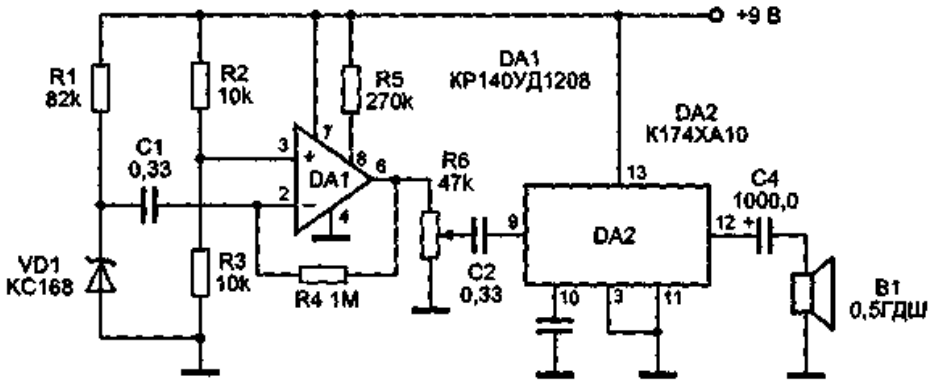


Рис. 52. Генератор шума

С нагрузки усилителя переменного резистора R6 усиленное напряжение шума поступает на усилитель мощности, выполненный на микросхеме DA2 типа К174ХА10. С выхода усилителя шумовой сигнал через конденсатор С4 поступает на малогабаритный широкополосный громкоговоритель В1. Уровень шума регулируется резистором R6. Стабилитрон VD1 генерирует шум в широком диапазоне частот от единиц герц до десятков мегагерц. Однако на практике он ограничен АЧХ усилителя и громкоговорителя. Стабилитрон VD1 подбирается по максимальному уровню шума, так как стабилитроны представляют собой некалиброванный источник шума. Он может быть любым с напряжением стабилизации менее напряжения питания. Микросхему DA1 можно заменить на КР1407УД2 или любой операционный усилитель с высокой граничной частотой коэффициента единичного усиления. Вместо усилителя на DA2 можно использовать любой УЗЧ.

2. Цифровой генератор шума. Цифровой шум представляет собой временной случайный процесс, близкий по своим свойствам к процессу физических шумов и называется, поэтому псевдослучайным процессом. Цифровая последовательность двоичных символов в цифровых генераторах шума называется псевдослучайной последовательностью, представляющей собой последовательность прямоугольных импульсов псевдослучайной длительности с псевдослучайными интервалами между ними. Период повторения всей последовательности значительно превышает наибольший интервал между импульсами. Наиболее часто применяются последовательности максимальной длины - М-последовательности, которые формируются при помощи регистров сдвига и сумматоров по модулю 2, использующихся для получения сигнала обратной связи. Принципиальная схема генератора шума с равномерной спектральной плотностью в рабочем

диапазоне частот приведена на Рис. 53. Этот генератор шума содержит последовательный восьмиразрядный регистр сдвига, выполненный на микросхеме К561ИР2, сумматор по модулю 2 (DD2.1), тактовый генератор (DD2.3, DD2.4) и цепь запуска (DD2.2), выполненные на микросхеме К561ЛП2. Тактовый генератор выполнен на элементах DD2.3 и DD2.4 по схеме мультивибратора. С выхода генератора последовательность прямоугольных импульсов с частотой следования около 100 кГц поступает на входы "С" регистров сдвига DD1.1 и DD1.2, образующих 8-разрядный регистр сдвига. Запись информации в регистр происходит по входам "D". На вход "D" регистра DD1.1 сигнал поступает с элемента обратной связи сумматора по модулю «2» DD2.1. При включении питания возможно состояние регистров, когда на всех выходах присутствуют низкие уровни. Так как в регистрах М-последовательности запрещено появление нулевой комбинации,
то в схему введена цепь запуска генератора, выполненная на элементе DD2.2.

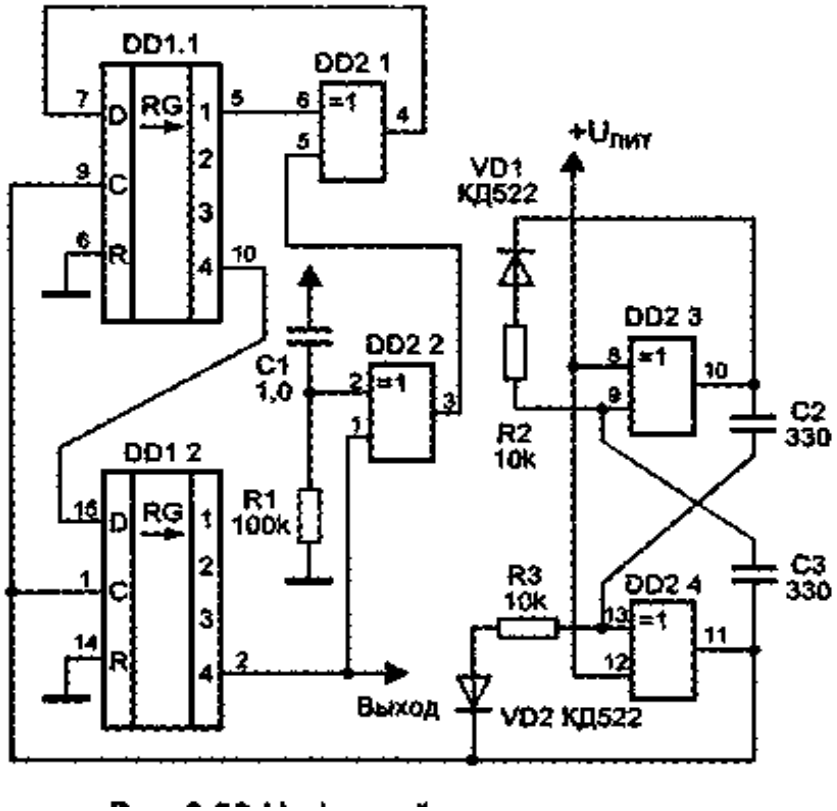


Рис. 53. Генератор шума

При включении питания последний формирует на своем выходе уровень логической единицы, который выводит регистр из нулевого состояния. На дальнейшую работу генератора цепь запуска не оказывает никакого влияния. Сформированный псевдослучайный сигнал снимается с 8-го разряда регистра сдвига и поступает для дальнейшего усиления и излучения. Напряжение источника питания может быть от 3 до 15 В. В устройстве использованы КМОП микросхемы серии 561, их можно заменить на микросхемы серий К564, К1561 или К176. В последнем случае напряжение пи-

тания должно быть 9 В. Правильно собранный генератор в налаживании не нуждается. Изменением тактовой частоты можно регулировать диапазон частот шума и интервал между спектральными составляющими для заданной неравномерности спектра.

3. Акустический генератор шума WNG 023 /4/, приведен на Рис. 54 и предназначен для защиты переговоров от любых видов съема акустической информации.

Рис. 54. Генератор шума

Принцип действия основан на постановке акустической помехи речевого диапазона частот. Перед началом проведения переговоров, генератор устанаваливается в защищаемом помещение максимально близко к наиболее вероятному месту размещения устройств съема акустической информации (например, дверь). Максимальный защищаемый объем составляет 50м^3.

4. Система защиты переговоров «ХАОС» фирмы «АСКОМ» /4/, предназначена для предотвращения несанкционированного перехвата акустической (речевой) информации любыми средствами акустического контроля, например радио микрофонами, проводными микрофонами, стетоскопами, любыми типами диктофонов, направленными микрофонами, диктофонами сотовых телефонов, а также с помощью технических средств обладающих «микрофонным эффектом» или к которым применительно использование метода «высокочастотного навязывания». Используемый микрофон также исключает возможность перехвата информации методом «чтения по губам». Система является универсальным прибором и может использоваться как в стационарных, так и в мобильных (неподготовленных) условиях, и рассчитана на длительный срок непрерывной эксплуатации. Переговоры осуществляются с помощью наушников с шумопоглащающими гарнитурами и специальных микрофонов. Речевые сигналы, поступающие с микрофонов, подвергаются обработке для отсева помеховой составляющей. Имеется возможность индивидуальной регулировки громкости и отключения микрофона. Речь говорящего абонента, перехватываемая средствами контроля, представляет собой смесь "речевой помехи", создаваемого прибором и речи абонента.

5.5. Средства защиты от несанкционированного применения диктофонов

Классификация средств защиты от несанкционированного применения диктофонов приведена на Рис. 55.

5.5.1. "Сапфир-К" подавитель диктофонов в кейсе.

Рассмотрим характеристики одного из устройств Сапфир, принцип работы которых описан в разделе генераторы шума /4/.

«Сапфир-К» предназначен для предотвращения утечки информации за счет несанкционированного (скрытного) применения диктофонов и других портативных средств звукозаписи в оперативных условиях.

Позволяет бороться с любыми типами диктофонов.

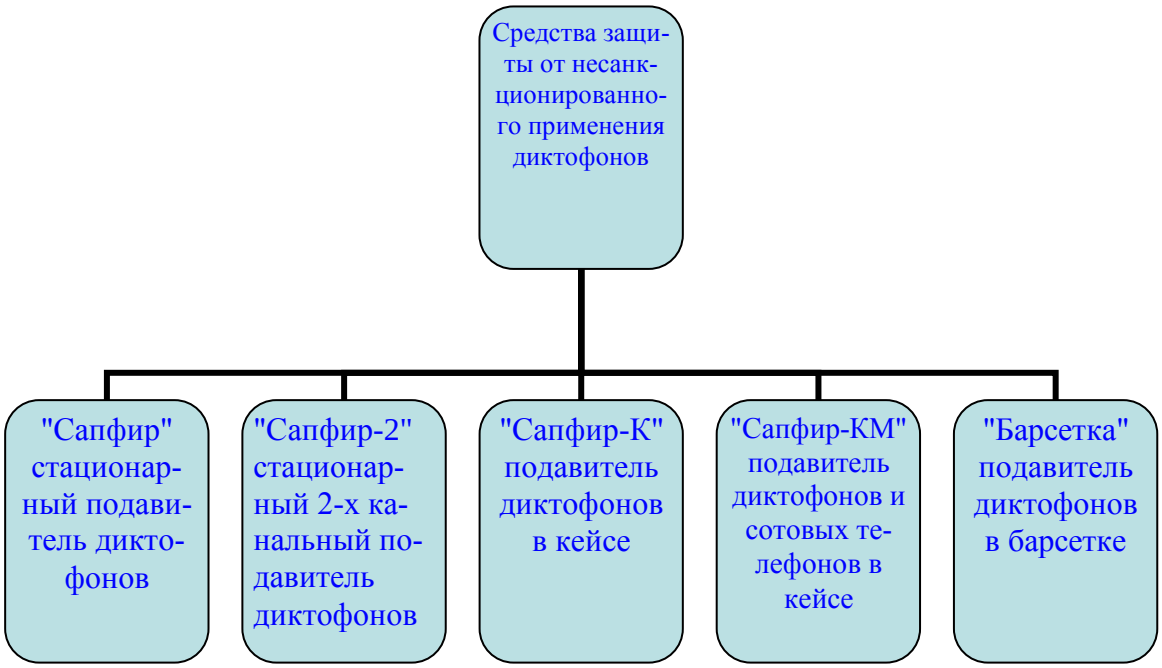


Рис. 55. Средства для подавления диктофонов

Подавитель выполнен в виде кейса со встроенной антенной. Лепесток излучения в этом случае направлен перпендикулярно поверхности кейса.
Технические характеристики:

- дальность подавления цифровых диктофонов: от 2 метров;
- дальность подавления кинематических диктофонов: от 3,5 метров;
- время непрерывной работы: 1,5 часа;
- управление: радиоканал, ручное;
- антенны: встроенные.

5.5.2.Стационарный подавитель диктофонов.

«Сапфир», см. Рис. 56 предназначен для предотвращения утечки информации за счет несанкционированного (скрытного) применения диктофонов и других портативных средств звукозаписи в стационарных условиях.

Позволяет бороться с любыми типами диктофонов.

Рис. 56. Стационарный подавитель диктофонов «Сапфир»

Дальность подавления лежит в следующих пределах:

- цифровые диктофоны: от 2 метров;
- кинематические диктофоны: от 3,5 метров.

Подавитель состоит из генератора сигнала помехи и внешней направленной излучающей антенны. С одним генератором применяется, как правило, одна антенна.

Возможные три типы применяемых антенн, одна из которых приведена на Рис. 57.

Рис. 57. Антенна с излучением в противоположные стороны

Антенна устройства «Сапфир» предназначена для защиты столов переговоров. Устанавливается под поверхностью стола. За счет излучения в противоположные стороны удается защитить 4 посадочных места одновременно, два с одной стороны и два с другой. Каждый лепесток излучения имеет размеры: 120 х 90 градусов.

Выводы по главе:

1. Одним из основных каналов утечки информации является телефонный аппарат и линия связи, его с автоматической телефонной станцией (АТС). Для специалиста, работающего в области шпионажа с применением технических средств контроля, наибольший интерес представляют комплексы средств, позволяющие получать информацию из интересующих помещений без необходимости физического присутствия в них.

2. При включении многих электронных приборов по защите телефонного аппарата и линии необходимо соблюдать полярность включения.

Вопросы для самоконтроля:

Вопрос 1. В чем достоинство цифрового генератора шума?

Вопрос 2. В чем заключается принцип метода защиты от утечки информации по оптическому каналу?

Вопрос 3. Какие существуют методы защиты телефонных аппаратов?

Вопрос 4. Зачем применяются индикаторы состояния линии связи?

Вопрос 5. Приведите сравнительный анализ средств защиты.

Вопрос 6. Приведите классификацию средств защиты по различным каналам.

Методические рекомендации.

Изучив материал главы, ответьте на вопросы. При возникновении трудностей обратитесь к материалам для закрепления знаний в конце пособия.

Для углубленного изучения воспользуйтесь литературой:

основной: 1 – 2; дополнительной: 4 – 6 и повторите основные определения, приведенные в конце пособия.

ГЛАВА 6 . ИСПОЛЬЗОВАНИЕ ВИДЕОТЕХНИКИ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

В первых главах были рассмотрены системы и устройства видеотехники, применяемые для контроля и добывания информации. Но, как довольно часто бывает в жизни, такая же техника с успехом может быть использована и для защиты информации. Прежде всего, это различные системы охраны помещений и территории. Такие системы можно условно разделить на:

- системы скрытой охраны, т.е. такие системы обнаружить без специальной техники невозможно;
- системы отрытого наблюдения, т.е. системы, применение которых явно заметно и кроме основной функции выполняют еще и функцию отпугивания;
- отпугивающие (имитирующие) системы.

Скрытые системы наблюдения имеют то преимущество, что с их помощью можно выявить поведение людей в обстановке, когда они остаются одни в помещении. Это может помочь в выявлении источников утечек информации. Системы открытого наблюдения применяются тогда, когда не нужно скрывать факты наблюдения. В этом случае сам факт присутствия видеокамеры сдерживает потенциального вредителя от неправомерных действий. Отпугивающие системы, как видно из названия, предназначены для имитации систем охраны помещений. Другими словами, это очень точно выполненные макеты видеокамер. Преимуществом таких устройств является дешевизна.

Системы скрытого и открытого наблюдения отличаются, прежде всего, типом применяемых видеокамер. Для ложных видеокамер используется чаще всего корпус от настоящей видеокамеры с подведенными к ней кабелями. Для повышения достоверности может встраиваться светящийся светодиод. Системы фототехники используются для фотосъемки посетителей банков, режимных учреждений и т.д. В качестве примера рассмотрим фотокамеру ROBOT, это автоматическая фотокамера с размером кадра 24х36 мм. На одной кассете помещается от 800 до 1600 снимков, в зависимости от того, используется стандартная или тонкая фотопленка. Скорость съемки - до 2 кадров в секунду, выдержка 1/30 или 1/60 с, объективы: 28, 35 или 50 мм. На фотоснимке электронным способом фиксируется время, дата и код офиса. Камера имеет размеры 270х135 мм.

ЗАКЛЮЧЕНИЕ

Целью данного учебного пособия является изучение основных каналов утечки информации, их характеристик, а также обобщение методов и устройств защиты от несанкционированного доступа, получения или искажения информации.

Необходимым условием разработки системы защиты информации является соблюдение следующих принципов:

- учет требований защиты информации при построении объекта защиты и разработке технологии автоматизированной обработки информации;
- комплексность использования средств и методов защиты;
- обеспечение непрерывности процесса защиты;
- обеспечение периодического контроля правильности функционирования всех подсистем защиты.

Защита выделенного помещения — проведение комплекса организационно-технических мероприятий по предотвращению утечки речевой секретной или конфиденциальной информации по техническим каналам за пределы выделенного помещения. В общем случае комплекс мероприятий по защите выделенных помещений включает:

- защиту речевой информации, обрабатываемой техническими средствами от утечки за счет электромагнитных излучений и наводок (ПЭМИН);
- защиту речевой информации от утечки за счёт эффекта электроакустического преобразования вспомогательных технических средств и систем (ВТСС);
- защиту речевой информации от утечки за счёт лазерного зондирования стекол или стетоскопического прослушивания ограждающих конструкций;
- защиту речевой информации от утечки за счет несанкционированного доступа в помещение и скрытой установки в нем подслушивающих приборов (микрофонов, магнитофонов, радиопередатчиков и т.д.);
- акустическую защиту помещений.

Все это влияет на выработку политики безопасности информационных систем организации и ведет к необходимости учета следующих факторов:

- определения целей защиты;
- определения объекта защиты;
- определения актуальных угроз, субъектов этих угроз, выбора профилей защиты;
- разработки методов определения качества защиты или выбора уже существующих систем критериальных оценок;
- получения гарантий защищенности системы.

Необходимо помнить, что эффективность защиты информации это степень соответствия достигнутого уровня защищенности информации поставленной цели.

ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ИТОГОВОГО КОНТРОЛЯ

1. Нормативная база по защите информации.
2. Основные методы ведения промышленного шпионажа.
3. Принцип работы закладных устройств.
4. Закладные устройства с передачей информации по радиоканалу.
5. Направленные микрофоны.
6. Диктофоны.
7. Устройства высокочастотного навязывания.
8. Устройства для перехвата речевой информации по проводным каналам связи.
9. Оптико-акустическая аппаратура перехвата речевой информации.
10. Приборы ночного видения.
11. Средства для получения материалов видеосъемки.
12. Система защиты информации.
13. Защита телефонных аппаратов от прослушивания.
14. Защита микрофонной сети.
15. Скремблеры.
16. Устройства активной защиты телефонных переговоров.
17. Системы виброакустического зашумления помещения.
18. Методы защиты информации от утечки по оптическому каналу.
19. Устройства модуляции оконного стекла.
20. Генераторы акустического шума.
21. Методы использования видеотехники для защиты информации.
22. Федеральный закон «О безопасности».
23. Федеральный закон «О техническом регулировании».
24. Федеральный закон «Об информации, информатизации и защите информации».
25. Методы ведения шпионажа в оптическом диапазоне.
26. Методы ведения шпионажа в звуковом диапазоне частот.
27. Сравнительная характеристика методов и средств нападения и защиты в аудио- и видеоинформационных каналах.
28. Перспективы развития средств промышленного шпионажа.
29. Основные направления развития методов и средств защиты информации в видео каналах.
30. Сравнительная характеристика основных предприятий по производству средств нападения и защиты в аудио- и видеоинформационных каналах.

ПЕРЕЧЕНЬ ТЕМ КОНТРОЛЬНЫХ РАБОТ

№ п/п	Тема контрольной работы	Буква алфавита, с которой начинается Ваша фамилия
1	Перспективы развития средств промышленного шпионажа.	А
2	Методы ведения шпионажа в оптическом диапазоне.	Б
3	Методы ведения шпионажа в звуковом диапазоне частот.	В
4	Сравнительная характеристика основных предприятий по производству средств нападения и защиты в аудио- и видеоинформационных каналах.	Г
5	Нормативная база по защите информации.	Д
6	Методы использования видеотехники для защиты информации.	Е
7	Направленные микрофоны.	Ж
8	Приборы ночного видения.	З
9	Устройства магнитной записи	И
10	Устройства видеосъемки	К
11	Федеральные законы о защите информации	Л
12	Средства активной защиты телефонных переговоров	М, Я
13	Фотоаппараты	Н
14	Защита телефонных аппаратов и линии связи	О
15	Скремблеры	П, Ю
16	Устройства CD	Р
17	Форматы DVD	С
18	Системы виброакустического зашумления помещения.	Т, Э
19	Методы защиты информации от утечки по оптическому каналу.	У, Ф,Х, Ц
20	Фотообъективы	
21	Основные методы ведения промышленного шпионажа.	Ч Ш, Щ

ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ

Акустическая защищённость выделенного помещения - уровень акустической защищенности выделенного помещения, достигнутый в результате проведения акустической защиты. Уровень акустической защищённости проверяется и оценивается при проведении аттестации выделенного помещения.

Аттестация выделенного помещения - официальное подтверждение органом по аттестации (сертификации) или другим специально уполномоченным органом наличия необходимых и достаточных условий, обеспечивающих надежную акустическую защищенность выделенного помещения в соответствии с установленными нормами и требованиями. По результатам аттестации выделенному помещению устанавливается группа защищенности.

Аутентификация пользователя — подтверждение подлинности пользователя с помощью предъявляемого им аутентификатора.

Безопасность информации — состояние уровня защищенности информации при её обработке техническими средствами, обеспечивающее сохранение таких ее качественных характеристик (свойств), как секретность (конфиденциальность), целостность и доступность.

Белый (акустический) шум — сложный акустический сигнал, имеющий постоянную спектральную плотность во всем диапазоне частот.

Виброакустический канал утечки акустической (речевой) информации - канал утечки акустической (речевой) информации, обусловленный распространением механических колебаний из твердой среды в воздушную и возбуждением последней.

Владелец информации — субъект информационных отношений, обладающий правом владения, распоряжения и пользования информационным ресурсом по договору с собственником информации.

Внешнее воздействие на информационный ресурс — фактор опасности, вызываемый стихийными бедствиями, мощными электромагнитными излучениями или диверсионными актами и приводящий к нарушению целостности информации или ее блокированию.

Воздушный канал утечки акустической (речевой) информации — канал утечки акустической (речевой) информации, средой распространения акустических сигналов в котором является воздух. Воздушная среда может быть обычной атмосферной или искусственно созданной газовой средой. В соответствии с этим различают атмосферный и газовый каналы утечки акустической (речевой) информации.

Возможности технической разведки — характеристики способности обнаружения, распознавания, измерения и регистрации технических демаскирующих признаков объекта средствами технической разведки.

Гарантия защиты — наличие сертификата соответствия для технического средства обработки информации или аттестата на объект информа-

тики, подтверждающих, что безопасность обрабатываемой информации соответствует требованиям стандартов и других нормативных документов.

Громкость звука — степень физиологического воздействия акустических (звуковых) колебаний на органы слуха человека. Степень физиологического воздействия звуковых колебаний на органы слуха человека пропорциональны логарифму изменения интенсивности этих колебаний (закон Вебера-Фехнера). Поэтому громкость звука выражается в логарифмических единицах - децибелах (Дб).

Защита выделенного помещения — проведение комплекса организационно-технических мероприятий по предотвращению утечки речевой секретной или конфиденциальной информации по техническим каналам за пределы выделенного помещения. В общем случае комплекс мероприятий по защите выделенных помещений включает:

- защиту речевой информации, обрабатываемой техническими средствами от утечки за счет электромагнитных излучений и наводок (ПЭМИН);
- защиту речевой информации от утечки за счёт эффекта электроакустического преобразования вспомогательных технических средств и систем (ВТСС);
- защиту речевой информации от утечки за счёт лазерного зондирования стекол или стетоскопического прослушивания ограждающих конструкций;
- защиту речевой информации от утечки за счет несанкционированного доступа в помещение и скрытой установки в нем подслушивающих приборов (микрофонов, магнитофонов, радиопередатчиков и т.д.);
- акустическую защиту помещений.

Защита информации — деятельность, направленная на сохранение государственной, служебной, коммерческой или личной тайн, а также на сохранение носителей информации любого содержания. Существуют три основные формы защиты информации: правовая, организационно-техническая и страховая.

Защита информации от технических разведок — деятельность, направленная на предотвращение или существенное снижение возможностей технических разведок по получению разведывательной информации путем разработки и реализации системы защиты. Замысел защиты информации от технических разведок должен удовлетворять требованиям (принципам) комплексности, активности, убедительности, непрерывности и разнообразия.

Зона разведдоступности - часть пространства вокруг объекта, в пределах которого реализуются возможности технической разведки.

Искажение информации - случайная несанкционированная модификация информации при ее обработке техническими средствами в результате внешних воздействий (помех), сбоев в работе аппаратуры или неумелых действий обслуживающего персонала.

Канал утечки акустической (речевой) информации — совокупность

источника акустических колебаний (источника речевой информации), среды распространения акустических сигналов и акустического приемника, обусловливающая возможность обнаружения и перехвата акустической (речевой) информации. В общем случае средой распространения могут быть газовые (воздушные), жидкостные (водные) и твердые среды, в том числе недра Земли.

Категория безопасности информации - уровень безопасности информации, определяемый установленными нормами в зависимости от важности (ценности) информации. Критериями безопасности могут быть следующие показатели:

- для ПЭМИН - абсолютный уровень ПЭМИН или соотношение: информационный сигнал/помеха в эфире и токопроводящих коммуникациях;
- для НСД - вероятность НСД;
- для аппаратных закладок - наличие проведенной спецпроверки по поиску и аннулированию закладных устройств;
- для внешних воздействий на информационный ресурс - вибростойкость, влагостойкость, пожаростойкость, устойчивость против электромагнитного воздействия.

Комплексность защиты — принцип защиты, предусматривающий мероприятия против всех опасных видов и средств технической разведки.

Контролируемая зона — территория вокруг технического средства обработки информации, в пределах которой не допускается несанкционированное пребывание посторонних лиц и транспортных средств. Размер контролируемой зоны должен быть не менее размера зоны

Критерий безопасности информации — показатель, характеризующий безопасность информации при воздействии различных факторов опасности.

Модель технической разведки — описание средств технической разведки, содержащее их технические характеристики и организацию использования в объеме, достаточном для оценки возможностей технической разведки.

Опасная зона 1 - пространство вокруг технического средства обработки информации, в пределах которого на случайных антеннах наводится опасный сигнал выше допустимого нормированного уровня. В зоне 1 запрещается размещение случайных антенн, имеющих выход по токопроводящим коммуникациям за пределы контролируемой зоны.

Опасная зона 2 - пространство вокруг технического средства обработки информации, в пределах которого отношение: опасный сигнал/помеха для составляющих напряженности электромагнитного поля превышает допустимое нормированное значение. Зона 2 должна быть контролируемой, так как в этой зоне возможен перехват побочных электромагнитных излучений с помощью идеального приемника и последующая расшифровка содержащейся в них информации.

Оптико-электронный (лазерный) канал утечки акустической (речевой)

информации — канал утечки акустической (речевой) информации, обусловленный процессом зондирования лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей (стекла, окон, картин, зеркал и т.п.), модуляции этого луча по закону вибрации поверхностей и приемом отраженного (зеркально или диффузно) луча оптическим (лазерным) приемником.

Организационное мероприятие по защите информации — мероприятие по защите информации, предусматривающее использование маскирующих свойств окружающей среды и установление временных, территориальных и пространственных ограничений на условия использования и режимы работ объекта.

Организационно-техническая форма защиты информации — защита информации, предусматривающая применение руководящих, нормативных и методических документов, лицензирование деятельности в области защиты информации, сертификацию защищенных изделий, технических средств и способов защиты, создание на объектах систем защиты информации и аттестацию этих объектов.

Организационный контроль эффективности защиты информации — контроль эффективности защиты информации путем проверки соответствия состояния, организации, наличия документов, полноты и обоснованности мероприятий по защите информации требованиям организационно-распорядительных и нормативных документов.

Параметр акустической защиты (защищенности) выделенного помещения — показатель, который принимается для оценки акустической защиты (защищенности) выделенного помещения. В качестве параметра акустической защиты (защищенности) выделенного помещения принято отношение уровня речевого сигнала, проникающего за пределы выделенного помещения, к уровню стабильного шумового фона в той же точке (отношение сигнал/шум).

Параметр технического демаскирующего признака — показатель технического демаскирующего признака объекта, используемый технической разведкой для получения разведывательной информации. К параметрам прямых демаскирующих признаков относятся напряженность магнитного и электромагнитного полей по сравнению с магнитным (электромагнитным) фоном окружающей среды, уровень электромагнитных наводок на вспомогательных технических средствах и системах, интенсивность (звуковое давление) акустического поля и т. д., а параметрами косвенных демаскирующих признаков могут быть геометрические размеры тех или иных объектов, контрастность их освещенности, уровень радиоактивного или химического заражения окружающей местности по сравнению с естественным фоном и другие параметры.

Параметрический канал утечки акустической (речевой) информации - канал утечки акустической (речевой) информации, обусловленный параметрическим преобразованием акустического (речевого) сигнала в нели-

нейном акустическом поле, создаваемом направленным излучением мощных высокочастотных бигармонических колебаний (волн накачки). Нелинейное взаимодействие акустических сигналов и разностной частоты волн накачки (так называемой вторичной волны) способствует созданию острой (без боковых лепестков) диаграммы направленности излучения, обеспечивающей передачу акустической информации на большие расстояния.

Пассивное техническое средство защиты — техническое средство защиты, обеспечивающее скрытие объекта защиты от технических разведок путем поглощения, отражения или рассеивания его излучений. К пассивным техническим средствам защиты относятся маски различного назначения, экранирующие устройства и сооружения, разделительные устройства в сетях электроснабжения, защитные фильтры и т. д.

Помеха технической разведке - физический процесс или действие, обеспечивающее полное подавление или существенное снижение возможностей технической разведки.

Правила доступа - правила, установленные для осуществления доступа субъекта к информационному ресурсу с использованием штатных технических средств.

Розовый (акустический) шум — сложный акустический сигнал, уровень спектральной плотности которого убывает с повышением частоты с постоянной крутизной, равной 3 Дб на октаву во всем диапазоне частот.

Способ защиты информации - прием (метод), используемый для организации защиты информации.

Специальное электронное закладное устройство (аппаратная закладка) - электронное устройство, несанкционированно и замаскировано установленное в техническом средстве обработки информации с целью обеспечить в нужный момент времени утечку информации, нарушение ее целостности или блокирование.

Способ защиты информации от технических разведок — преднамеренное воздействие на технический канал утечки информации или на объект защиты для достижения целей защиты от технических разведок. Основными способами защиты информации от технических разведок являются скрытие и дезинформация. Разновидностями дезинформации являются легендирование и имитации.

Технико-экономическое обоснование защиты информации — определение оптимального объема организационных и технических мероприятий в составе системы защиты информации на объекте, необходимого для достижения цели защиты. При проведении исследований по технико-экономическому обоснованию следует исходить из того, что стоимость затрат на создание системы защиты информации на объекте не должна превышать стоимость защищаемой информации. В противном случае защита информации становится нецелесообразной.

Техническая дезинформация — способ защиты информации от технических разведок, предусматривающий введение технической разведки в

заблуждение относительно истинного местоположения (дислокации) объекта защиты и его функционального назначения путем проведения комплекса мер по искажению технических демаскирующих признаков.

Техническая защита информации — защита информации при ее обработке техническими средствами, осуществляемая с использованием технических средств и способов защиты. К техническим средствам и способам защиты информации при ее обработке техническими средствами в общем случае относятся аппаратные, автономные (инженерные) и программные средства, а также криптографические методы.

Техническая разведка — деятельность по получению разведывательной информации с помощью технических средств.

Технический канал утечки информации — совокупность объекта технической разведки, физической среды и средства технической разведки, которыми добываются разведывательные данные.

Технический контроль эффективности защиты информации — контроль эффективности защиты информации с использованием технических средств (инструментальный контроль).

Техническое мероприятие по защите информации — мероприятие по защите информации, предусматривающее применение технических средств и способов защиты и реализацию технических решений.

Техническое решение по защите информации — техническое, планировочное, архитектурное или конструкторское решение по защите информации.

Техническое средство защиты информации — техническое средство, предназначенное для устранения или ослабления демаскирующих признаков объекта, создания ложных (имитирующих) признаков, а также для создания помех техническим средством доступа информации.

Утечка (рассекречивание) информации — утрата информации, при ее обработке техническими средствами, свойства секретности (конфиденциальности) в результате несанкционированного ознакомления с нею или несанкционированного документирования (снятия копий).

Цель защиты информации — заранее намеченный уровень защищенности информации, получаемый в результате реализации системы защиты на объекте.

Эффективность защиты информации — степень соответствия достигнутого уровня защищенности информации поставленной цели.

СПИСОК ЛИТЕРАТУРЫ

1. Основная:

1. Технические методы и средства защиты информации/Ю.Н. Максимов, В.Г. Сонников, В.Г. Петров и др. - СПб.: ООО Изд-во Полигон, 2000. – 320 с.
2. Андрианов В.И., Соколов А.В., Золотарев С.А /Под ред. Золотарева С.А. Устройства для защиты объектов и информации: Справочное пос. - М.: ООО Фирма "Изд-во АСТ"; СПб: ООО Изд-во Полигон, 2000. – 256с.
3. Энциклопедия промышленного шпионажа/Ю.Ф. Каторин, Е.В. Куренков, А.В. Лысов, А.Н. Остапенко/ Под общ. ред. Е.В. Куренкова – СПб: ООО Изд-во Полигон,1999. – 512с.
4. Материалы фирмы МАСКОМ: www.mascom.ru.
5. Алексеенко В. Н., Сокольский Б. Е. Система защиты коммерческих объектов. Технические средства защиты. -М., 1992.
6. Киселев А. Е. и др. Коммерческая безопасность. - М., ИнфоАрт.1993.
7. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Руководящий документ. Гостехкомиссия России. М.: 1995. —36с.
8. Положение о сертификации средств защиты информации. Введено постановлением Правительства РФ №608. М., 1995.
9. Положение по аттестации объектов информатики по требованиям безопасности информации. ГТК. М., 1994.
10. Кутин Г.И., Кузнецов А.С. Охраняемые сведения и демаскирующие признаки при противодействии техническим разведкам.- Л.: МО, 1989. - 55 с.

2. Законы о защите информации:

1. Федеральный закон **«О коммерческой тайне»** (от 9.07.2004) (zip - архив 10 кбайт текст rtf)
2. Федеральный закон **«О Государственной тайне»** (в редакции Федерального закона от 6.10.97 № 131-ФЗ)(zip - архив 21 кбайт текст rtf)
3. Федеральный закон **«О банках и банковской деятельности»** (в ред. - Федеральных законов от 03.02.96 № 17-ФЗ, от 31.07.98 № 151-ФЗ, от 05.07.99 № 126-ФЗ, от 08.07.99 № 136-ФЗ, от 19.06.2001 № 82-ФЗ) (zip - архив 31 кбайт текст rtf)
4. Федеральный закон **«Об информации, информатизации и защите информации»** (Федеральный Закон РФ № 24-ФЗ от 20.02.95 Принят Гос. Думой 25.01.95)(zip - архив 18 кбайт текст rtf)
5. Федеральный закон **«О безопасности»** (№2446-1) (zip - архив 11 кбайт текст rtf)
6. Федеральный закон **«О государственной дактилоскопической регистрации в Российской Федерации»** (в ред. Федерального закона от 09.03.2001 № 25-ФЗ)(zip - архив 7кбайт текст rtf)
7. Федеральный закон **«О техническом регулировании»** (№184-ФЗ от 27.12.2002)(zip - архив 33кбайт текст rtf)

8. Федеральный закон **«Об основах государственной службы Российской Федерации»** (в ред. - Федеральных законов от 18.02.99 № 35-ФЗ, от 07.11.2000 № 135-ФЗ)(zip - архив 19кбайт текст rtf)
9. Федеральный закон **«О связи»** (от 7.07.2003 №126-ФЗ)

3. Сайты:

www.mascom.ru. , http://www.sbchel.ru/price/?id=kpk ,

Устройства защиты офисных технических средств
Скремблеры
Защита телефонных линий
Средства контроля проводных линий
Индикаторы электромагнитного поля
Тестовые приёмники
Детекторы диктофонов
Подавление диктофонов
Индикаторы поля
Многофункциональные поисковые устройства
Средства подавления сотовых телефонов

ПРИЛОЖЕНИЕ

Табл. П1.

Основные характеристики активных радиозакладных устройств

Тип	Частота, МГц вид модуляции	Мощность,мВт, Дальность, м	Тип антенны, Питание, В	Габариты Масса, г	Примеч.
STG 4007	395,41 частотная	15 150	Гибкая	66x27x14 52	Акустомат
РК1380 S	115 – 200 ЧМ 5КГц,	40	Гибкая 9	33x33x20 52	Кварцевая стабилизация частоты, код
SIMHR 9000T	350-450 ЧМ 5МГц,	100	Встроенная 6-10	70x39x5 52	2 канала, код
РК 540SS	427 ЧМ 5КГц	20	Гибкая 9	65x50x30 52	Кварцевая стабилизация частоты, код
РК1195 SS	427 ЧМ 5КГц	1-100		20x55x5 52	Дистанционное. Управление, Акустомат, код

Табл. П2.

Основные характеристики сетевых закладных устройств

Тип	Частота, МГц вид модуляции	Дальность, м, Мощность,мВт	Габариты Масса, г	Примеч.
РК1295S	60-200 Узкополосная ±6 кГц			
Сеть 2НК	100 ЧМ	200	33х33х20	Передача информации по сети
HKG-2221	120-260 ЧМ	100	67х3х25	6 закладок в комплекте
РК 1295SS	200-400 ЧМ	20 100	60х40х16	Скачкообразное изменение частоты,
Сеть 2Ч	ЧМ	200 100		Скачкообразное изменение частоты,

Табл. П3.

Технические характеристики диктофонов

Тип	DT1000	OLIMPUS L400	SONI V-490	VOICE-IT VR500
Акустомат	+	+	+	+
Изменение чувствительности микрофона	+	+	+	-
Ускоренное воспроизведение	+	+	+	+
Источник питания	Адаптер, 9В, 800 мА	1.5 батарея	2AAA	1AAA
Габариты	240х78х170	73х52х20	68х65х19	120х55х24
Дистанционное управление	+	+	+	-
Микрофон, наушники, пауза, реверс, индикатор, счетчик ленты	+	+	+	+

Табл. П4.

Лазерные системы акустической разведки

Тип	Назначение	Тип прибора, Ток, мА/ напряжение	Длина волны, мкм, Мощность мВт	Фокусное расстояние, мм (Расходимость)	Габариты, мм Вес, кг,
STG4510-LASER	Передатчик	Полупроводниковый, 150/12	0.8 – 0.82 5	135	
	Приемник	PIN –диод 30/9	0.8 - 1	500	
ЗК-1035 SS	Передатчик	Полупроводниковый, -/12	0.85 5	(0.5 мрад)	250хØ65 1.5
	Приемник	Диод -/3	0.8 - 1	135	250хØ65 1.5
	Электронный блок	Фильтр, усилитель, магнитофон, -/12			460х 330х120 3.2

Табл. П5.

Телевизионные и видеокамеры для скрытой съемки и наблюдения

Тип	Освещенность минимальная, лк	Разрешение горизонтальное ТВ линий	Размер чувствительного элемента	Параметры	Напряжение, В
JT-241S Тайвань	0.04	400	1/3	D= 0.3 – 1.2 мм F2.8 110 град	12
MYTHOS Республика Корея	0.3.	380	1/3	D= 4мм F1.6	12
ПКС-504С Россия	0.08	380	1/3	F1.4	
ПКС-504Н Россия	0.005	380	1/3	F1.4	