А. В. СОКОЛОВ

ШПИОНСКИЕ ШТУЧКИ НОВОЕ И ЛУЧШЕЕ

Санкт-Петербург
2000

ББК 67.99(2)116.2
С59

Соколов А. В.

С59 Шпионские штучки. Новое и лучшее. — СПб.: ООО «Издательство Полигон», 2000. — 256 с., ил.

ISBN 5-89173-107-X

Помимо всего лучшего, что выходило в популярной серии «Шпионские штучки», книга содержит много нового и оригинального о современной коммерческой разведке и методы защиты информации. Большое внимание уделяется описанию устройств противодействия шпионажу. Издание рассчитано на специалистов, имеющих опыт практической работы, а также может быть использовано как учебное пособие. Несомненно, книга интересна и для людей, впервые столкнувшихся с проблемой сохранения тайны.

ББК 67.99(2)116.2

Андрей Викторович Соколов

ШПИОНСКИЕ ШТУЧКИ. НОВОЕ И ЛУЧШЕЕ

Главный редактор *Н. Л. Волковский.* Редактор *И. В. Петрова.* Корректор *Н. Б. Абалакова.*
Компьютерная верстка *Е. М. Петровой.* Зав. производством *Е. С. Фоменко*

ЛР № 64346 от 09.12.95 г. Подписано в печать 04.08.2000. Формат 70×100 $^{1}/_{16}$. Печать офсетная.
Гарнитура TimeRoman. Печ. физ. л. 16,0. Усл. печ. л. 21,9. Тираж 10 000 экз. Зак. № .

Налоговая льгота — общероссийский классификатор продукции ОК-00-93, том 2;
953 000 — книги, брошюры

ООО «Издательство Полигон», С.-Петербург, Б. Сампсониевский пр., 38/40.
Тел.: 320-74-24; тел./факс: 320-74-23. Для писем: 191119, С.-Петербург, $^{а}/_{я}$ 80
E-mail:polygon@spb.cityline.ru

Отпечатано с готовых диапозитивов в ордена Трудового Красного Знамени ГП «Техническая книга»
Министерства Российской Федерации по делам печати,
радиовещания и средств массовых коммуникаций
198005, Санкт-Петербург, Измайловский пр., 29

ISBN 5-89173-107-X

Оглавление

КЛЕН

ВВЕДЕНИЕ

Каждые десять лет объем информационных ресурсов человечества удваивается, а в дальнейшем эти темпы не только сохранятся, но и, скорее всего, будут возрастать. В связи с этим так же резко возрастает актуальность вопросов, связанных со своевременным получением большого объема информации и ее дальнейшего анализа-обработки для принятия взвешенных решений. Вхождение России в рыночное мировое сообщество сопровождается параллельно идущим процессом вхождения нашей страны в мировое информационное и телекоммуникационное пространство.

Сегодня нас уже трудно удивить переговорами, ведущимися с использованием портативных сотовых телефонов. На очереди — системы телефонии с трансляцией сигналов в любую точку Земли через сеть спутниковой связи. Налицо принципиальная круглосуточная доступность абонента к необходимой информации независимо от его местонахождения. Но ведь первые системы сотовой связи появились в России всего лишь несколько лет назад!

Трудно себе представить и функционирование любых сложных, быстротекущих процессов в современной экономике без использования искусственного интеллекта, основанного на применении современных достижений компьютерных технологий. Принципиально невозможна работа биржевых структур, фондовых рынков, крупных банков без развитой информационной сети, в которую включены филиалы, клиенты, партнеры, информационные центры и другие участники технологического процесса. Вслед за глобальной телекоммуникационной сетью наступает глобальная информационная сеть, ярким демонстрационным примером которой является «всемирная паутинка» — Internet.

Крылатая фраза «владеющий информацией владеет миром» ныне получает почти дословное звучание! Информация в буквальном смысле становится реальной материальной ценностью. Деньги, переводимые через систему электронной почты, технологические «ноу-хау», политические, коммерческие секреты — вся эта информация может быть реализована и преобразована в весьма солидные суммы.

До 1991 г. в России основным держателем информационных ценностей было само государство, но с развитием рыночных отношений все бóльшая часть материальных и информационных ресурсов перераспределяется в сторону коммерческого сектора экономики. Поскольку информация является безусловной ценностью, находятся желающие получить эту ценность даже путем совершения преступления.

Незаконное применение специальной техники в целях получения конфиденциальной информации приняло широкие масштабы. И если для государства потеря нескольких миллиардов — «пустяк», то частный предприниматель в таком случае может справедливо опасаться за само существование своего бизнеса. Ситуации, когда фирмы оказывались под угрозой краха из-за утечки информации по техническим каналам, обычно не афишируются. Однако для собственника информации (частного лица, фирмы, государства) ее потери могут иметь самые плачевные последствия. Так, например, проведенная на показе мод в Париже съемка новых моделей с целью определения реакции публики на «революционное изменение линии талии» привела к тому, что, когда французские модельеры повезли свою продукцию за океан, они увидели там тысячи платьев, сшитых по их новым фасонам. И вместо планировавшихся барышей появились огромные убытки.

Проблема защиты коммерческой тайны приобретает тем большее значение, чем крепче становится на ноги отечественный бизнес. Сегодня настало время обсуждать, какие законные пути могут найти компании, чтобы уберечь от посторонних глаз и ушей то, что для них не предназначается.

Разведке уделяется много внимания, как действенному способу добывания интересующей информации на разных уровнях: от конфиденциальной, коммерческой и до государственной секретной информации. На разведывательные мероприятия разных уровней во всем мире тратится огромное количество материальных, организационных и интеллектуальных затрат. В разведывательных целях используются современнейшие технологии и достижения в электронике и других областях науки и техники.

Разгром Испанской Армады в 1588 г., которому в значительной степени способствовала информация, переданная Великобритании ее секретными агентами, успешные операции союзников, подготовленные напряженной работой Штирлицев, победа Советского Союза в соревновании по скоростному конструированию — все эти вехи славной истории военного шпионажа вполне отвечают утверждению, что «цель оправдывает средства». Однако после окончания холодной войны спрос на оправдания резко упал, и теперь требуется, чтобы цель окупала средства, ибо речь идет уже о промышленном шпионаже, а объектом шпионских посягательств все чаще служат не идеологические противники, а стратегические союзники.

Главной причиной промышленного (экономического) шпионажа является стремление к реализации конкурентного преимущества — важнейшего условия достижения успеха в условиях рыночной экономики. Информация, добытая таким путем, позволяет быть в курсе дел конкурентов, использовать их

научно-технические достижения. На ее основе возможно принятие наиболее рациональных управленческих решений, экономия собственных средств на проведение научно-исследовательских, конструкторских разработок и фундаментальных исследований. Экономический шпионаж может проводиться с целью овладения рынками сбыта, подделки товаров, дискредитации или экономического подавления конкурентов, срыва переговоров по заключению контрактов, шантажа отдельных лиц и т. д.

Всю информацию по степени защищенности можно разделить на секретную, для служебного пользования и несекретную. Любые серьезные мероприятия начинаются со сбора информации для ее дальнейшего анализа и принятия решения. Например, в бизнесе — это анализ рынка, информация о конкурентах, об их сильных и слабых сторонах, информация о новейших разработках в сфере бизнеса и т. п. Таким образом, если вы бизнесмен, то обязательно обладаете информацией, которая необходима вашим конкурентам. Рано или поздно вы столкнетесь с промышленным шпионажем (этим в той или иной степени занимаются все фирмы). Промышленный шпионаж подразумевает сбор открытой и закрытой информации о вас и вашей фирме.

В наше неспокойное время вы можете явиться объектом шантажа, если конкуренты обошли вас по части шпионажа и не уважают закон. Естественно, что шантаж подразумевает наличие компрометирующей информации. Вспомните историю гражданина Корейко А.И., проживавшего в городе Черноморске в 1928 г. («Золотой теленок» Ильфа и Петрова). Вас могут прослушивать просто из любопытства — чужая личная жизнь до сих пор является объектом пристального внимания некоторых людей.

Современный деловой человек не может отмахиваться от проблем доступа к закрытой информации и ее сокрытия. Естественно, не рекомендуется использовать криминальные пути достижения своих целей: заниматься шпионажем для шантажа и вторжения в личную жизнь граждан. Но обязательно необходимо представлять, как это могут сделать другие по отношению к вам.

Основные методы современного промышленного шпионажа также можно разделить на две основные группы: требующую доступа к фирме, намеченной в жертвы, и не требующую такового.

К первой группе относятся следующие методы:

- электронный доступ к секретным данным;
- подслушивание при помощи подсоединения к кабельным сетям;
- установка подслушивающей аппаратуры в офисе;
- перехват переговоров по мобильным телефонам;
- несанкционированный доступ к компьютерным системам посредством проникновения в сеть;
- взлом программного или аппаратного обеспечения;
- физический доступ к секретным материалам;
- применение скрытого визуального наблюдения, фото- или видеосъемки;

- использование личных связей с сотрудниками фирмы;
- хищение информации, содержащейся в документах, чертежах, на дискетах или компакт-дисках;
- использование услуг проституток с целью последующего шантажа сотрудников фирмы;
- метод «подсадной утки» (коммуникабельной женщины или компанейского мужчины, способных установить тесный контакт с сотрудником фирмы с целью выведать у него секретную информацию);
- подкуп служащих фирмы;
- взяточничество;
- компрометация руководящих сотрудников фирмы с целью развала всей системы экономической безопасности конкурирующей фирмы;
- выведывание секретной информации под видом проверки уровня профессионализма сотрудников фирмы (например, при имитации предложения более выгодных условий работы).

Вторая группа методов собственно к технике шпионажа не относится, так как она подразумевает использование только официально доступной информации. Тысячи информационных агентств занимаются отслеживанием, сбором, обработкой и анализом коммерческой, научной и технической информации, и в этом нет ничего противозаконного. Но именно такие обзоры и результаты анализов как раз и служат источником той информации, на основании которой принимаются решения об объектах применения методов первой группы. Как правило, наиболее «передовые», с точки зрения методологии промышленного шпионажа, страны используют все доступные на данный момент методы.

Учитывая известный афоризм «цель оправдывает средства», зададим вопрос: какие цели преследует злоумышленник, осуществляя несанкционированный доступ к источникам конфиденциальной информации? В новых рыночно-конкурентных условиях возникает масса проблем, связанных не только с обеспечением сохранности предпринимательской (коммерческой) информации как вида интеллектуальной собственности, но и физических и юридических лиц, их имущественной собственности и личной безопасности. Известно, что предпринимательская деятельность тесно связана с получением, накоплением, хранением, обработкой и использованием разнообразных информационных потоков. Коль скоро информация представляет определенную цену, то факт получения информации злоумышленником приносит ему определенный доход, ослабляя тем самым возможности конкурента. Отсюда главная цель — получение информации о составе, состоянии и деятельности объекта конфиденциальных интересов (фирмы, изделия, проекта, рецепта, технологии и т. д.) в целях удовлетворения своих информационных потребностей.

Профессионально проведенные мероприятия, преследующие чисто экономические цели (с достаточной долей вероятности), следующие:

- перехват выгодных контрактов;
- получение выгодного инвестирования;
- борьба за рынок;
- разведка рынка в регионе конкурентов;
- смена руководства фирмы;
- срыв контрактов;
- поглощение фирм.

Многие предприниматели превращают свои дома и квартиры в офисы, где проводят деловые встречи, работают с компьютером, факсом, наивно полагая, что их дом — надежная крепость. С помощью современных средств шпионажа, которые приобрести не составляет труда, внедриться в компьютерную базу данных или прослушать незащищенный офис проще, чем вы думаете. Создание и совершенствование современных электронных устройств шпионажа привело к тому, что даже самый совершенный и секретный тайник не в состоянии обезопасить вас от утечки информации, содержащейся в хранимых документах. В настоящем издании мы рассмотрим основные методы съема информации и дадим рекомендации, как с ними бороться.

На российском рынке промышленного шпионажа за последние 10 лет, по принципу — от простого к сложному, можно условно выделить несколько этапов появления и продвижения на рынок специальных технических средств.

Первый этап характеризуется появлением самых простых радиопередатчиков, собранных из подручных компонентов, по схемам, взятым из учебников или радиожурналов. Как правило, это были элементарные схемы на одном транзисторе. Технические характеристики были неудовлетворительны, но именно на данной технике начиналось становление сегодняшнего рынка специальной техники.

Второй этап характерен появлением более серьезной аппаратуры. Доступными стали изделия с кварцевой стабилизацией частоты, изделия, выполненные с применением бескорпусных компонентов, стали использоваться специализированные элементы питания. Появились на рынке и зарубежные образцы специальной техники — своего рода дорогой «ширпотреб», часто не оправдывающий затраченных на его приобретение денег.

Более поздний, «профессиональный» этап обусловлен тем, что после развала СССР, массовых сокращений и ухудшения материального благосостояния большинства населения произошел отток бывших «спецов»-профессионалов из государственных, в том числе и силовых, учреждений в коммерческие и криминальные структуры. Многие стали использовать свои знания и умения для зарабатывания денег как на законной основе, так и в обход, а иногда и в полном противоречии закону. Отсюда появились и развились специализированные фирмы, которые занимаются разработкой, изготовлением и применением специальных технических средств. Отсюда появились и доморощенные кулибины, и бойцы различных группировок.

На этом этапе среди множества радиомикрофонов и телефонных ретрансляторов появляются системы с дистанционным включением, с узкополосной частотной модуляцией. Широко используются другие виды модуляции, скрем-

блирование, сжатие информации и другие способы маскировки радиоканала. Имеют место попытки создания специализированных микросхем, делается ставка на создание автоматизированных программно-аппаратных комплексов сбора, обработки, накопления и передачи полученной информации. Примером этому могут служить комплексы перехвата сообщений, передаваемых по сотовым радиотелефонам и пейджерам. Сегодня существует множество подобных комплексов, и многие из них выполнены на достаточно высоком профессиональном уровне.

На кого работает вся эта техника? В чьих интересах? Если совсем недавно в большинстве случаев ответ был бы однозначный —информационной разведкой занимались в основном криминальные структуры, то сегодня ситуация изменилась очень сильно. И прежде всего в тех секторах рынка, где уже становится «тесновато», где приходится все тщательнее приглядываться к деятельности конкурентов. Это такие отрасли экономики, например, как:

- туристический бизнес;
- шоу-бизнес;
- воздушные перевозки;
- производство продуктов питания;
- бизнес недвижимости;
- крупная оптовая торговля.

В подавляющем большинстве случаев нелегальные получатели информации прибегают к использованию современных методов и технических средств разведки. В сети Internet можно почерпнуть сведения о специальных технических средствах разведки, где приобрести, как изготовить простейшие устройства, получить необходимую информацию о методах ведения разведки с использованием технических средств. Наверное, многим памятен сюжет из фильма «Операция “Ы” и другие приключения Шурика», в котором один горе-студент пытался сдать экзамен с помощью хитрого приспособления, примотанного к уху. Но, как известно, в любой шутке есть доля шутки... Это было только начало!..

При существующем уровне развития техники не составляет особого труда найти и обезвредить «жучка», гораздо сложнее определить, кто, когда, с какой конкретной целью его установил, и принять предусмотренные законом меры к пресечению преступления. К сожалению, такая точка зрения еще не нашла должного отражения в официальных структурах и документах.

ГЛАВА ПЕРВАЯ

ОСНОВНЫЕ СПОСОБЫ ВЕДЕНИЯ ПРОМЫШЛЕННОГО ШПИОНАЖА

В конкурентно-рыночных отношениях возникает масса проблем, связанных с обеспечением сохранности конфиденциальной (коммерческой) информации. Ведь бизнес тесно связан с получением, накоплением, хранением, обработкой и использованием разнообразных массивов информации. И если информация представляет определенную ценность, то факт тайного получения ее конкурентом приносит ему определенный доход, ослабляя тем самым возможности тех, кто противостоит ему на рынке.

Возможно также внесение определенных изменений в состав информации, совершаемое в корыстных целях, например с целью дезинформации. Однако внесение изменений трудно осуществлять, так как для правдоподобия ее надо согласовывать с общим ходом событий по времени, месту, цели и содержанию, что требует глубокого знания обстановки в конкурирующей фирме. Поэтому более распространенной и опасной целью является уничтожение накопленных информационных массивов или программных продуктов в документальной и магнитной форме.

Таким образом, злоумышленник может преследовать три цели:

- получить необходимую информацию в объеме, необходимом для конкурентной борьбы;
- внести изменения в информационные потоки конкурента в соответствии со своими интересами;
- нанести ущерб конкуренту путем уничтожения коммерчески ценной информации.

Полный объем сведений о деятельности конкурента невозможно получить только каким-нибудь одним из возможных способов доступа к информации. Поэтому чем большими разведывательными возможностями обладает злоумышленник, тем больших успехов он может добиться в конкурентной борьбе. И вообще, на успех может рассчитывать только тот, кто быстрее и полнее собирает необходимую информацию (в том числе конфиденциальную), перерабатывает ее и принимает правильные решения.

1.1. Основные носители информации и возможные каналы утечки

Задача первостепенной важности для предпринимателя — надежно перекрыть каналы утечки конфиденциальной информации. Конфиденциальную информацию удается получать из весьма разнообразных источников, бóльшую часть которых неискушенный человек попросту не принимает во внимание. Следует учитывать самые невероятные возможности, какими бы нереалистичными они ни показались, ибо в цепочке прохождения информации иной раз случается найти потрясающе ценный источник.

Главными носителями информации (рис. 1.1) всегда являются:

- открытые источники (печать, телевидение, радио и т. п.);
- люди (руководители, специалисты);
- документы (справки, отчеты, ведомости, договоры и т. п.) и изделия (образцы товаров, продукции);
- средства беспроводной и проводной связи (телефоны, телефаксы, радиостанции, пейджеры, сотовые телефоны и т. п.);
- электронные системы обработки информации (компьютеры, электрические пишущие машинки, принтеры и т. п.);
- разные отслеживаемые факторы (поведение, разговоры, результаты действий).

К открытым источникам информации (обнародованные сведения) относятся публикации в газетах и журналах, радио- и телесюжеты, прочитанные лекции и выступления. Такие источники знакомят с кулуарными материалами, открывают новых носителей информации. Любопытнейшую информацию могут содержать тиражированные тем или иным способом листовки, обращения либо заметки, рекламные плакаты.

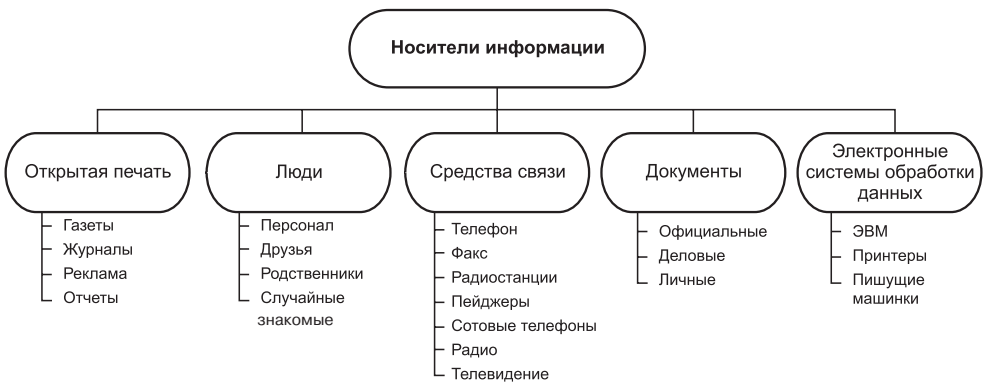


Рис. 1.1. Носители информации

Понятно, что основная работа по получению необходимой информации из этих источников при этом ложится на специально подготовленных аналитиков, которые пропускают через себя горы материалов, отсеивая и накапливая необходимую информацию. Подобным образом работают большинство разведок мира и специальные отделы больших корпораций. Основными направлениями получения открытого доступа к конфиденциальной информации являются:

- сбор информации, содержащейся в средствах массовой информации — книгах, технических и научных изданиях, рекламных материалах, включая официальные документы, например судебные отчеты;
- использование сведений, распространяемых служащими конкурирующих фирм;
- биржевые отчеты и отчеты консультантов, финансовые отчеты и документы, находящиеся в распоряжении маклеров; выставочные экспонаты и проспекты, брошюры конкурирующих фирм; отчеты коммивояжеров своей фирмы;
- изучение продукции конкурирующих фирм, выставочных и промышленных образцов;
- использование данных, полученных во время бесед со служащими конкурирующих фирм (без нарушения законов);
- замаскированные опросы и «выуживание» информации у служащих конкурирующих фирм на научно-технических конгрессах (конференциях, симпозиумах);
- беседы о найме на работу со служащими конкурирующих фирм — заполнение ими анкет и вопросников (хотя опрашивающий вовсе не намерен принимать данного человека на работу в свою фирму);
- так называемые «ложные» переговоры с фирмой-конкурентом относительно приобретения лицензии или продукции;
- наем на работу служащего конкурирующей фирмы для получения требуемой информации, обычно с резким увеличением оклада (своего рода законный подкуп);
- использование информации на основе платежной ведомости фирмы-конкурента;
- подслушивание переговоров, ведущихся в фирмах-конкурентах (без нарушения закона);
- мусор обыкновенный, подлежащий утилизации.

Люди среди источников конфиденциальной информации занимают особое место, ибо способны выступать не только обладателями неких сведений, но и субъектами злонамеренных действий. Действительно, их, в отличие от технического устройства, можно подкупить или шантажировать. Люди являются обладателями и распространителями информации не только в пределах своих функциональных обязанностей, их возможности гораздо шире. Помимо простого обладания набором сведений люди способны их анализировать, обоб-

щать и делать выводы. То есть получать требуемую информацию и 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. Обнаружение последних — очень сложная и трудоемкая задача, требующая специальных навыков.

Образно выражаясь, степень надежности любого шифра определяется не его сложностью, а неподкупностью шифровальщика. Иными словами, ключевыми фигурами систем защиты коммерческих секретов являются сотрудники фирм. Причем не только те, которые работают с закрытой информацией. Рядовой сотрудник, не имеющий доступа к коммерческой тайне, тоже может оказать помощь конкурентам в проведении электронного шпионажа, обеспечить условия для хищения носителей информации, для выведывания, снятия копий.

По мнению зарубежных специалистов, вероятность утечки сведений, составляющих коммерческую тайну, при проведении таких действий, как подкуп, шантаж, переманивание сотрудников фирмы, внедрение своих агентов, составляет 43 %; получение сведений путем их выведывания у сотрудников — 24 %. Таким образом, персонал фирмы является, с одной стороны, важнейшим ресурсом предпринимательской деятельности, а с другой — отдельные сотрудники в силу различных обстоятельств могут стать источником крупных потерь и даже банкротства фирмы. Именно поэтому организационные и административные меры защиты конфиденциальной информации необходимо сочетать с социально-психологическими мерами. Это связано с тем, что человек, имеющий по долгу службы дело с коммерческими тайнами, испытывает постоянное психологическое давление, обусловленное спецификой этой деятельности. Ведь сохранение чего-либо в тайне противоречит потребности человека в общении посредством обмена информацией. А взяв на себя обязательства соблюдать требования режима секретности, сотрудник вынужден действовать в рамках существенного ограничения своей свободы. Кроме того, над ним ежедневно дамокловым мечом висит угроза возможной потери документа (или дискеты), содержащего коммерческую тайну. Психологически слабого человека подобное давление может привести к стрессам, нервным срывам, развитию извращенных наклонностей и другим негативным последствиям.

Итак, какие же качества личности сотрудника не способствуют сохранности доверенных ему секретов, кто из сотрудников в силу этого требует особого внимания и поддержки со стороны руководства? Специальные исследования и практический опыт показывают, что к таким качествам относятся следующие:

- завышенная самооценка своего «я», своих возможностей контролировать людей и ситуации;
- склонность к поиску радости или забвения в алкоголе, наркотиках, острых ощущениях;

- хвастовство, стремление казаться значительнее, чем есть, пускать пыль в глаза;
- острое недовольство служебным или материальным положением;
- разочарованность в своих способностях и возможностях;
- неумение предвидеть последствия своих поступков;
- эмоциональная неустойчивость;
- недисциплинированность;
- низкая самооценка;
- безответственность;
- неаккуратность;
- крайний эгоизм;
- завистливость;
- лживость;
- трусость.

Соответственно, надо стремиться к тому, чтобы у людей, причастных к коммерческим секретам фирмы, указанные качества либо отсутствовали, либо не были развиты слишком сильно. И все же, как уже сказано, главное — не то, каковы люди по своей сути, а чем они воодушевлены.

Немало информации можно почерпнуть и из различных слухов, распространяемых людьми. Как говорят: «Дыма без огня не бывает». Слухи можно определить как официально неподтверждаемые сообщения, циркулирующие по межличностным горизонтальным каналам. Многие из них, как правило, правдоподобны, а нередко и достоверны, причем передают и распространяют их даже те, кто этому ни капельки не верит.

Человек передает подхваченные слухи из-за свойственного всем желания похвастаться, а поэтому перехватить их можно где угодно и от кого угодно. Очень активны в этом отношении все коммуникабельные люди, всегда имеющие самые обширные социальные и деловые контакты, и особенно — женщины.

Любой документ несет в себе информацию, цена которой определяется (рис. 1.2) статусом этого документа.

К официальным документам принадлежат личные дела и медицинские карты, докладные, объяснительные записки и письма в разные инстанции, всевозможные задокументированные данные, собранные официальными (отдел кадров, жилконтора, милиция и т. п.) службами о конкретном лице или организации. Наряду с обзорным представлением здесь можно найти и прочие сведения, полезные при детальной разработке всякого объекта. Информация, получаемая с таких носителей, считается достаточно надежной, хотя не исключена и намеренная фальсификация.

К деловым бумагам и архивам относятся всевозможные договоры, отчеты, факсы, письма, методички, внутренние телефонные справочники, меморандумы и прочие бумаги, связанные с деловой активностью человека или организации. Они представляют первосортный источник конфиденциальной информа-

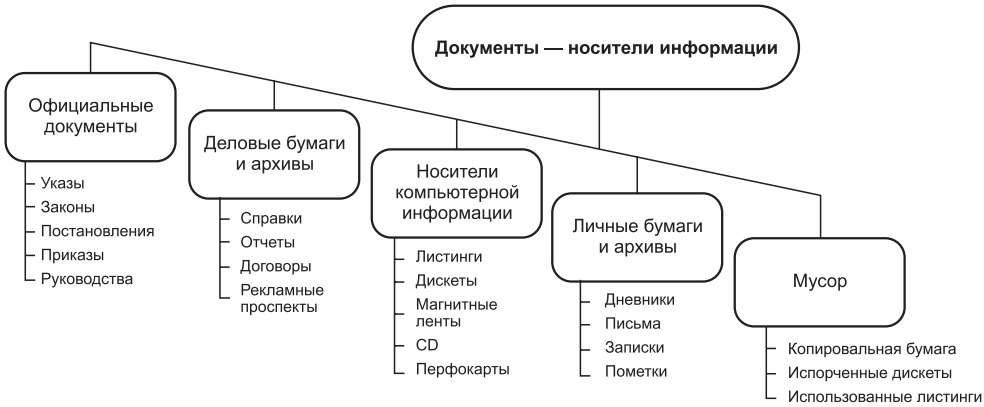


Рис. 1.2. Документы — носители информации

ции, позволяющей ориентироваться в делах объекта, прояснять его намерения и методы работы, прогнозировать поступки и возможности, выявлять функционеров и связи. Достоверность информации при этом преимущественно высшая.

Работа с документами, содержащими важную информацию, должна быть организована так, чтобы исключить ее утечку на всех этапах — от подготовки текстов до учета и хранения поступающих и исходящих телеграмм, писем, образцов и т. п.

Личные бумаги и архивы — это замечательный набор носителей информации, в который входят записные книжки, разные пометки на листках календаря, дружеские и интимные письма, поздравительные открытки, фотографии, аудио- и видеозаписи, дневники и т. д.

Разорванные черновики и машинные распечатки, сигаретные коробки и бумажные обрывки с всевозможными пометками, испорченные копии и случайные подкладочные листки, отработанная копировальная бумага и использованные ленты от пишущих машинок — весь этот мусор в руках умелого специалиста может превратиться в потрясающие документы, причем добывать такие материалы иной раз значительно проще, чем оригиналы.

Так как на подобного рода «мусор» редко обращают пристальное внимание, то и избавляются от него самым обычным способом — просто выбрасывают. Изъятие его обычно не замечается и осуществляется очень просто, причем как из закрытого помещения (визитером, сервисным ремонтником, уборщицей, сотрудником и т. п.), так и вне такового (на мусорной свалке).

Для чтения обнаруженных таким образом материалов применяют нижеследующие приемы:

- восстановление разорванных документов; прием позволяет восстановить разорванные бумажные документы путем тщательной сортировки отдельных обрывков по:

цвету и типу носителя;
окраске и положению штрихов;
способу письма;
линиям разрыва и сгиба;
содержанию текста;

- выявление вдавленных следов на подложках. Если при написании документа или его печати под ним находилась бумажная или иная подложка, например полиэтиленовая папка для бумаг, то на ней всегда остаются вдавленные следы. Разместив такой документ так, чтобы высвечивающий пучок света оказался сбоку, перпендикулярно основным направлениям вдавленных штрихов и под острым углом к фоновой поверхности подложки, можно просто прочитать его, а при необходимости и сфотографировать;
- чтение зачеркнутых и залитых текстов. Если штрихи текста имеют некоторый рельеф, то при боковом освещении с лицевой и оборотной стороны можно восстановить его. При просмотре залитого, например, чернилами листа его осматривают на просвет — обычно краситель штрихов текста резко контрастирует с красителем пятна. То же самое можно сделать, используя светофильтры;
- восстановление текста по копировальной бумаге.

Использованная копировальная бумага, в особенности если она применялась для исполнения лишь одного документа, является идеальным носителем информации. Но даже если копиркой пользовались неоднократно, текст нескольких документов может быть восстановлен.

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

Подробно на этих вопросах мы останавливаться не будем. Скажем только о главном правиле — 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.

Средства проводной и беспроводной связи — великолепный источник и носитель информации. По ним ведутся переговоры с реальными и потенциальными партнерами, властями, деловая переписка, предоставление документации компаньонам и контрольным органам, реклама, общение с представителями прессы, государственных органов, общественных организаций.

Любая фирма, любое предприятие имеет разнообразные технические средства, предназначенные для приема, передачи, обработки и хранения информации. Физические процессы, происходящие в таких устройствах при их функ-

ционировании, создают в окружающем пространстве побочные излучения, которые можно обнаруживать на довольно значительных расстояниях (до нескольких сотен метров) и, следовательно, перехватывать.

Физические явления, лежащие в основе излучений, имеют различный характер, тем не менее утечка информации за счет побочных излучений происходит по своего рода «системе связи», состоящей из передатчика (источника излучений), среды, в которой эти излучения распространяются, и приемника. Такую «систему связи» принято называть техническим каналом утечки информации.

Существует множество технических каналов, по которым происходит утечка информации. Они возникают при появлении различных физических полей, несущих информацию. Несмотря на то что для большинства предпринимательских структур количество вероятных каналов утечки довольно ограничено, ни один из них не стоит сбрасывать со счетов, так как с помощью современных средств получения информации внедриться в компьютерную базу или прослушать незащищенный офис проще, чем кажется на первый взгляд.

Будучи наиболее распространенным инструментом, обеспечивающим человеческое общение, телефон способен легко выдавать секреты своего владельца. Интересно, что при этом можно слушать не одни лишь телефонные переговоры, но и то, что говорят в закрытой комнате при положенной на рычаг трубке.

По каналам таких аппаратов, как телеграф, телетайп, телефакс, циркулирует как графическая, так и знаковая информация, выводимая на бумажные носители, что весьма удобно в деловых взаимоотношениях. Перехват подобных материалов запросто осуществляется подключением к проводным линиям связи, а порой и бесконтактно, опираясь на особенности работы специфической приемо-передающей аппаратуры.

Сотовые и транковые радиосистемы, ситемы персонального радиовызова (пейджеры), предназначенные для разговорного и текстового общения, весьма удобны в обращении, но открыты для обычного эфирного радиоперехвата. К этой же категории носителей информации относятся и персональные радиостанции, применяемые для служебной и гражданской радиосвязи. При неиспользовании объектом мер защиты они позволяют очень легко и незаметно проникать в познания и намерения контролируемого объекта.

Электронные системы обработки информации (компьютеры) представляют собой уникальный электронный механизм для хранения, циркуляции и обработки информации. Более того, компьютеры отдельных структур связаны между собой посредством телефонной сети, что нередко позволяет скачивать с них информацию, даже пребывая в другом городе или стране. В ходе вывода данных на экран дисплея их можно незаметно считывать как бесконтактно (через радиоизлучение), так и контактно (за счет подключения к компьютерной сети или кабелю питания). Достоверность получаемых при этом материалов, разумеется, предельно высокая.

Далее мы более подробно остановимся на технических аспектах получения и защиты информации. Рассмотрим устройства промышленного производства, их принцип действия и характеристики. Остановимся и на рассмотрении принципиальных схем, доступных для повторения.

1.2. Технические каналы утечки информации

Офисы большинства коммерческих фирм занимают одну или несколько комнат в здании, где помимо них размещаются и другие организации. В такой обстановке значительно облегчается доступ злоумышленников к информации, циркулирующей в офисе, так как можно в непосредственной близости или из соседних помещений с большой вероятностью осуществить перехват и запись конфиденциальной информации по техническим каналам утечки. Поэтому ниже описаны ситуации, когда заинтересованные лица (злоумышленники) добывают сведения по техническим каналам, находясь как на самом объекте, так и за его пределами. Вообще говоря, количество моделей подслушивающих и записывающих речь технических устройств, которые имеются на рынке, не поддается никакому учету. С их помощью можно принимать, усиливать, очищать и записывать любые разговоры (в том числе ведущиеся шепотом или под звук льющейся из крана воды) достаточно четко и надежно.

Технические каналы утечки информации делятся на:

- акустические и виброакустические (распространение звуковых колебаний в любом звукопроводящем материале или среде);
- электрические (напряжения и токи в различных токопроводящих коммуникациях);
- радиоканалы (электромагнитные излучения радиодиапазона);
- оптические (электромагнитные излучения в видимой, инфракрасной и ультрафиолетовой частях спектра).

Кроме того, источником излучений в технических каналах утечки информации может быть голос человека. Средой распространения акустических излучений в этом случае является воздух, а при закрытых окнах и дверях — воздух и различные звукопроводящие коммуникации. Если для перехвата используются специальные микрофоны, то образуется акустический канал утечки информации. Обычные микрофоны способны регистрировать человеческую речь на расстоянии, не превышающем нескольких десятков метров. Для увеличения дистанции, на которой можно производить прослушивание, практикуют применение направленного микрофона, который собирает звуки, приходящие только с одного направления, т. е. обладает узкой диаграммой направленности. Такие устройства широко применяются не только в разведке, но и журналистами, охотниками, спасателями и т. д. Можно выделить следующие основные типы направленных микрофонов:

- с параболическим отражателем;
- трубчатый щелевой микрофон;
- резонансный микрофон.

В микрофоне с параболическим отражателем собственно микрофон расположен в фокусе параболического отражателя звука. Направленный параболический микрофон концентрирует приходящие только с одного направления звуки и усиливает их. Обычно в комплект такого устройства входят микрофон, усилитель, кабель и головные телефоны (рис. 1.3). Выпускаются несколько моделей. Общим в конструкции всех этих микрофонов является наличие рукоятки пистолетного типа, параболического отражателя диаметром около 40 см и усилителя низкой (звуковой) частоты. Диапазон воспринимаемых частот составляет 0,1—18 кГц. Все микрофоны имеют автономное питание и разъемы для подключения к магнитофону. Острая диаграмма направленности микрофонов позволяет, при отсутствии помех, контролировать человеческую речь на значительном расстоянии.

Резонансный микрофон основан на использовании явления резонанса в металлических трубках разной длины. Например, в одной из модификаций такого микрофона используется набор из 37 трубок длиной от 1 до 92 см. Звуковые волны, приходящие к приемнику по осевому направлению, приходят к микрофону в одинаковой фазе, а с боковых направлений (по причине отличной скорости распространения звуковых волн в металле, а также разной длины трубок) — оказываются сдвинутыми по фазе.

С точки зрения скрытого контроля звука, применение направленных микрофонов затруднено, как правило, из-за неприемлемых их габаритов и сильных источников акустических помех. Кроме того, для того чтобы не быть прослушанным в автомобиле, достаточно просто поднять стекло.

Слуховой контроль акустики может осуществляться через резонирующие перегородки: стены, стекла, батареи отопления и т. п. (рис. 1.4), а также по прямому каналу утечки — открытые форточки, окна или двери, системы вентиляции, нахождение в непосредственной близости и т. п.

В настоящее время предлагается широкий спектр приборов, позволяющих вести прослушивание таким методом. Один из них — использование электронного стетоскопа, предназначенного для регистрации и идентификации акустических шумов в замкнутых объемах (рис.1.4, *а*). Электронный блок стетоскопа способен обеспечивать прием сигналов от вибродатчика по кабельной линии связи, их усиление, возможность прослушивания с помощью головных телефонов и запись на магнитофон. Вибродатчик спе-

Рис. 1.3. Микрофон с параболическим отражателем

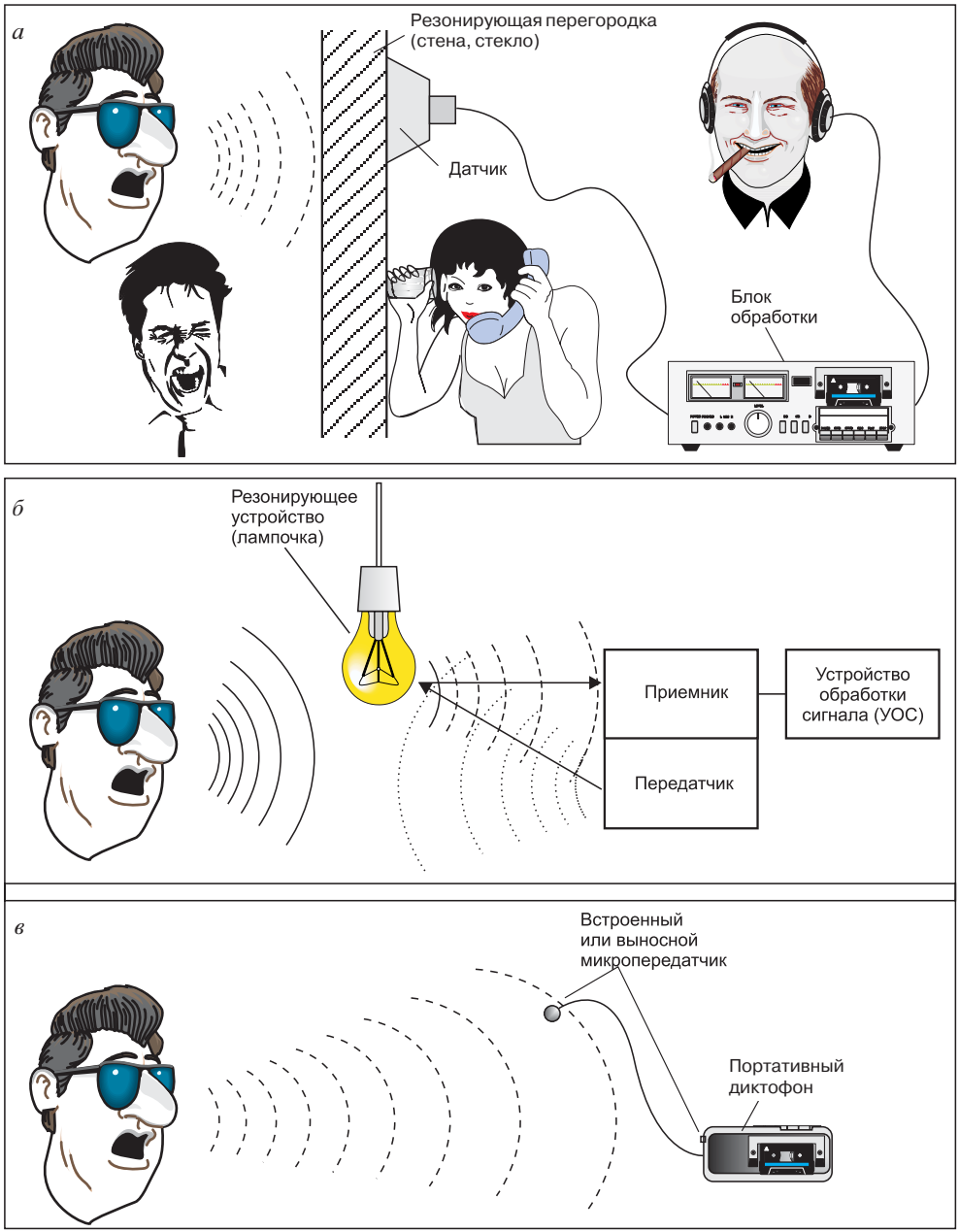


Рис. 1.4. Прослушивание помещений через звукопроводящий материал

циальной мастикой прикрепляется к стене, потолку и т. п. С помощью подобных устройств можно осуществлять прослушивание разговора через стены толщиной до 1 м. Стетоскоп может оснащаться проводом, радио- или другим каналом передачи информации. Основным преимуществом стетоскопа можно считать трудность обнаружения, так как он может устанавливаться в соседних помещениях.

Большинством специалистов прогнозируется постоянный рост случаев применения стетоскопов, что прежде всего объясняется удобством применения подобной техники, а также тем, что их чрезвычайно трудно обнаружить.

Самыми распространенными техническими средствами ведения коммерческой разведки являются радиомикрофоны. Как следует из названия, радиомикрофон — это микрофон, объединенный с радиоканалом передачи звуковой информации.

В самом простом случае радиомикрофон состоит из собственно микрофона, т. е. устройства для преобразования звуковых колебаний в электрические, а также радиопередатчика — устройства, излучающего в пространство электромагнитные колебания высокой частоты (несущую), промодулированные электрическими сигналами с микрофона. Микрофон определяет зону акустической чувствительности (обычно она колеблется от нескольких до 20—30 м), а радиопередатчик — дальность действия всей системы. Определяющими параметрами, с точки зрения дальности действия, для передатчика являются мощность, стабильность несущей частоты, диапазон частот, вид модуляции. Существенное влияние на длину радиоканала оказывает, конечно, и тип радиоприемного устройства. В настоящий момент нет устоявшегося названия этих устройств. Их называют радиозакладками, радиобагами, радиокапсулами, иногда «жуками», но все-таки самым точным названием следует признать название — «радиомикрофон».

Теоретически возможно использование и лазерного детектора, состоящего из передатчика и приемника лазерного луча (рис. 1.4, *б*). Звуковые колебания в помещении приводят к синхронной вибрации стекол, зеркал, картин и т. п., которая и модулирует лазерный луч. Принятый фотоприемником отраженный луч детектируется, звук усиливается и записывается. Приемник и передатчик выполнены раздельно, имеется блок компенсации помех. Вся аппаратура может быть размещена в кейсе и иметь автономное питание. Подобные системы имеют очень высокую стоимость и, кроме того, требуют специального обучения персонала и использования компьютерной обработки речи для увеличения дальности. Первые образцы подобных детекторов были приняты на вооружение американскими спецслужбами еще в 60-е гг. Современные устройства используют лазеры с длиной волны, расположенной в невидимой части светового диапазона. Следует отметить, что эффективность применения такой системы возрастает с уменьшением освещенности оперативного пространства.

Кроме обычного подслушивания очень часто существует реальная угроза несанкционированной записи переговоров непосредственно на диктофон, находящийся в кармане или портфеле собеседника (рис. 1.4, *в*).

Источниками излучений, а следовательно, и каналами утечки информации в технических каналах являются разнообразные технические средства, особенно те, в которых циркулирует конфиденциальная информация. К ним относятся:

- автоматические сети телефонной связи;
- системы факсимильной, телекодовой и телеграфной связи;
- средства громкоговорящей связи и звукоусиления речи;
- средства звуко- и видеозаписи;
- сети электропитания и линии заземления;
- электронно-вычислительная техника и оргтехника.

Для каждого конкретного помещения существует свой набор технических средств, которые могут создавать опасные сигналы и способствовать их распространению, т. е. служить каналами утечки. Эту технику можно разделить на две основные группы — основные и вспомогательные технические средства.

Основные технические средства:

- телефонные аппараты городской АТС;
- телефонные аппараты внутренней связи;
- селекторная связь;
- персональные компьютеры (возможно с модемами), компьютерные сети;
- факс;
- телетайп;
- средства размножения документов.

Вспомогательные технические средства и системы:

- телевизор;
- магнитофон и видеоаппаратура;
- радиоприемник;
- радиотрансляционный громкоговоритель;
- датчики охранной и пожарной сигнализации;
- кондиционер;
- объектовая сеть электрочасофикации;
- табельное электрооборудование помещения.

Пример получения информации через вспомогательные технические средства и системы (радиотрансляционный громкоговоритель и сеть электрочасофикации) представлен на рис. 1.5.

Перечень основных технических средств, приведенный выше, составлен с учетом того факта, что коммерческая информация передается в первую очередь этими средствами, другие защищенные системы передачи и обработки информации используются достаточно редко.

Канал утечки информации за счет побочных электромагнитных излучений и наводок в силу своей стабильности и неявной форме получения информации является одним из основных каналов, по которому технические разведки стараются получить закрытые сведения. Например, работа компьютера сопровождается побочными электромагнитными излучениями, модулированными информативными сигналами. Эти излучения наблюдаются в диапазоне частот от десятков килогерц до сотен мегагерц с уровнями в ближней зоне от 40 до 80 дБ.

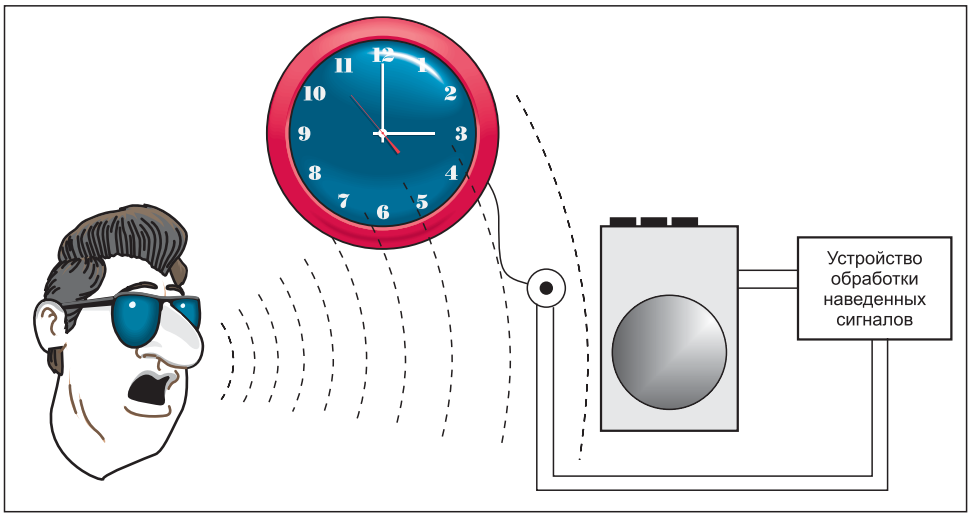


Рис. 1.5. Воздействие электрических, магнитных и акустических полей на вспомогательные технические средства и системы

Существующие методы радиоперехвата позволяют фиксировать циркулирующую в работающих компьютерах информацию на расстоянии до нескольких сотен метров (рис. 1.6). Аналогичный перехват информации может осуществляться через незащищенные цепи питания и заземления, через радиосеть.

Характеристики методов получения информации о различных сторонах деятельности и перечень используемых при этом технических средств приведены в табл. 1.1. Она содержит самые общие данные. Подробно о каждом из

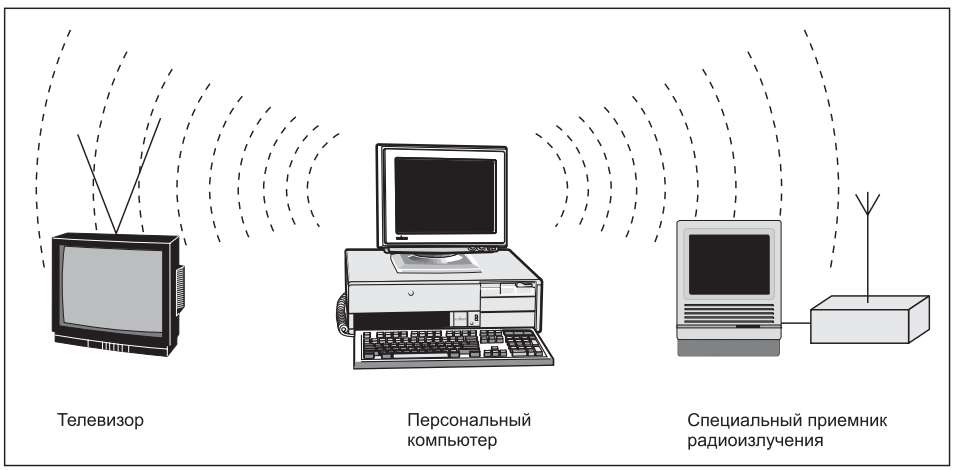


Рис. 1.6. Перехват электромагнитных излучений основных средств

Таблица 1.1. **Характеристики методов получения информации**

П.	Действия	Физическое явление	Способ съема информации
1.	Разговор	Акустический сигнал	Подслушивание, в том числе случайное Диктофоны Микрофоны с передачей информации по: имеющимся коммуникациям, трубам, цепям сигнализации, сетям 220 В; специально проложенным проводам; телефонным линиям; радио- и ИК-каналу Направленный микрофон Полуактивная система
		Виброакустический сигнал	Стетоскоп Вибродатчик с передачей информации по: радиоканалу; проводам; коммуникациям; ИК-каналу Оптический лазерный микрофон
		Гидроакустический сигнал	Гидроакустический датчик
		Акустоэлектрический сигнал	Радиоприемник спецназначения
		Движение губ	Визуально, в том числе оптическими приборами Камера, в том числе с передачей по проводам и радиоканалу
2.	Разговор по телефону	Акустический сигнал	Аналогично п.1
		Электрический сигнал в линии	Параллельный телефон Прямое подключение Подключение через электромагнитный датчик Диктофон Телефонная радиозакладка
		Паразитные электромагнитные сигналы и наводки	Специальные радиотехнические устройства

Окончание табл. 1.1

П.	Действия	Физическое явление	Способ съема информации
3.	Разговор по радиотелефону	Акустический сигнал Электромагнитные волны	Аппаратура п. 1 Радиоприемные устройства (Приказ Минсвязи (1995 г.) о введении в сети сотовых и пейджинговых компаний аппаратуры прослушивания)
4.	Документ на бумажном носителе	Наличие	Визуально, в том числе оптическими средствами Фотографирование, втом числе с дистанционной передачей снимка Копирование
5.	Размножение документа на бумажном носителе	Следы на нижнем листе, копировальной бумаге и на красящей ленте	Кража, визуально
		Шумы принтера	Спецаппаратура акустического контроля
		ПЭМИН от ЭВМ	Специальные радиотехнические устройства
6.	Почтовые отправления	Наличие	Прочтение: с вскрытием; без вскрытия
7.	Документ на небумажном носителе	Носитель	Копирование Вскрытие Несанкционированное использование ЭВМ
8.	Изготовление документа на небумажном носителе	Изображение на дисплее	Визуально, в том числе с помощью оптических средств Фотографирование
		ПЭМИН	Специальные радиотехнические устройства
		Электрические сигналы в сетях	Аппаратные закладки
9.	Передача документа на небумажном носителе	Электрические сигналы	Несанкционированное подключение Имитация пользователя

перечисленных в ней средств можно узнать из материалов этой книги, а также предыдущих книг по этой тематике.

ГЛАВА ВТОРАЯ

ПЕРЕХВАТ ИНФОРМАЦИИ, ЦИРКУЛИРУЮЩЕЙ ПО АКУСТИЧЕСКОМУ КАНАЛУ

С научной точки зрения, источниками акустической информации являются движущиеся тела, перемещающиеся массы жидкости или газа, человеческая речь. Во всех случаях излучение звука является следствием реакции среды на возмущения, вносимые в нее при движении тел или части объема жидкости (газа). Генерирование звука связано также с механическими возмущениями и колебаниями (вибрациями) твердых тел. И наконец, источниками звуковых колебаний являются преобразователи электрических колебаний в акустические и механические (вибрационные). Механические колебания частиц упругой среды в виде акустических колебаний распространяются до границ среды, воздействуя на граничную среду по закону колебаний частиц упругой среды. Колебания упругой среды возбуждают граничащую среду. Акустическая (звуковая) информация — это информация, переносимая упругими колебаниями и волнами в газах, жидкостях и твердых телах в диапазоне от 0,1 Гц до 100 кГц.

Более просто это звучит так. Вокруг нас все время рождаются и затухают колебательные явления. Колеблется ветка, с которой слетела птица. Колеблются маятники часов, качели. Под действием ветра колеблются деревья, провода, подвешенные на столбах, вода в озерах и морях.

Такие и многие другие подобные механические колебания мы можем видеть. В природе же существует больше невидимых колебаний, чем видимых. Некоторые из них мы ощущаем и слышим в виде звука. Не всегда, например, можно заметить колебания струны музыкального инструмента, но это не мешает нам слышать, как она звучит. Мы с вами живем в мире звуков, потому что многие окружающие нас тела, колеблясь, звучат.

Как возникают звуковые колебания в воздухе? Воздух состоит из невидимых глазом частиц. При ветре они могут переноситься на большие расстояния. Но они, кроме того, могут и колебаться, а результатом этого является акустический сигнал (звук). Распространяясь в воздухе со скоростью около 340 м/с, они несут в себе некоторый запас энергии. В тот момент, когда до нашего уха доходит область повышенного давления звуковой волны, она надавливает на барабанную перепонку, несколько прогибая ее внутрь. Когда же

до уха доходит разреженная область звуковой волны, барабанная перепонка выгибается немного наружу. Эти колебания передаются по слуховому нерву в мозг, и человек или животное воспринимает их как звук.

Наше ухо способно реагировать на сравнительно небольшую полосу (участок) частот звуковых колебаний — примерно от 20 Гц до 20 кГц. Колебания частотой до 20 Гц, называемые инфразвуковыми, и выше 20 кГц, называемые ультразвуковыми, мы не слышим (рис. 2.1). Но это не означает, что их не существует.

Акустические (речевые) сигналы генерируются органами человека и относятся к биологическим сигналам. Они воспринимаются органами чувств человека или регистрирующей технической системой. В них заключена содержательная и структурная информация. Реально для получения необходимой информации достаточно отслеживать диапазон частот от 300 Гц до 3—5 кГц.

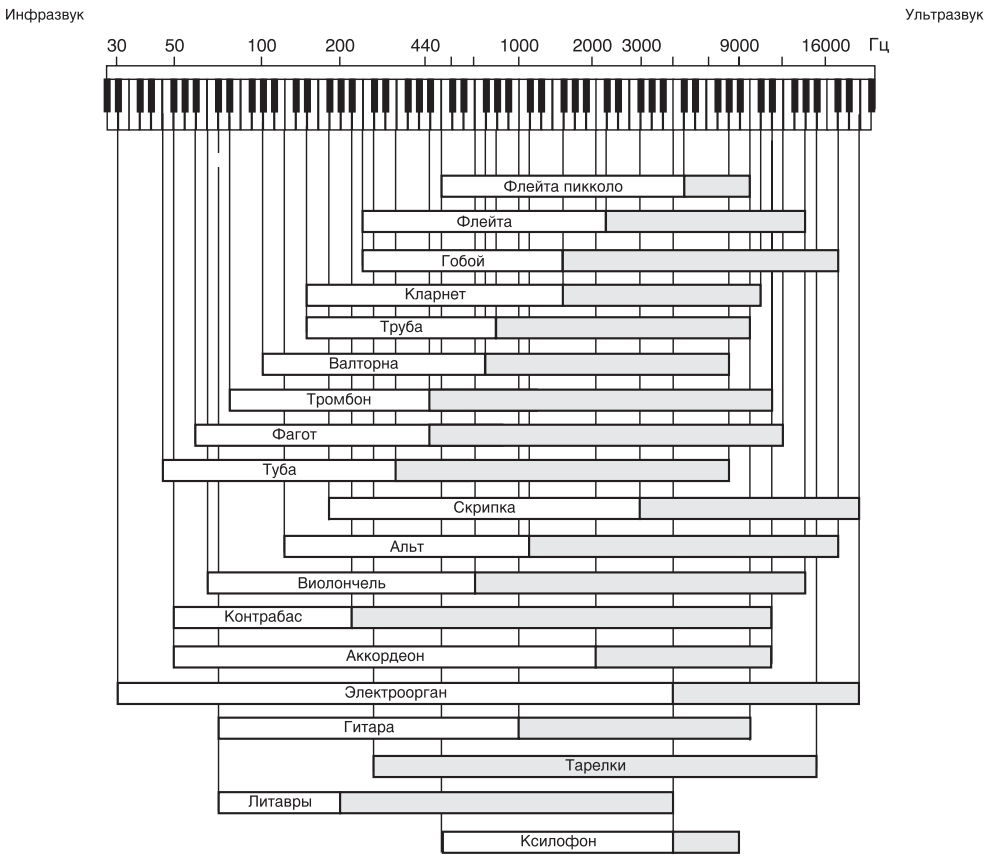


Рис. 2.1. Диапазоны частот звуковых колебаний

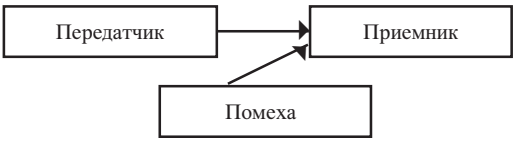


Рис. 2.2. Структурная схема акустической информационной системы

Структурная схема акустической информационной системы представлена на рис. 2.2. Объект, являющийся источником возбуждения и излучения акустических колебаний, создает акустическое поле. На входе акустического приемника присутствуют различного вида акустические помехи, ограничивающие технические возможности приема колебаний объекта исследования. Канал утечки информации в этом случае включает источник акустического излучения, среду распространения, акустический приемник.

Съем акустической информации можно рассматривать как комплекс мероприятий, объединяющий совокупность различных методов и специальных технических средств, обеспечивающих извлечение данных посредством приема (иногда переизлучения и приема) возбужденных объектом упругих волн в воздушной, жидкой и твердой средах. При съеме и обработке акустической информации различают следующие сигналы:

- акустические речевые;
- широкополосные;
- тональные.

Из множества возможных вариантов можно выделить наиболее вероятные каналы утечки речевой информации следующего вида:

- воздушный;
- вибрационный и микросейсмический;
- электроакустический;
- оптоэлектронно-акустический.

Для получения информации по воздушному каналу утечки используются микрофоны, в том числе установленные в портативных диктофонах и радиомикрофонах. Чувствительность микрофонов позволяет прослушивать разговор шепотом на расстоянии до 10 м, нормальным голосом — до 20 м. Кроме того, используются узконаправленные микрофоны, воспринимающие и усиливающие звуки, приходящие только с одного направления и ослабляющие все остальные. Направленность формируется за счет использования длинной трубки, нескольких трубок различной длины или параболического концентратора звука.

Вибрационный канал обусловлен распространением механических колебаний в твердой среде (кирпичные или бетонные стены, потолки, перегородки, батареи отопления и т. п.). При воздействии звуковых волн на земную поверхность они вызывают микросейсмические колебания земной поверхности и образуют микросейсмический канал утечки информации.

Вибрационные и микросейсмические колебания регистрируются с помощью специальных вибро- и сейсмодатчиков. С помощью таких устройств можно

получить акустическую информацию из помещения, находящегося за 30-сантиметровой кирпичной стеной, а некоторые типы тональных сигналов, распространяющихся по техническим коммуникациям, фиксируются даже за пределами здания.

Электроакустический канал обусловлен преобразованием акустических колебаний среды в электрические сигналы и обратным преобразованием электрических сигналов в акустические колебания.

Оптоэлектронно-акустический канал, выражаясь научным языком, обусловлен процессом когерентного облучения точечным источником монохроматического излучения объекта, модуляции, зеркально или диффузно отраженной от объекта. Проще говоря, под действием звуков вибрируют окна, зеркала, корпуса оборудования, и отраженный от них лазерный луч оказывается промодулированным по закону этих звуков. Дальность действия таких систем составляет до 250 м, работают они в ближнем ИК-диапазоне.

2.1. Микрофоны

Общепринятыми и довольно эффективными средствами получения акустической информации в закрытом помещении являются микрофоны. Микрофоны (от греч. *mikros* — малый и *phone* — звук), как известно, преобразуют звук в электрический сигнал. В совокупности со специальными усилителями и фильтрами они могут использоваться в качестве подслушивающих устройств. Для этого создается скрытая проводная линия связи, обнаружить которую можно лишь физическим поиском либо, что сложнее, путем контрольных измерений сигналов во всех проводах, имеющихся в помещении. Методы радиоконтроля, эффективные для поиска радиомикрофонов, о чем будет сказано ниже, в этом случае бессмысленны.

В зависимости от принципа действия все микрофоны делятся на следующие типы:

- порошковые угольные;
- электростатические (конденсаторные и электретные);
- пьезоэлектрические;
- электродинамические;
- электромагнитные;
- полупроводниковые.

Кратко рассмотрим историю их создания и принцип действия.

Порошковый угольный микрофон был сконструирован независимо друг от друга русскими изобретателями М. Махальским в 1878 г. и П. Голубицким в 1883 г. Принцип действия этого микрофона основан на том, что угольная или металлическая мембрана под действием звуковых волн колеблется, изменяя плотность и, следовательно, электрическое сопротивление угольного порош-

ка, находящегося в капсюле и прилегающего к мембране. В результате сила тока, протекающего через микрофон, изменяется, повторяя звуковой сигнал. Эти микрофоны имеют большую неравномерность амплитудно-частотной характеристики (АХЧ) и низкую чувствительность, поэтому они практически не используются в интересах съема информации.

В конденсаторном микрофоне, изобретенном американским ученым Э. Венте в 1917 г., звуковые волны воздействуют на тонкую металлическую мембрану, изменяя расстояние и, следовательно, электрическую емкость между ней и неподвижным металлическим корпусом, которые в совокупности представляют собой не что иное, как пластины электрического конденсатора. При подведении к пластинам постоянного напряжения изменение емкости вызывает появление тока через конденсатор, сила которого изменяется в такт со звуковыми колебаниями.

В пьезоэлектрическом микрофоне, сконструированном советскими учеными С. Ржевкиным и А. Яковлевым в 1925 г., звуковые колебания воздействуют на пластинку, которая изготовлена из вещества (например, из сегнетовой соли), обладающего пьезоэлектрическими свойствами. Это воздействие приводит к появлению на пластинке электрических зарядов.

Электретный микрофон был изобретен в начале 20-х гг. XX в. японским ученым Егути. По принципу действия и конструкции он схож с конденсаторным микрофоном. Разница лишь в том, что роль неподвижной обкладки конденсатора и источника постоянного напряжения в нем играет пластина из электрета. Существенным недостатком такого микрофона является высокое выходное сопротивление, которое приводит к большим потерям сигнала. На практике для снижения выходного сопротивления микрофона до величины не более 3—4 кОм в него встраивают истоковый повторитель.

Электродинамический микрофон катушечного типа изобрели американские ученые Э. Венте и А. Терас в 1931 г., в нем в качестве диафрагмы используется полистирольная пленка или алюминиевая фольга. Катушка, сделанная из тонкой проволоки, жестко связана с диафрагмой и постоянно находится в кольцевом зазоре магнитной системы. При колебаниях диафрагмы под действием звуковых волн витки катушки пересекают магнитные силовые линии и в обмотке наводится электродвижущая сила (ЭДС), создающая переменное напряжение на выходе микрофона.

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 на такую систему акустических волн на выводах обмотки появляется ЭДС. Эти микрофоны имеют большую неравномерность АЧХ.

Обобщенные характеристики перечисленных микрофонов приведены в табл. 2.1.

Чаще всего применяются микрофоны электретного типа, так как они имеют наилучшие электроакустические характеристики:широкий частотный диа-

Таблица 2.1. **Основные характеристики микрофонов**

Тип микрофона	Диапазон частотной характеристики, кГц	Неравномерность воспроизводимых частот, дБ	Осевая чувствительность на частоте 1 кГц, мВм²/н
Порошковые угольные	0,3—3,4	20	1000
Электродинамические	0,03—15	12	1
Конденсаторные	0,03—15	5	5
Электретные	0,02—18	2	1
Пьезоэлектрические	0,1—5	15	50
Электромагнитные	0,3—5	20	5

пазон; малую неравномерность АХЧ; низкий уровень искажений, вызванных нелинейными и переходными процессами, а также высокую чувствительность и малый уровень собственных шумов.

Встроенные микрофоны

Эти микрофоны маскируются в самых неожиданных местах контролируемого пространства и соединяются тончайшими проводниками с создаваемым неподалеку пунктом прослушивания. Отличными микрофонами могут служить ДСП-плиты столов, шкафов и книжных полок с жестко приклеенными к ним пьезокристаллами. Тоненькие провода протягиваются под обоями либо в плинтусах и обычно покидают комнату вместе с телефонной или радиотрансляционной линией. Явным недостатком тут является необходимость предварительного проникновения в намечаемое помещение при довольно долгом, вплоть до нескольких часов, пребывании там, хотя иной раз подобное мероприятие удается обеспечить под прикрытием жилищного ремонта.

Эти подсоединяемые к усилителю микрофоны могут иметь самую разнообразную конструкцию, соответствующую «акустическим щелям», обнаруженным в интересующем помещении. Тяжелый динамический капсюль, например, можно опустить в вентиляционную трубу с крыши, а плоский кристаллический микрофон — подвести под дверь снизу. Подобной лазейкой могут быть и электрические розетки, которые в смежных комнатах часто бывают спаренными. Через защитную коробку с одной из них открывается доступ к другой, а через нее — и в близлежащее соседнее помещение. Иногда в неприметном для глаз месте (где-нибудь в углу либо на уровне плинтусов) сверлят в стене отверстие диаметром 1,5—3 мм или пользуются замочной скважиной для подведения микрофонов. Для таких изощренных вариантов существует

Рис. 2.3. «Игольчатый»

специфичный тонкотрубковый, или «игольчатый», микрофон, звук к которому подводится через довольно тонкую трубку (рис. 2.3) длиной до 30 см.

Ниже приведены принципиальные схемы и описания конкретных изделий, которые могут быть использованы в качестве встроенных микрофонов или устройств акустического контроля.

Чувствительный микрофон с усилителем на малошумящих транзисторах

Конструирование чувствительных усилителей для прослушивания речи имеет свои особенности. Одна из практических схем микрофонного усилителя приведена на рис. 2.4. Это устройство содержит двухкаскадный усилитель низкой частоты на малошумящих транзисторах *VT1* и *VT2*, корректирующий фильтр на транзисторе *VT3* и оконечный усилитель, собранный по двухтактной бестрансформаторной схеме, на транзисторах *VT4—VT6*. Акустическое усиление сигнала звуковой частоты приведенным устройством составляет 85 дБ, начальный ток потребления — 1,8 мА, полоса усиливаемых частот — от 0,3 до 3 кГц, максимальный выходной уровень сигнала — 124 дБ.

Сигнал с микрофона *M1* типа «Сосна» через конденсатор *C1* поступает на базу транзистора *VT1*. Поскольку чувствительность усилителя звуковой частоты ограничена внутренними шумами транзисторов, то для уменьшения шу-

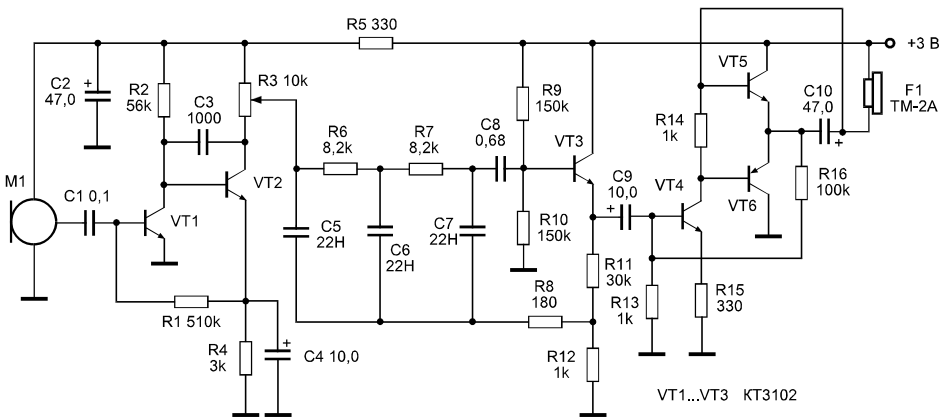


Рис. 2.4. Схема чувствительного микрофона с усилителем

мов в первых каскадах усилителя использованы малошумяще транзисторы типа КТ3102.

Усилительные каскады на транзисторах *VT1* и *VT2* охвачены глубокой отрицательной обратной связью, которая позволяет обеспечить устойчивую работу каскадов и более линейную АЧХ. Нагрузкой второго каскада усилителя является переменный резистор *R3*, он же является и регулятором громкости. Сложный RC-фильтр, состоящий из элементов *R3, C5, R6, C6, R7, C7*, отсекает «шумовые» ВЧ-составляющие, принимаемые микрофоном, и оставляет только сигналы в полосе частот до 4 кГц. Этот диапазон обеспечивает наибольшую разборчивость речевой информации.

С выхода фильтра сигнал поступает на оконечный усилитель звуковой частоты (УЗУ), выполненный на транзисторах *VT4, VT5* типа КТ315 и транзисторе *VT6* типа КТ361. Нагрузкой усилителя служит головной телефон типа ТМ-2А или ТЭМ. Резисторы в схеме используются типа МЛТ-0,125. Резистор *R3* — СП3-41 или другой небольших габаритов.

Настройка устройства сводится к подбору сопротивлений резисторов *R1* и *R16*, соответственно, и установке напряжения в точках *A* и *B*, равного половине напряжения питания.

Микрофон на специализированной микросхеме

В отличие от предыдущего устройства, собранного на дискретных элементах, предлагаемое устройство собрано на широко распространенной микросхеме типа К237УН1 и предназначено для обнаружения слабых акустических сигналов. Принципиальная схема устройства приведена на рис. 2.5. В схеме использован электретный микрофон типа МКЭ-333. Сигнал с микрофона *M1* поступает на вход микросхемы *DA1* типа К237УН1, которая представляет собой усилитель низкой частоты. Усилитель включен по типовой схеме. Транзисторы *VT1* типа КТ315 и *VT2* типа КТ361 включены по схеме эмиттерных повторителей и служат для усиления сигнала по току. В качестве нагрузки используется телефон типа ТМ-2А.

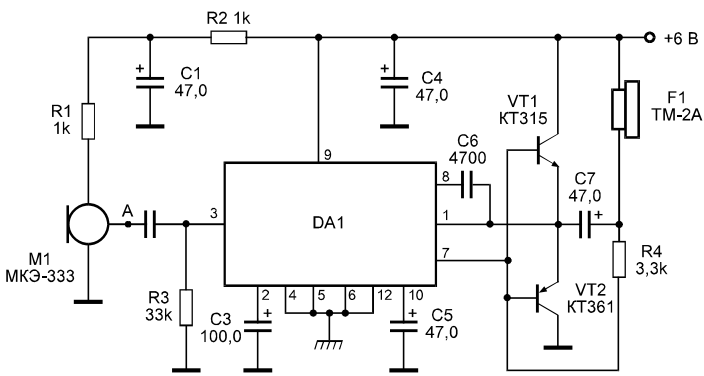


Рис. 2.5. Принципиальная схема микрофона на специализированной микросхеме

Настройка УЗЧ заключается в получении максимальной мощности сигнала на выходе микросхемы *DA1* путем изменения сопротивления резистора *R3*. Сопротивление резистора *R3* подбирают таким, чтобы при номинальном напряжении питания 9 В и отсутствии сигнала звуковой частоты на входе микросхемы *DA1* потенциал на выводе *1* микросхемы *DA1* находился в пределах 3,75—3,85 В.

В случае неустойчивой работы усилителя, его самовозбуждения, необходимо между выходом микрофона *M1* и конденсатором *C2* включить резистор сопротивлением 2—68 кОм.

Устройство работоспособно в диапазоне питающих напряжений 3—9 В, потребляемый при этом ток составляет 2—6 мА.

Вместо микрофона возможно подключение многовитковой катушки индуктивности. Она подключается между точками *A* и *B*. Микрофон *M1* и резистор *R1* при этом отключаются. В последнем случае возможна регистрация переменных магнитных полей.

Выносной микрофон с питанием от линии связи

Дистанционная передача информации возможна при использовании проводных линий связи, которые соединяют выносной чувствительный микрофон и оконечный усилитель. Поскольку выходной сигнал, снимаемый непосредственно с микрофона, имеет небольшую амплитуду, то передавать его по линии связи просто нецелесообразно. Это связано с тем, что на длинных соединительных проводах наводятся разного рода помехи, имеющие значительную амплитуду. Чтобы передавать сигнал по этим проводам, последний необходимо усилить до некоторой величины. Для усиления сигнала используется чувствительный микрофонный усилитель, расположенный в непосредственной близости с микрофоном. Питание такого усилителя осуществляется по проводам линии связи.

Ниже приведена схема выносного микрофона с питанием от линии связи, рис. 2.6. В устройстве используется динамический или электромагнитный микрофон. Коэффициент усиления по напряжению усилителя, собранного по схеме, составляет около 3500. Передача сигнала может осуществляться на десятки и сотни метров.

Сигнал с микрофона *M1* поступает на усилитель, собранный на транзисторах *VT1, VT2* и *VT3*. Между выходом и входом усилителя введена отрицатель-

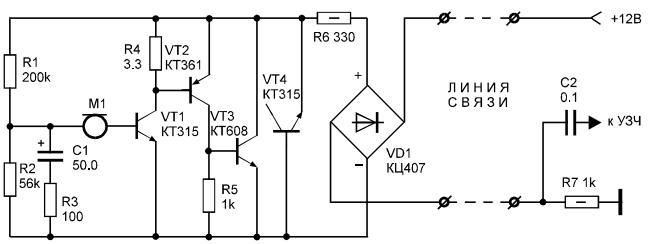


Рис. 2.6. Принципиальная схема выносного микрофона с питанием от линии связи

ная обратная связь по напряжению, образованная резисторами *R1, R2, R3* и конденсатором *C1.* При этом начальный ток, протекающий через усилитель по цепи, постоянен и зависит от напряжения источника питания и сопротивления нагрузочного резистора *R7*. Сигнал, усиленный усилителем, вызывает изменение выходного тока усилителя, что приводит к изменению напряжения на нагрузке. Это напряжение поступает на УЗЧ через конденсатор *C2.* УЗЧ может быть использован любой. Резистор *R6* нужен для согласования внутреннего сопротивления микрофонного усилителя с сопротивлением линии связи. Выпрямительный мост *VD1* типа КЦ407 необходим для предотвращения выхода устройства из строя вследствие ошибочного подключения источника питания. Транзистор *VT4*, включенный по схеме «аналога» стабилитрона, предотвращает скачки напряжения на усилителе в момент подключения питания. Кроме того, он позволяет получить симметричное ограничение выходного сигнала при перегрузках усилителя, что исключает появление четных гармоник, особенно неприятных для слухового восприятия.

В устройстве используются резисторы типа МЛТ-0,125 (кроме *R6* и *R7*). Транзисторы *VT1, VT4* могут быть типов КТ315, КТ312, КТ201, КТ342, КТ3102. Транзистор *VT2* — КТ361, КТ345, КТ3107. Транзистор *VT3* — КТ608, КТ603, КТ630, КТ626, КТ940. Диодный мост *VD1* можно заменить четырьмя диодами типов КД102, КД103.

Настройка сводится к установке необходимого коэффициента усиления путем подбора сопротивления резистора *R3.* При изменении сопротивления резистора *R3* от 0 до 20 кОм можно получить коэффициент усиления от 3500 до 10.

Питание усилителя осуществляется от источника постоянного тока напряжением от 12 до 60 В. Ток, протекающий через устройство, не должен выходить за пределы 0,5—60 мА. Его значение устанавливается подбором сопротивления *R7.*

Если сопротивление обмотки электромагнитного или динамического микрофона *M1* по постоянному току менее 600 Ом, то его желательно включить в цепь эмиттера транзистора *VT1*. В качестве линии связи используется экранированный или обычный провод. В последнем случае провода желательно свить между собой.

Малогабаритный выносной микрофон с низким питающим напряжением

Схема, приведенная на рис. 2.7, в отличие от выше описанной, работает при более низком питающем напряжении. Выносная часть устройства имеет малые размеры. Длина соединительного кабеля составляет 15—30 м.

Устройство разделено на две части. Одна из них собрана на транзисторе *VT1* типа КТ315 по схеме с общим коллектором, а вторая — на транзисторе *VT2* по схеме с общим эмиттером. Сигнал, снимаемый с электретного микрофона с усилителем типа МКЭ-3, поступает на базу транзистора *VT1*. Нагрузкой этого каскада служит резистор *R3*, расположенный во второй части уст-

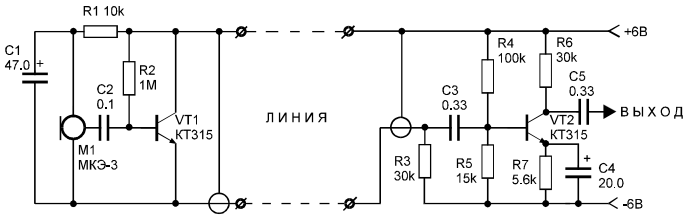


Рис. 2.7. Принципиальная схема малогабаритного выносного микрофона с низким питающим напряжением

ройства. Это сопротивление необходимо для обеспечения питания входного каскада на транзисторе *VT1* при минимальном количестве соединительных проводов. Сигнал, снимаемый с резистора *R3*, через конденсатор *C3* поступает на УЗЧ, собранный на транзисторе *VT2* типа КТ315.

Обе части устройства соединены экранированным проводом. Причем отрицательное напряжение источника питания и сигнал звуковой частоты поступают по центральной жиле провода, а положительное напряжение — по оплетке.

В качестве микрофона *M1* можно использовать любой электретный микрофон с усилителем. Транзистор *VT1* типа КТ315 лучше заменить малошумящим транзистором КТ3102. Резисторы в схеме должны быть типа МЛТ-0,125. В качестве источника питания используется аккумуляторная батарея на напряжение 6—9 В.

Настройка устройства заключается в установке режимов работы транзисторов *VT1*, *VT2* путем подбора сопротивлений резисторов *R2* и *R4* соответственно. При этом ток коллектора каждого транзистора должен быть 0,1—0,2 мА.

Выносной микрофон с усилителем, обеспечивающим дальность передачи сигнала до 100 м

Это устройство является улучшенным вариантом предыдущего. Оно позволяет передавать сигнал на расстояние до 100 м. Изменения в предлагаемой схеме касаются микрофонного блока. Схема устройства приведена на рис. 2.8.

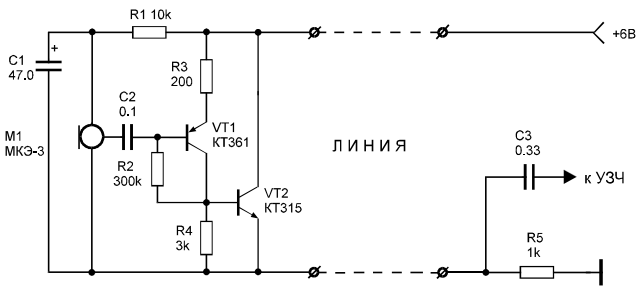


Рис. 2.8. Принципиальная схема выносного микрофона с усилителем, обеспечивающим дальность передачи сигнала до 100 м

Транзистор *VT1* типа КТ361, на базу которого через конденсатор *C2* поступает сигнал с микрофона *M1*, вместе с резисторами *R2—R4* образует однокаскадный микрофонный усилитель. Транзистор *VT2* типа КТ315 является эмиттерным повторителем и выполняет функцию динамической нагрузки первого каскада. Ток, потребляемый микрофонным усилителем, не превышает 0,4—0,5 мА, так что его можно питать от источника питания УЗЧ. Усилитель работоспособен в интервале питающих напряжений 3—9 В.

Резисторы для устройства применяются типа МЛТ-0,125. Микрофон *M1* — любой электретный микрофон со встроенным усилителем. Вместо транзисторов *VT1* и *VT2* можно использовать транзисторы типа КТ3107 и КТ3102 соответственно.

Настройка УЗЧ состоит в установке путем подбора сопротивления резистора *R3* возможно большего напряжения выходного сигнала.

Соединение микрофонного блока с основным выполняется экранированным проводом, но возможно использование и обычного провода или провода типа «лапша». При использовании длинного соединительного кабеля наблюдается ухудшение качества воспроизведения сигнала из-за больших наводок на проводах.

Выносной микрофон с питанием от трехпроводной симметричной линии связи

Как уже говорилось ранее, кабели, связывающие микрофон с основным УЗЧ, очень часто становятся источником дополнительных шумов. Снижение уровня полезного сигнала, как правило, происходит на соединительном кабеле большой длины, которое можно компенсировать УЗЧ, но при этом одновременно будут усилены и шумы.

Нижеприведенная схема устройства с передачей сигнала по симметричной линии отличается от ранее рассмотренных. В этом случае шумы на уровне усиленного сигнала маскируются в большей степени.

Принципиальная схема микрофонного усилителя дана на рис. 2.9.

Сигнал, снимаемый с микрофона *M1* типа МКЭ-3 «Сосна», поступает на усилитель, собранный на транзисторе *VT1*. Коэффициент передачи каскада,

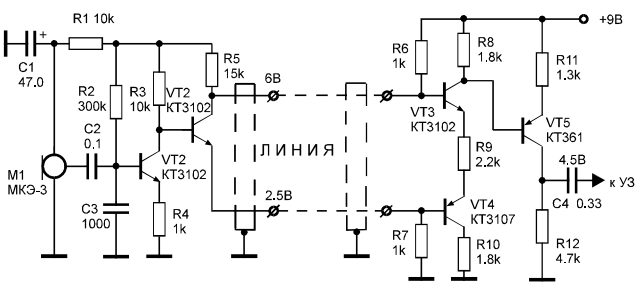


Рис. 2.9. Принципиальная схема выносного микрофона с питанием от трехпроводной симметричной линии связи

выполненного на транзисторе *VT1*, приблизительно определяется соотношением сопротивлений резисторов *R3* и *R4*. Сигнал, усиленный транзистором *VT1*, поступает на базу транзистора *VT2*. А так как фаза сигнала на коллекторе транзистора *VT2* противоположна фазе сигнала на эмиттере, то и сигнал, поступающий в линию, тоже противофазный.

Входной каскад правой части схемы, собранный на транзисторах VT3, *VT4*, представляет собой сумматор со сдвигом фазы на 180°. Таким образом, противофазный полезный сигнал складывается в фазе и на выходе образуется полезный сигнал с удвоенной амплитудой. А возникающие одинаковые по фазе шумы и помехи в каждом из проводов линии взаимно уничтожаются в сумматоре. Суммарный сигнал подается на базу транзистора *VT5* типа КТ361. Этот каскад имеет коэффициент усиления 4. С нагрузки этого каскада, резистора *R12*, сигнал подается на оконечный УЗЧ или магнитофон.

В устройстве используются резисторы типов МЛТ-0,125. Транзисторы *VT1—VT3* могут быть типов КТ315 и КТ342, транзисторы *VT4*, *VT5* — КТ361, КТ3107. В качестве микрофона *M1* может быть использован любой электретный микрофон со встроенным усилителем.

Настройка усилителя заключается в подборе сопротивления резистора *R7*. При этом необходимо контролировать напряжения, указанные на принципиальной схеме.

Для подключения выносного микрофона необходим экранированный кабель с двумя внутренними жилами.

Микрофонный усилитель с дифференциальным входом

Такой недостаток, как питание выносного микрофона по трем проводам, можно устранить. Принципиальная схема устройства с двухпроводной соединительной линией, имеющая лучшие выходные характеристики, чем выше описанная, приведена на рис. 2.10. В качестве предварительного усилителя используется дифференциальный операционный усилитель.

Работа выносного микрофона (левая часть схемы) подробно изложена при описании работы схемы, представленной на рис. 2.8. Остановимся на подроб-

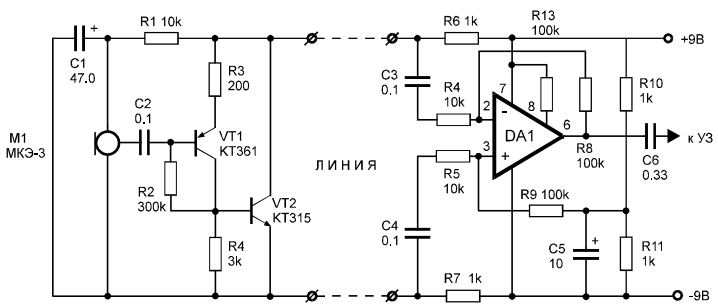


Рис. 2.10. Принципиальная схема микрофонного усилителя с дифференциальным входом

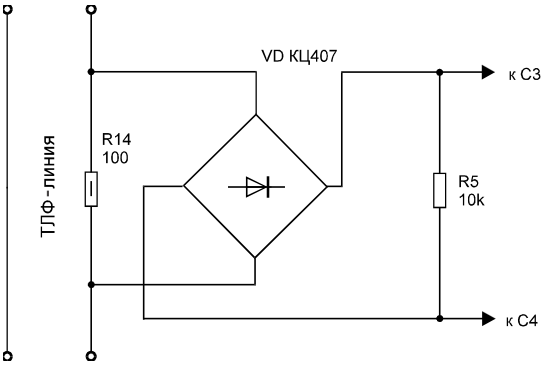


Рис. 2.11. Принципиальная схема специализированного аналога микрофона

ном описании правой части схемы, основу которой составляет операционный усилитель *DA1* типа КР1407УД2, включенный по схеме дифференциального усилителя. Он представляет собой малошумящий операционный усилитель с малым током потребления. Схема имеет коэффициент ослабления синфазных входных напряжений около 100 дБ. Это свойство и используется для подавления помех, наводимых в проводах и имеющих синфазный характер. Полезный сигнал и помеха снимаются с нагрузочных резисторов *R6* и *R7* и через конденсаторы *C3* и *C4* поступают на инвертирующий и неинвертирующий входы микросхемы *DA1* соответственно. Вследствие этого сигнал помехи ослабляется в микросхеме на 100 дБ. Полезный звуковой сигнал усиливается операционным усилителем в 10 раз. Коэффициент усиления сигнала можно изменять путем изменения сопротивления резисторов *R8* и *R9*. Увеличение их номиналов приводит к увеличению коэффициента усиления, определяемого как отношение *R3*/*R4* (*R9*/*R5*). Сигнал, усиленный микросхемой, с выхода *6* через конденсатор *C6* поступает на основной УЗЧ или магнитофон.

Резисторы *R10*, *R11* и конденсатор *C5* создают искусственную среднюю точку, в которой напряжение равно половине напряжения источника питания. Это обусловлено тем, что для питания устройства используется однополярное питание, а для нормальной работы операционного усилителя необходимо двухполярное. Резистор *R13* устанавливает необходимый ток потребления микросхемы.

Микросхему *DA1* можно заменить на операционный усилитель типа КР140УД1208. Но возможно и применение любого другого операционного усилителя, включенного по типовой схеме со своими цепями коррекции. Резистор *R13* в этом случае из схемы исключается.

При исправных деталях устройство начинает работать без дополнительных регулировок. Увеличить (уменьшить) усиление можно подбором сопротивлений *R8* и *R9*.

Если левую часть схемы заменить схемой, приведенной на рис. 2.11, а из правой части убрать резисторы *R6* и *R7*, то можно записывать на магнитофон телефонный разговор при снятой телефонной трубке.

Контактные микрофоны (стетоскопы)

Наряду с узконаправленными и проводными выносными микрофонами существуют устройства, которые регистрируют вибрационные колебания стен, потолков, стекол, вентиляционных шахт и т. д. Эти устройства называются микрофоны-стетоскопы. Они представляют собой довольно сложные изделия. Поэтому ниже описано устройство и принцип его работы, которое может служить прообразом микрофона-стетоскопа. Принципиальная схема устройства приводится на рис. 2.12.

УЗЧ собран на микросхеме *DA1* типа К140УД6. Резисторы *R1* и *R2* задают режим работы микросхемы. Коэффициент усиления определяется значением сопротивления резистора *R3*. Транзисторы *VT1* типа КТ315 и *VT2* типа КТ361 включены по схеме эмиттерных повторителей и усиливают выходной сигнал по току. Нагрузкой усилителя служат головные телефоны ТЭМ-2.

Датчик вибрации делается из пьезокерамической головки *B1*, снятой со старого проигрывателя. Виброколебания преобразуются пьезодатчиком в электрические и усиливаются усилителем *DA1*. В качестве пьезодатчика *B2* можно применить пьезоизлучатель типов ЗП-1, ЗП-22 и им подобные от электронных часов и игрушек. Они хорошо воспроизводят частоты в диапазоне 800—3000 Гц, что в основном перекрывает речевой диапазон частот.

При необходимости можно дополнительно усилить сигнал до нужной величины, используя дополнительный УЗЧ. Сигнал на него поступает с выхода операционного усилителя DA1. Подобный датчик может быть с успехом использован как датчик охранной сигнализации. В качестве пьезодатчика B1 можно использовать, например, ПЭ-1, ГЗП-308 и др.

Очень чувствительные контактные микрофоны получаются из пьезокерамических головок от проигрывателей или из стандартных пьезоизлучателей электрических часов, звуковых игрушек, сувениров и телефонов. Так как данные устройства фиксируют микроколебания контактных перегородок, требуется весьма тщательно выбирать место их приложения, зависящее от конструктивных осо-

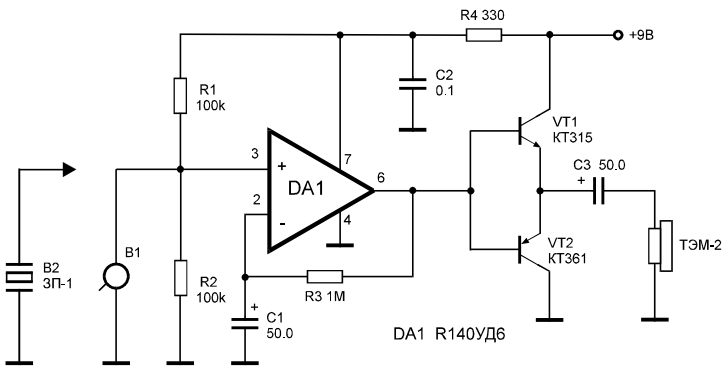


Рис. 2.12. Принципиальная схема микрофона-стетоскопа

бенностей конкретной стены (сплошная, пустотелая). В некоторых случаях имеет смысл накрепко приклеить пьезоэлемент к доступной стороне стены или наружному стеклу, пусть даже парной рамы. Превосходный акустический сигнал иной раз удается снимать с труб водоснабжения и батареи отопления.

Направленные микрофоны

Спектр направленных микрофонов, существующих на рынке спецтехники, довольно широк: от банальных тарелок до резонансных сеток, предназначенных для скрытого ношения. Возможно применение остронаправленного микрофона, закамуфлированного под вписывающиеся в облик и ситуацию трость или зонтик.

Данные устройства просто изготовить и самому (склеив, к примеру, длинную — около 2 м — трубку из плотной бумаги и поместив в ее торец диаметром 10—15 см любой в меру чувствительный микрофон). Они позволят слушать разговоры и другие посторонние звуки, приходящие преимущественно с одного направления, на значительном расстоянии. Количество посторонних сигналов будет тем меньше, чем у́же диаграмма направленности микрофона. Чтобы повысить их дальность действия, в схеме последующего усилителя можно использовать так называемые селективные фильтры, а проще — бытовые эквалайзеры (многополосные регуляторы тембра), активно выделяющие узкие полосы частот. Ниже приведен пример изготовления направленного микрофона органного типа.

Направленный микрофон органного типа

Необходимо помнить, что микрофонный усилитель усиливает звуки, приходящие со всех сторон, и, если соотношение сигнал/шум будет недостаточным, нужно применять пространственные направляющие системы (направленные микрофоны). В этом случае дистанционное звуковое прослушивание ведется с помощью дистанционно направленных микрофонов, имеющих очень узкую диаграмму направленности. С помощью такого микрофона можно прослушать разговор на расстоянии до 1 км в пределах прямой видимости, здесь имеет место принцип: «Поблизости никого нет, но тем не менее вас хорошо прослушивают». Использование явления резонанса звуковых волн в направленных системах приводит к увеличению уровня сигнала звуковой энергии, который поступает в микрофон.

Простой направленный микрофон представляет собой набор из 7 алюминиевых трубок диаметром 10 мм. Длина трубки определяет резонансную частоту звукового сигнала. Формула для расчета длины трубок имеет следующий вид:

$$L = 330/2F,$$

где L — длина трубки, м; F — резонансная частота, Гц.

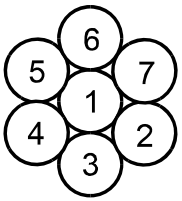


Рис. 2.13. Избирательная система из направленных трубок

Исходя из выше приведенной формулы, можно построить табл. 2.2, где № — номер трубки.

Вариант размещения избирательной системы, составленной из направленных трубок, приведен на рис. 2.13.

Таблица 2.2. **Характеристики трубок направленного микрофона**

№	1	2	3	4	5	6	7
L, мм	550	400	300	200	150	100	50
F, Гц	300	412	550	825	1100	1650	3300

Микрофон располагается в параболическом улавливателе, фокусом которого является направляющая система (рис. 2.14). Дальнейшее усиление сигнала происходит за счет использования высокочувствительного микрофонного усилителя *МУ*.

Этот направленный микрофон перекрывает диапазон частот 300 — 3300 Гц, т. е. основной информационный диапазон речевого сигнала.

Если необходимо получить более качественное восприятие речи, то необходимо расширить диапазон принимаемых частот. Это можно сделать путем увеличения количества резонансных трубок, например, до 37 штук. В табл. 2.3 приведены расчетные данные для использования в избирательной системе от 1 до 37 трубок. Такая резонансная система перекрывает диапазон частот от 180 до 8200 Гц. Вариант размещения резонансных трубок приведен на рис. 2.15, где трубки располагаются «улиткой».

Вместо резонансной системы можно использовать параболический рефлектор диаметром 30—80 см.

Однако эффективная дальность используемых остронаправленных микрофонов обычно не превышает 15—20 м. Реально же, в условиях городского шума, можно рассчитывать на расстояние порядка 5—6 м. Почему? Теоретически создать микрофон с узкой диаграммой направленности, удовлетворяю-

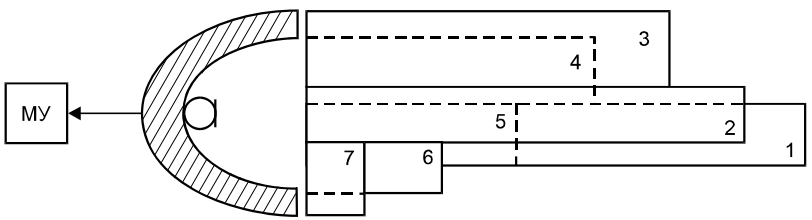
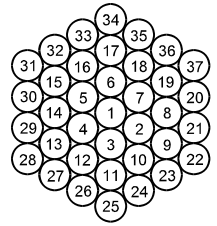


Рис. 2.14. Микрофон в параболическом улавливателе



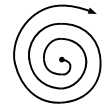


Рис. 2.15. Избирательная резонансная система

щей дальности снятия информации с расстояния 100—150 м, возможно. Вопрос только в том, что с ним делать, как использовать его основное преимущество — острую диаграмму направленности.

Попробуйте удержать на одном месте солнечный зайчик, пляшущий, скажем, на стене в 50 м от вас. Трудно? Так вот, размер «акустического пятна», которым нужно будет накрывать рот говорящего, будет у нашего микрофона не намного больше этого зайчика. На расстоянии 100 м, даже если микрофон жестко закрепить, случайный порыв вет-

Таблица 2.3. **Расчетные данные избирательной системы**

№	1	2	3	4	5	6	7	8	9	10	11	12	
L, мм	920	895	870	845	820	792	770	745	720	695	670	645	
F, мм	180	184	190	195	201	208	214	222	229	237	246	256	
№	13	14	15	16	17	18	19	20	21	22	23	24	
L, мм	620	595	570	545	520	495	470	445	420	395	370	345	
F, мм	266	277	290	303	317	333	351	371	393	4418	446	478	
№	25	26	27	28	29	30	31	32	33	34	35	36	37
L, мм	320	295	270	245	220	195	170	145	120	95	70	45	20
F, мм	516	560	611	674	750	846	971	1138	1375	1737	2357	3667	8250

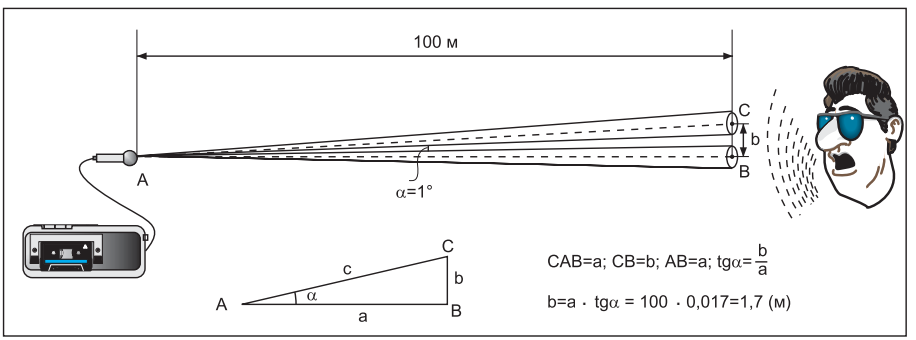


Рис. 2.16. Расчет дальности действия узконаправленного микрофона

ра, вибрация от проезжающего рядом транспорта и т. п. будут уводить «прицел» на некоторое расстояние. Допустим, что ось диаграммы направленности микрофона сместилась относительно своего первоначального положения всего на 1° (рис. 2.16). Как видно из этого рисунка, при расстоянии 100 м центр «акустического пятна» переместился на 1,7 м. На самом деле направленный микрофон смещается не на один, а на несколько градусов (результат посчитайте сами). А если при этом еще и источник звука перемещается, то шансы получения информации с такого расстояния стремятся к нулю.

Защита информации, циркулирующей по акустическому каналу

Методы защиты информации, циркулирующей по акустическому каналу, разделяют на *пассивные* и *активные*, в которых используют или не используют дополнительный источник энергии. Пассивные методы основаны на снижении уровня звуковой мощности акустического сигнала в расчетной точке.

Классификация пассивных методов представлена на рис. 2.17.

К пассивным методам относятся и так называемые архитектурно-планировочные методы защиты, которые основаны на:

- рациональном расположении источника акустического сигнала;
- акустической обработке помещений, обеспечивающих наибольшую разборчивость речи в помещении при минимально заданном уровне мощности источника;
- соответствующем решении конструкции и планировки зданий;
- звукоизоляции;
- звукопоглощении;
- звукоотражении;
- снижении уровня звука на пути его распространения.

Звукоизоляция — это ослабление звуковой энергии при распространении ее через ограждение путем отражения падающей на него звуковой энергии. Изолирующими преградами звуковой энергии на пути распространения являются стены, перегородки, специальные кожухи, кабели и т. п.

Звукопоглощение — это ослабление падающей акустической энергии, характеризующейся коэффициентом звукопоглощения (отношение разности падающей и отраженной от поверхности акустической энергии к падающей энергии). К звукопоглощающим конструкциям относятся звукопоглощающие облицовки ограждающих поверхностей помещений, штучные звукопоглотители, облицованные поверхности акустических экранов, звукопоглощающие облицовки в камерных глушителях и звукоизолирующих кожухах. Глушители шума предназначены для снижения звука, распространяющегося по системам вентиляции и кондиционирования воздуха.

Рис. 2.17. Классификация пассивных методов защиты акустической информации

Пассивные методы защиты подразделяют на снижающие шум в источнике его возникновения и снижающие шум на пути его распространения от источника (передатчика) до расчетной точки (приемника). Снижение звука в источнике возникновения возможно уменьшением его возбуждающей активности и звукоизлучающей способности через воздушную среду (воздушный звук) или через элементы конструкции (структурный звук).

Для уменьшения уровня звуковой мощности, проникающей из изолированного помещения, при проектировании перекрытий стен, сплошных и остекленных дверей рекомендуют применять материалы и конструкции, обеспечивающие требуемую звукоизоляцию, устанавливать звукопоглощающие облицовки, изменять виброизолирующие и вибродемпфирующие покрытия на поверхности трубопроводов, проходящих через помещения, использовать глушители шума в системах вентиляции и кондиционирования воздуха.

Звукоизоляция стен и перекрытий осуществляется путем создания многослойной конструкции на основе звукопоглощающих материалов (войлок, гипсобетон, гипсоволокно и т. д.). Необходимо отметить, что существенное влияние на звукоизоляцию ограждающих конструкций оказывает наличие в них щелей и отверстий.

Наиболее уязвимыми являются окна и двери защищаемых помещений. Рассмотрим решения по их звукоизоляции более подробно. Основным направлением повышения звукоизоляции дверей является организация тамбурной системы. При этом целесообразно применять утяжеленные полотна дверей, обивку полотен дверей обивочными материалами со слоями ваты или войлока, использовать дополнительные уплотнительные прокладки, герметизирующие щели. Целесообразна облицовка внутренних поверхностей тамбура звукопоглощающими покрытиями. Окна, занимающие по условиям освещенности достаточно большие площади ограждающих конструкций, являются, так же как и

двери, наиболее слабыми элементами с точки зрения звукоизолирующей способности. Наиболее совершенными в настоящее время являются конструкции окон с повышенным звукопоглощением на основе стеклопакетов с герметизацией воздушного промежутка и заполнением промежутка между стеклами различными газовыми смесями. Стеклопакеты устанавливаются в выполненных из различных материалов рамах. Стекла выбираются разной (не кратной) толщины и устанавливаются с небольшими наклонами относительно друг друга. Все это позволяет при значительном ослаблении сигнала избежать резонансных явлений в воздушных промежутках. В результате интенсивность речевого сигнала на внешнем стекле оказывается значительно ниже интенсивности фоновых акустических шумов, и съем информации традиционными для акустики методами является невозможным или сильно затрудненным.

Наиболее радикальной мерой защиты является прерывание распространения звука. Это достижимо только в случае применения вакуумной звукоизоляции. В основе способа лежит физическое явление, состоящее в том, что звук не может распространяться в пустоте. Таким образом, теоретически при вакууме между точкой получения информации и источником речи получаем идеальную звукоизоляцию. Однако на практике обеспечить полное прерывание невозможно, так как требуется обеспечить герметизацию не только межстекольного пространства, но и пространства между переплетом и рамой, а кроме того, предотвратить структурное распространение через материал рам. Окна обычной конструкции имеют низкий уровень звукоизоляции. Очевидно, что возможно увеличить значения поверхностных масс внешнего и внутреннего стекол и расстояния между ними. Кроме того, на звукоизоляцию влияет:

- герметичность швов между стеклом и переплетом, переплетом и оконной рамой, оконной рамой и стеной;
- длина, высота и размер поперечного сечения переплета и стекла;
- поглощение звука в звукопоглощающих элементах между стеклами и рамой;
- особенности конструкции и способы ее изготовления и т. д.

Широкое распространение получили акустические экраны, которые используются при невозможности применения стационарных методов звукоизоляции. Обычно применяются передвижные, складные и легко монтируемые акустические экраны. При решении задач по защите выделенных помещений акустические экраны могут быть использованы для дополнительной защиты дверей, окон, технологических проемов и других элементов ограждающих конструкций, имеющих локальную низкую звукоизолирующую способность.

Активные методы защиты акустической информации, например речи, основаны на использовании различных генераторов акустического шума, маскирующих полезный звуковой сигнал. С их помощью производится зашумление речевого диапазона в помещениях и линиях связи, а также они используются для оценки акустических свойств помещений.

В широком смысле под шумом понимают помехи, представляющие собой смесь случайных и кратковременных периодических сигналов. В узком смысле под шумом понимают так называемый белый шум, характеризующийся тем, что его амплитудный спектр распределен по нормальному закону, а спектральная плотность мощности постоянна для всех частот. Примером белого шума является тепловой шум резистора. Кроме белого шума выделяют такие разновидности шума, как фликкер-шум и импульсный шум. В генераторах шума обычно используется белый шум. Он позволяет замаскировать полезную информацию на фоне шума. В отличие от однотональной или многотональной периодической помехи (музыки, шума двигателя и т. п.), которые путем специальной обработки сигнала могут быть отфильтрованы, помехи типа белого шума практически не поддаются полной фильтрации и поэтому являются наиболее эффективными для закрытия полезной информации. Кроме того, акустические генераторы белого шума эффективны еще и тем, что воздействуют непосредственно на входные низкочастотные тракты подслушивающих систем (микрофоны) независимо от особенностей их схемотехники и принципов передачи информации.

Для защиты от утечки информации по каналам побочных электромагнитных излучений электронно-вычислительной техники используют генераторы шума, излучающие активную широкополосную радиопомеху, воздействующую на входные цепи радиоприемных устройств. Аналогичные приборы используются для защиты от утечки информации по электрической сети и телефонным линиям.

У подобных систем имеется целый ряд недостатков. Во-первых, значительно повышается уровень фоновых акустических шумов в защищаемом помещении, что приводит к быстрой утомляемости находящихся в нем людей. Во-вторых, при разговоре в зашумленном помещении человек инстинктивно начинает говорить громче, тем самым повышается отношение сигнал/помеха на выходе приемника акустической разведки. В-третьих, в случае, когда в качестве исполнительных механизмов станций активных акустических помех используются вибродатчики, которые позволяют несколько снизить уровень акустических шумов в помещении, в действие вступают медицинские факторы. Создаваемые станциями постановки помех виброколебания, имея широкий частотный диапазон (от единиц герц до 20 Гц), раздражающе воздействуют на нервную систему, вызывая изменения как физиологического, так и функционального характера в организме человека. При определенных условиях действие широкополосной вибрации становится опасным для здоровья, снижаются производительность и качество труда, может возникнуть вибрационная болезнь. В связи с этим отмечается тенденция отказа от применения активных систем зашумления в акустическом диапазоне.

Кроме генераторов белого шума в качестве маскирующего воздействия при разговоре рекомендуется использовать помехосоздающие магнитные пленки, которые можно записать в местном баре, ресторане или другом месте, где ведется несколько разговоров одновременно. Музыка также может использоваться для того, чтобы труднее было отличить голос от посторонних шумов.

Любой фоновый шум поможет предупредить считывание лазерным лучом вибраций окон и использование компьютера для преобразования вибраций (фильтрации сигнала) в звук.

Генераторы шума промышленного производства

В настоящее время на российском рынке представлен целый ряд моделей генераторов акустического шума. Коротко рассмотрим лишь некоторые из них. Существуют стационарные генераторы шума, звуковые колонки которых устанавливают в вентиляционных отверстиях, воздуховодах и пр., а также — портативные генераторы акустического белого шума, которые могут применяться везде, где это необходимо.

В их названиях недаром присутствуют два слова: «акустический» и «белый». Акустический потому, что максимум излучения лежит в речевом диапазоне частот. И сами разговаривающие этот шум тоже слышат. Белым называется шум, спектральный состав которого однороден по всему диапазону излучаемых частот. Такой сигнал является сложным, как и наша речь, и в нем нельзя выделить каких-то преобладающих спектральных составляющих. Дело в том, что существующие на сегодняшний день методы очистки звуковых сигналов с легкостью справляются с простыми помеховыми сигналами, которые имеют в своем составе одну или несколько, но ограниченное количество, спектральных составляющих. Если противник встроил микрофон в блок питания вашего компьютера, то шум его вентилятора полностью «забивает» полезный сигнал. Однако устройство под названием «адаптивный фильтр» позволяет «вытаскивать» полезный сигнал из-под этого шума с вполне приемлемым качеством. Еще один момент: если зашумить помещение сложным, но известным сигналом, например включить радиоприемник, то у подслушивающего есть теоретическая возможность записать два сигнала — полезный с наложенной на него радиопередачей и отдельно радиопередачу, а затем вычесть один сигнал из другого, в результате чего останется только полезный сигнал. Белый шум такими способами отфильтровать не удается.

Генератор шума ANG-2000

Генератор акустического шума ANG-2000 (рис. 2.18) предназначен для защиты помещений от возможного прослушивания через проводные микрофоны, радиомикрофоны и стетоскопы, блокирования лазерного съема акустической информации с окон, создания помех звукозаписывающей аппаратуре. Генератор имеет плавную регулировку и светодиодную индикацию уровня шума, возможность подключения акустических излучателей типа OMS-2000 и вибрационных излучателей типа TRN-2000. В комплект изделия входит сетевой адаптер питания. Акустические и вибрационные излучатели, элементы крепления вибрационных излучателей к стеклам поставляются отдельно.

Рис. 2.18. Генератор акустического шума ANG-2000 с акустическими и вибрационными излучателями

Основные технические характеристики

Диапазон акустического шума, Гц ..... 250—5000
Пределы регулировки выходного напряжения
на нагрузке 6 Ом, В ..... 0—14
Минимальное сопротивление нагрузки, Ом 1
Сопротивление одного излучателя, Ом..... 6
Количество подключаемых излучателей на один
блок, шт. ..... до 18
Напряжение питания, В ..... 12—18
Потребляемый ток, А ..... не более 2
Габариты, мм .....43×152×254

Система акустовиброзашумления VNG-0006D

Предназначена для защиты помещений от утечки акустической информации по виброканалам и через технические средства съема акустической информации, использующие микрофон. Устройство формирует акустические и вибрационные шумоподобные сигналы, воспроизводимые через акустические колонки и вибропреобразователи. Имеется возможность плавной регулировки уровня шумового акустического сигнала. Особенностью устройства является использование вибропреобразователей на основе пьезокерамики, обладающих высокой эффективностью при формировании требуемого уровня вибрационных помех. Генератор шума и используемых с ним датчиков показан на рис. 2.19. Пре-

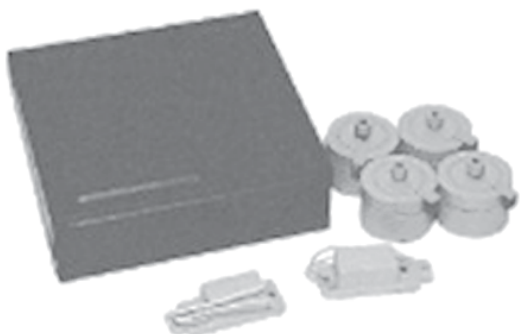


Рис. 2.19. Генератор шума VNG-0006D и вибрационные датчики

дусмотренная в устройстве возможность подключения преобразователей позволяет зашумлять пространство над подвесным потолком, вентиляционные каналы и дверные тамбуры. Комплект поставки предусматривает все необходимые установочные элементы для монтажа.

Основные технические характеристики

Диапазон акустического шума, Гц ..... 200—15 000
Уровень громкости защищаемых речевых сигналов, дБ ..... не более 75
Максимальное количество вибропреобразователей, шт. 12
Минимальное сопротивление нагрузки, Ом 8

Комплекс ультразвуковой защиты помещений «Завеса»

Используется для нарушения работоспособности (подавления) различных микрофонных устройств, предназначенных для несанкционированного перехвата акустической информации (диктофонов, радио- и встроенных микрофонов).

Комплекс предназначен для работы в замкнутом пространстве (помещении) и обеспечивает защиту, в зависимости от необходимости, какой-либо локальной области или помещения в целом, используя многоканальную версию комплекса.

Минимальная конфигурация комплекса — двухканальная, обеспечивающая защиту в объеме 27 м^3. При необходимости комплекс имеет возможность наращивания.

Отличительной особенностью комплекса является воздействие на микрофонное устройство и его усилитель достаточно мощным ультразвуковым сигналом (группой сигналов). Это воздействие вызывает блокирование усилителя или возникновение значительных нелинейных искажений, приводящих в конечном счете к нарушению работоспособности микрофонного устройства (его подавлению).

Поскольку воздействие осуществляется по каналу восприятия акустического сигнала, то совершенно неважны дальнейшие трансформация, способы и каналы передачи перехваченной акустической информации (они могут быть сколь угодно сложными), так как информационный акустический сигнал подавляется на этапе его восприятия. Все это делает комплекс достаточно универсальным по сравнению с существующими комплексами и средствами активной защиты акустической информации от утечки по техническим каналам.

Принципиальные схемы генераторов шума

Кроме промышленных образцов для защиты акустического канала могут с успехом использоваться и генераторы, изготовленные самостоятельно. Ниже приводятся несколько принципиальных схем различных генераторов акустического шума, пригодных для изготовления в домашних условиях.

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. 2.20.

Источником шума является полупроводниковый диод — стабилитрон *VD1* типа К*С1*68, 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 конденсатор *C1* поступает на инвертирующий вход операционного усилителя *DA1* типа КР140УД1208. На неинвертирующий 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*. 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 *C4* поступает на малогабаритный широкополосный громкоговоритель *B1*. 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 усилитель типа КР1407УД2 или любой операционный усилитель с высокой граничной частотой коэффициента единичного усиления. Вместо усилителя на *DA2* можно использовать любой УЗЧ.

Для получения калиброванного по уровню шума генератора используют специальные шумящие вакуумные диоды. Спектральная плотность мощности генерируемого шума пропорциональна анодному току диода. Широкое распространение получили шумовые диоды двух типов — 2Д3Б и 2Д2С. Первый генерирует шум в полосе до 30 МГц, а второй — до 600 МГц. Принципиаль-

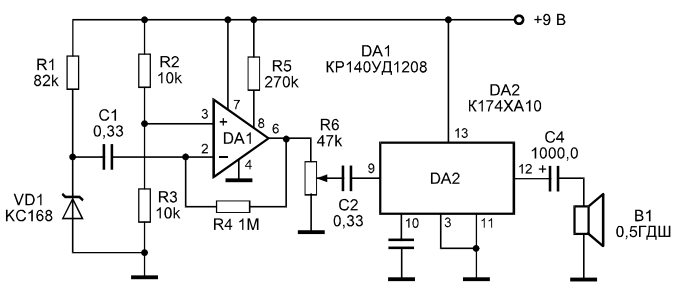


Рис. 2.20. Принципиальная схема генератора белого шума

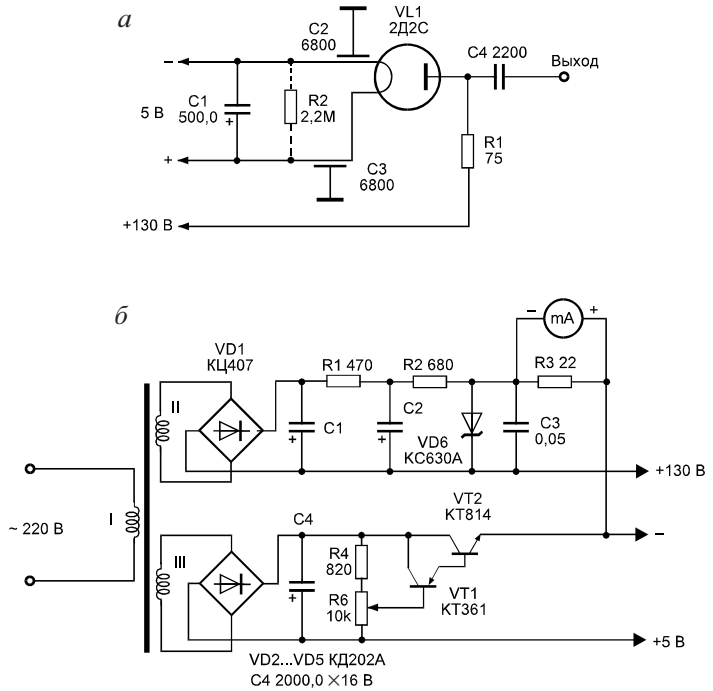


Рис. 2.21. Принципиальная схема генератора шума: *а* — на шумящих вакуумных диодах; *б* — специального блока питания

ная схема генератора шума на шумящих вакуумных диодах приведена на рис. 2.21, *а*. Резистор *R1* типа МЛТ-0,25; *R2* — проволочный, используется совместно с диодом 2Д3Б. Питание генератора осуществляется от специального блока, схема которого приведена на рис. 2.21, *б*.

Цифровой генератор шума

Цифровой шум представляет собой временной случайный процесс, близкий по своим свойствам к процессу физических шумов, и поэтому называется 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. 2.22.

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),* собранные 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 *C* 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.* 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 питания 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.

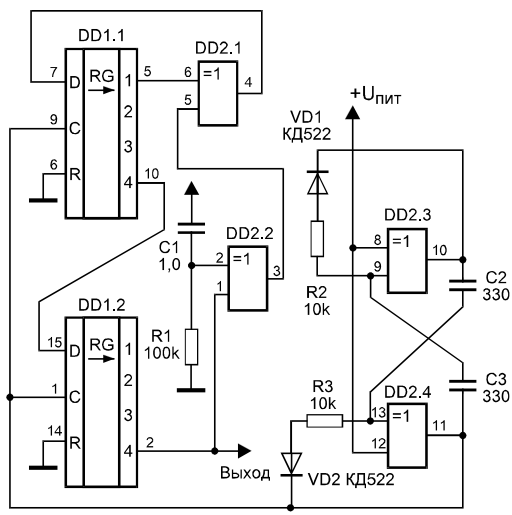


Рис. 2.22. Принципиальная схема цифрового генератора шума

2.2. Радиомикрофоны

Радиомикрофоны являются самыми распространенными техническими средствами ведения коммерческой разведки. Их популярность объясняется прежде всего удобством их оперативного использования, простотой применения (не требуется длительного обучения персонала), дешевизной, очень небольшими размерами.

Радиомикрофон, как следует из названия, это микрофон, объединенный с радиоканалом и предназначенный для передачи акустической информации на расстояние. В настоящий момент нет устоявшегося названия этих устройств. Их называют *радиозакладками*, *закладными устройствами*, *радиобагами*, *радиокапсулами*, иногда «жучками» или «клопами», но все-таки самым точным названием следует признать название «радиомикрофон». Мы будем придерживаться в дальнейшем именно этого названия.

В общем виде структурная схема радиомикрофона приведена на рис. 2.23.

В простейшем случае радиомикрофон состоит из собственно микрофона, т. е. устройства для преобразования звуковых колебаний в электрические, задающего высокочастотного (ВЧ) генератора — устройства, генерирующего ВЧ-колебания (несущую частоту), промодулированные электрическими сигналами с микрофона, и антенны, излучающей эти электромагнитные колебания. Устройства управления и записи не являются обязательными элементами радиомикрофона. Они предназначены для расширения его возможностей: дистанционного включения/выключения передатчика, микрофона, переключения режимов работы, записи и сжатия информации.

Микрофон определяет зону акустической чувствительности (обычно она колеблется от нескольких до 20—30 м), радиопередатчик — дальность действия радиолинии. Основными параметрами с точки зрения дальности действия для передатчика являются мощность, стабильность несущей частоты, диапазон частот, вид модуляции. Дальность действия, габариты и время непрерывной работы находятся в очень тесной зависимости друг от друга. В самом деле, для увеличения дальности прежде всего необходимо увеличить мощность передатчика, одновременно с этим возрастает ток, потребляемый от

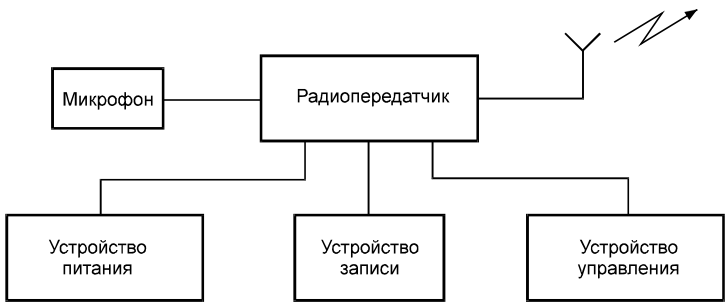


Рис. 2.23. Структурная схема радиомикрофона

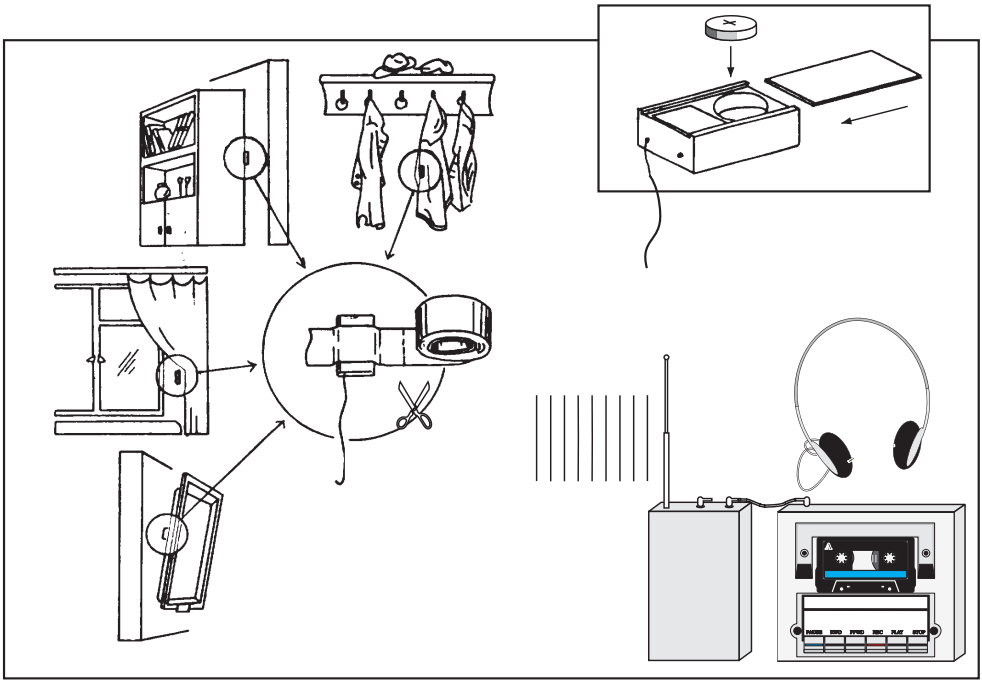


Рис. 2.24. Возможные места установки радиомикрофонов

источника питания, который быстрее расходует свой ресурс, а значит, сокращается время непрерывной работы. Чтобы его повысить, увеличивают емкость батарей питания, что влечет за собой рост габаритов радиомикрофона. Можно увеличить длительность работы передатчика введением в его состав устройства дистанционного управления (включение/выключение), однако это также скажется на габаритах (необходим приемник системы ДУ). Для увеличения дальности применяют промежуточные ретрансляторы, а радиомикрофоны иной раз устанавливают на металлические предметы — трубы водоснабжения, радиаторы отопления, бытовые электроприборы, которые в этом случае служат дополнительной передающей антенной. Существенное влияние на длину радиоканала оказывает, конечно, и тип радиоприемного устройства. Кроме того, нужно иметь в виду, что увеличение мощности передатчика облегчает возможность его обнаружения.

Наличие большого количества моделей радиомикрофонов объясняется тем, что в различных ситуациях требуется вполне определенная модель. Стационарные модели питаются от электрической сети и обычно размещаются в торшерах, телевизорах, электророзетках, люстрах и других стандартных элементах обстановки (рис. 2.24).

Все подбрасываемые модели питаются от автономного источника питания и закладываются при тайном или легальном посещении нужного помещения в

Рис. 2.25. Замаскированные радиомикрофоны

самые укромные его места (за книги, картины, среди бижутерии, в обивке мебели) и часто маскируются под шариковые ручки, фломастеры (рис. 2.25), коробки от спичек, безделушки, микрокалькуляторы, зажигалки и прочие вещи. Существуют модели, выполненные в виде заколки или зажима для галстука, наручных часов, значка, губной помады и другие, внешне ничем не отличающиеся от вещей, которые используются по прямому назначению.

Очень часто радиомикрофоны маскируются под элементы радиотехнических конструкций — конденсаторы, резисторы, реле и т. п. Пример такого использования представлен на рис. 2.26.

Главным недостатком большинства данных конструкций является ограниченный период их автономной работы, от десятков до нескольких сотен часов, в частности зависящий от излучаемой в пространство мощности (от долей до сотен милливатт) и электроемкости используемых батарей. Сами разговоры перехватываются на расстоянии от 5 до 30 м, тогда как радиус передачи информации составляет от десятков до сотен метров. Для увеличения дальности применяют промежуточные ретрансляторы, а радиомикрофоны иной раз устанавливают на металлические предметы — трубы водоснабжения, радиаторы отопления, бытовые электроприборы, которые служат дополнительной передающей антенной.

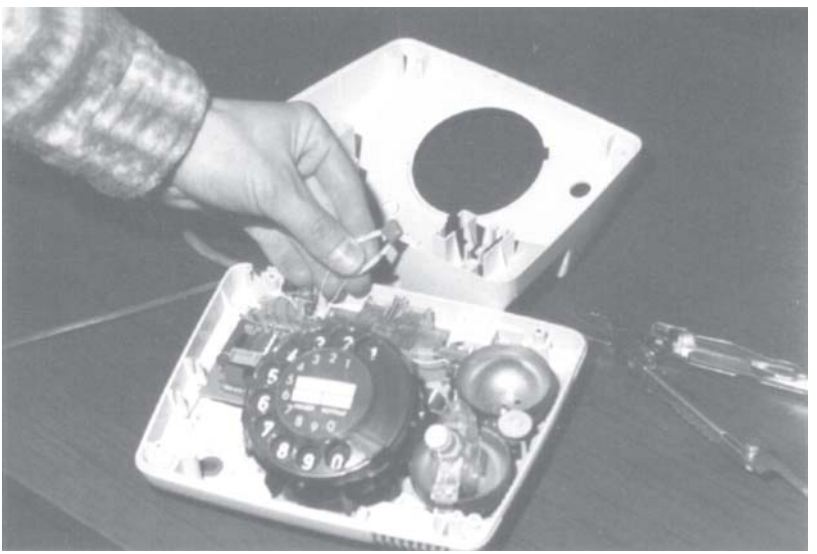


Рис. 2.26. Радиомикрофон-«конденсатор», включенный в схему телефона

Фирменные радиомикрофоны работают на самых разных частотах: от десятка до тысячи мегагерц. Повышение рабочей частоты увеличивает дальность действия в бетонных зданиях, но здесь требуются специальные радиоприемники или преобразующие приставки (конверторы) к бытовым УКВ-приемникам. Подстраховываясь от случайного обнаружения, профессионалы иногда задействуют такие уловки, как необычное растягивание спектра передаваемого сигнала, сдвоенную модуляцию несущей частоты, уменьшение исходной мощности с применением промежуточного ретранслятора, прыгающие изменения несущей.

Очень эффективным и простым приемом повышения скрытности работы радиомикрофона представляется его использование в радиовещательном диапазоне (66—74 или 88—108 МГц) в непосредственной близости от несущей частоты мощной радиостанции. В этом случае радиоприемники, имеющие автоматическую подстройку частоты (АПЧ), обычно не реагируют на слабый сигнал из-за наличия более сильного, а у приемника подслушивающего данная система АПЧ отключается для значительного увеличения избирательности.

Кроме того, для уменьшения вероятности обнаружения мощность передатчика радиомикрофона делается минимально необходимой, но достаточной для приема информации высокочувствительным приемником с небольшого расстояния.

Как уже говорилось выше, дальность действия радиопередатчиков определяется в существенной степени качествами радиоприемных устройств, прежде всего чувствительностью. В качестве приемников часто используют бытовые радиоприемные устройства. В этом случае предпочтительным является применение магнитол, так как появляется возможность одновременного ведения записи. К недостаткам таких устройств относятся низкая чувствительность и возможность настройки посторонних лиц на частоту передатчика. Частично эти недостатки можно устранить перестройкой частотного диапазона, в том числе с помощью конверторов, а также переналадкой усилителей для повышения чувствительности. Достоинством таких систем является низкая стоимость, а также то, что они не вызывают подозрений. Но все же предпочтительным считается применение специальных приемных устройств.

Миниатюрный радиопередатчик на туннельном диоде

Схема простого микропередатчика изображена на рис. 2.27. В основе этого устройства лежит схема ВЧ-генератора на туннельном диоде. Ток, потребляемый генератором от источника питания, составляет примерно 15 мА и зависит от типа туннельного диода. Последний может быть выбран, по усмотрению радиолюбителя, с током потребления не более 10—15 мА (например, диод АИ201А).

Генератор сохраняет свою работоспособность при напряжении источника питания 1 В и выше при соответствующем выборе рабочей точки резистором *R2*. Дроссель *Др1* наматывается на резисторе МЛТ 0,25 проводом ПЭВ 0,1 мм и содержит 200—300 витков. Чтобы провод не соскакивал с резистора, он пери-

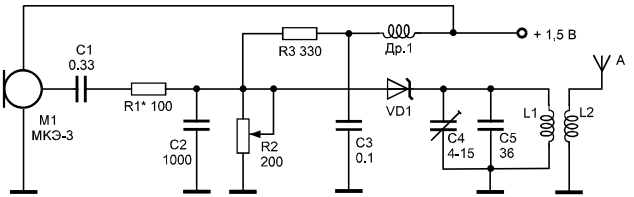


Рис. 2.27. Принципиальная схема радиопередатчика на туннельном диоде

одически смазывается клеем «Момент», БФ-2 и др. Индуктивность дросселя должна быть 100—200 мкГн. Дроссель может быть заводского изготовления. Катушка колебательного контура *L1* выполнена без каркаса и содержит 7 витков провода ПЭВ 1,0. Диаметр катушки — 8 мм, длина намотки — 13 мм. Катушка связи *L2,* так же, как и *L1,* бескаркасная, намотана проводом ПЭВ 0,35, 3 витка, диаметр катушки — 2,5 мм, длина намотки — 4 мм. Катушка *L2* располагается внутри катушки колебательного контура *L1*.

Настройка передатчика сводится к установке рабочей точки туннельного диода путем вращения движка подстроечного резистора *R2* до появления устойчивой генерации и подстройке частоты колебаний конденсатором *C4*. Антенной является отрезок монтажного провода длиной примерно в четверть длины волны. Глубину модуляции можно изменять подбором сопротивления резистора *R1*. Сигнал этого передатчика можно принимать на телевизионный приемник.

Мощность излучения приведенного устройства составляет доли единиц милливатт. Соответственно и радиус действия этих устройств составляет единицы метров.

Микропередатчик с частотной модуляцией

Схема микропередатчика, выполненного на одном транзисторе, приведена на рис. 2.28.

Модулирующее напряжение, снимаемое с электретного микрофона МКЭ-3 (МКЭ-333, МКЭ-389, *M1*-А2 «Сосна»), через конденсатор *C1* поступает на базу транзистора *VT1*, на котором выполнен задающий генератор. Так как управляющее напряжение приложено к базе транзистора *VT1*, то, изменяя напряжение смещения на переходе «база — эмиттер» и, соответственно, емкость цепи «база — эмиттер», которая является одной из составных частей колебательного контура задающего генератора, осуществляется частотная модуляция передатчика. Этот же контур включает в себя также катушку индуктивности *L1*, расположенную по высокой частоте между базой транзистора *VT1* и массой и конденсаторами *C3* и *C4*. Конденсатор *C4* включен в цепь обратной связи емкостной трехточки, являясь одним из плеч делителя $C_{бэ}$—*C4*, с которого и снимается напряжение обратной связи. Емкость конденсатора *C4* позволяет регулировать уровень возбуждения. Во избежание влияния шунтирующего резистора *R2* в цепи эмиттера транзистора *VT1* на колебательный контур, которое может

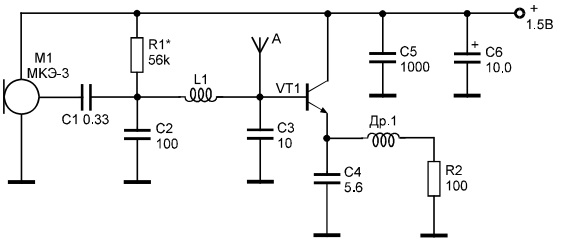


Рис. 2.28. Принципиальная схема микропередатчика с частотной модуляцией

вызвать чрезмерное расширение полосы частот резонансной кривой, последовательно с резистором *R2* включен дроссель *Др1*, блокирующий прохождение токов высокой частоты. Индуктивность этого дросселя должна быть около 20 мкГн. Катушка *L1* бескаркасная, диаметром 3 мм, намотана проводом ПЭВ 0,35 и содержит 7—8 витков.

Для получения максимально возможной мощности необходимо правильно выбрать генерирующий элемент (транзистор *VT1*) и установить оптимальный режим работы генератора. Для этого надо применять транзисторы, верхняя граничная частота которых должна превышать рабочую частоту генератора не менее чем в 7—8 раз. Этому условию наиболее полно отвечают транзисторы типа n—p—n КТ368, хотя можно использовать и более распространенные транзисторы КТ315 или КТ3102.

Миниатюрный радиопередатчик с питанием от батареи для электронных часов

Схема следующего радиопередатчика приведена на рис. 2.29. Устройство содержит минимум необходимых деталей и питается от батарейки для электронных часов напряжением 1,5 В.

При столь малом напряжении питания и потребляемом токе 2—3 мА сигнал этого радиомикрофона может приниматься на удалении до 150 м. Продолжительность работы около 24 ч. Задающий генератор собран на транзисторе *VT1* типа КТ368, режим работы которого по постоянному току задается резистором *R1*. Частота колебаний задается контуром в базовой цепи транзистора *VT1*. Этот контур включает в себя катушку *L1*, конденсатор *C3* и емкость цепи «база — эмиттер» транзистора *VT1*, в коллекторную цепь которого в качестве нагрузки включен контур, состоящий из катушки *L2* и конденсаторов *C6*, *C7*. Конденсатор *C5* включен в цепь обратной связи и позволяет регулировать уровень возбуждения генератора.

В автогенераторах подобного типа частотная модуляция производится путем изменения потенциалов выводов генерирующего элемента. В нашем случае управляющее напряжение прикладывается к базе транзистора *VT1*, изменяя тем самым напряжение смещения на переходе «база — эмиттер» и, как следствие, изменяя емкость перехода «база — эмиттер». Изменение этой ем-

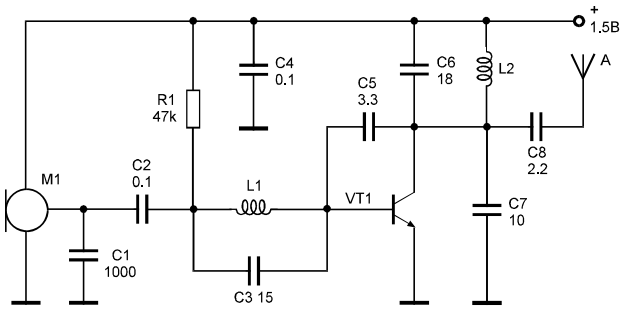


Рис. 2.29. Принципиальная схема радиопередатчика с питанием от батареи 1,5 В

кости ведет к изменению резонансной частоты колебательного контура, что и приводит к появлению частотной модуляции. При использовании УКВ-приемника импортного производства требуемая величина максимальной девиации несущей частоты составляет 75 кГц (для отечественного стандарта — 50 кГц) и получается при изменении напряжения звуковой частоты на базе транзистора в диапазоне 10—100 мВ. Именно поэтому в данной конструкции не используется модулирующий УЗЧ. При использовании электретного микрофона с усилителем, например, МКЭ-3, *M1*-Б2 «Сосна», уровня сигнала, снимаемого непосредственно с выхода микрофона, оказалось достаточно для получения требуемой девиации частоты радиомикрофона. Конденсатор *C1* осуществляет фильтрацию колебаний высокой частоты. Конденсатором *C7* можно в небольших пределах изменять значение несущей частоты. Сигнал в антенну поступает через конденсатор *C8*, емкость которого специально выбрана малой для уменьшения влияния возмущающих факторов на частоту колебаний генератора. Антенна сделана из провода или металлического прутка длиной 60—100 см. Длину антенны можно уменьшить, если между ней и конденсатором *C8* включить удлинительную катушку *L3* (на рис. 2.4 не показана). Катушки радиомикрофона бескаркасные, диаметром 2,5 мм, намотаны виток к витку. Катушка *L1* имеет 8 витков, катушка *L2* — 6 витков, катушка *L3* — 15 витков провода ПЭВ 0,3.

При настройке устройства добиваются получения максимального сигнала высокой частоты, изменяя индуктивности катушек *L1* и *L2*. Подбором конденсатора *C7* можно немного менять величину несущей частоты, в некоторых случаях его можно исключить совсем.

Микропередатчик со стабилизацией тока

Схема предлагаемого миниатюрного устройства (рис. 2.30) заметно отличается от приведенных выше. Она проста в настройке и изготовлении, позволяет изменять частоту задающего генератора в широких пределах. Устройство сохраняет работоспособность при величине питающего напряжения выше 1 В.

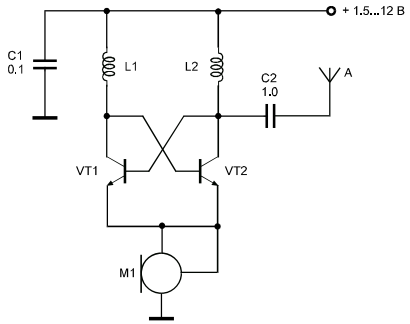


Рис. 2.30. Принципиальная схема микропередатчика со стабилизацией тока

Генератор высокой частоты собран по схеме мультивибратора с индуктивной нагрузкой. Изменение частоты колебаний высокой частоты происходит при изменении тока, протекающего через транзисторы *VT1*, *VT2* типа КТ368. При изменении тока меняются параметры проводимости транзисторов и их диффузионные емкости, что позволяет варьировать частоту такого генератора в широких пределах без изменения частотозадающих элементов — катушек *L1* и *L2*. Для повышения стабильности частоты и возможности управления генератором с целью получения частотной модуляции питание последнего осуществляется через стабилизатор тока. Стабилизатор и модулирующий усилитель выполнены на электретном микрофоне *M1* типа МКЭ-3, *M1*-Б2 «Сосна» и им подобным. При использовании кондиционных деталей уход несущей частоты при изменении напряжения питания с 1,5 до 12 В не превышает 150 кГц (при средней частоте генератора 100 МГц).

В схеме используются бескаркасные катушки *L1* и *L2* диаметром 2,5 мм. Для диапазона 65—108 МГц катушки содержат по 15 витков провода ПЭВ 0,3. Настройка заключается в подгонке частоты путем изменения индуктивности катушек *L1* и *L2* (сжатием или растяжением). Рассматриваемый генератор может работать на частотах до 2 ГГц при использовании транзисторов типов КТ386, КТ3101, КТ3124 и им подобных и при изменении конструкции контурных катушек.

Радиопередатчик с ЧМ в УКВ-диапазоне частот 61—73 МГц

Радиопередатчик (рис. 2.31) представляет собой однокаскадный УКВ ЧМ-передатчик, работающий в вещательном диапазоне частот 61—73 МГц. Выходная мощность передатчика при использовании источника питания с напряжением 9—12 В — примерно 20 мВт. Он обеспечивает дальность передачи информации около 150 м при использовании приемника с чувствительностью 10 мкВ.

Режимы транзисторов УЗЧ (*VT1*) и ВЧ-генератора (*VT2*) по постоянному току задаются резисторами *R3* и *R4* соответственно. Напряжение 1,2 В на них и на питании микрофона *M1* подается с параметрического стабилизатора на *R1*, *C1, VD1*. Поэтому устройство сохраняет свою работоспособность при снижении напряжения питания до 4—5 В. При этом наблюдается уменьшение выходной мощности устройства, а несущая частота изменяется незначительно.

Модулирующий усилитель выполнен на транзисторе *VT1* типа КТ315. Напряжение звуковой частоты на его вход поступает с электретного микрофона с усилителем *M1* типа МКЭ-3 и ему подобным. Усиленное напряжение звуко-

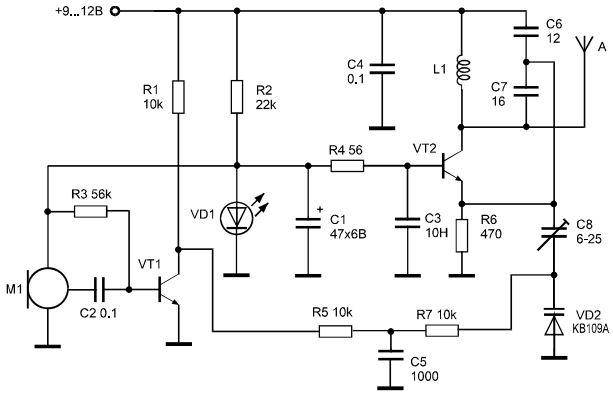


Рис. 2.31. Принципиальная схема радиопередатчика УКВ-диапазона

вой частоты с коллектора транзистора *VT1* поступает на варикап *VD2* типа КВ109А через фильтр нижних частот на резистор *R5,* конденсатор *C5* и резистор *R7*. Варикап *VD1* включен последовательно с подстроечным конденсатором *C8* в эмиттерную цепь транзистора *VT2*. Частота колебаний задающего генератора, выполненного на транзисторе *VT2* типа КТ315 (КТ3102, КТ368), определяется элементами контура *L1*, *C6*, *C7* и емкостью *C8* и *VD1*.

Вместо светодиода *VD1* типа АЛ307 можно использовать любой другой светодиод или три последовательно включенных в прямом направлении диода типа КД522 и им подобных. Катушка *L1* бескаркасная, диаметром 8 мм, имеет 6 витков провода ПЭВ 0,8.

При налаживании передатчик настраивают на свободный участок УКВ ЧМ-диапазона сжатием или растяжением витков катушки *L1* или подстройкой конденсатора *C8*. Девиация частоты устанавливается конденсатором *C8* по наиболее качественному приему на контрольный приемник. Передатчик можно настроить и на вещательный диапазон УКВ ЧМ (88—108 МГц), для этого необходимо уменьшить количество витков *L1* до 5 и емкость конденсаторов *C6* и *C7* до 10 пФ. В качестве антенны используется отрезок провода длиной 60 см. Для уменьшения влияния дестабилизирующих факторов антенну можно подключить через конденсатор емкостью 1—2 пФ.

Радиопередатчик с ЧМ в диапазоне частот 100—108 МГц

Дальность приема сигнала этого радиомикрофона (рис. 2.32) составляет около 50 м. Питание устройства осуществляется от источника питания от 1,5 до 9 В.

Передатчик состоит из однокаскадного усилителя звуковой частоты и однокаскадного генератора высокой частоты. Задающий генератор собран по распространенной схеме. Частота несущей определяется элементами *C4*, *L1*, *C5* и межэлектродными емкостями транзистора *VT2*. Модулирую-

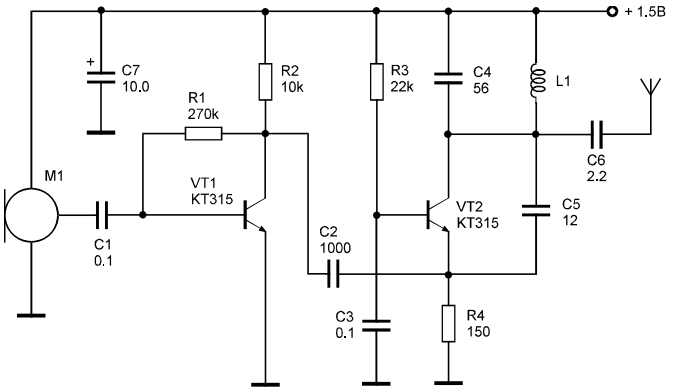


Рис. 2.32. Принципиальная схема радиопередатчика с частотной модуляцией

щий усилитель выполнен на транзисторе *VT1* типа КТ315. Усиленный сигнал через конденсатор *C2* поступает на эмиттер транзистора *VT2* типа КТ315. Модулирующее напряжение вызывает изменение емкости перехода «база — эмиттер» транзистора *VT2* и тем самым осуществляет частотную модуляцию задающего генератора. Сигнал с генератора через конденсатор *C6* поступает в антенну, в качестве которой используется отрезок провода длиной 10—40 см.

Катушка *L1* бескаркасная, намотана на оправке диаметром 3 мм и содержит 4 витка провода ПЭВ 0,6, шаг намотки — 2 мм.

Настройка радиомикрофона заключается в сжатии или растяжении витков катушки *L1* для приема сигнала в свободном от вещательных станций участке УКВ-диапазона вещательного приемника.

Радиопередатчик с питанием от сети 220 В

Устройство (рис. 2.33) работает в диапазоне 27—30 МГц с амплитудной модуляцией несущей частоты. Его основное достоинство заключается в том, что оно питается от электросети. Эту же сеть оно использует для излучения сигнала высокой частоты. Приемник принимает сигнал, используя телескопическую антенну или специальный сетевой адаптер.

Задающий генератор собран на транзисторе *VT2* типа КТ315 по традиционной схеме. Для питания микрофона *M1* применен параметрический стабилизатор напряжения, собранный на резисторе *R1* и светодиоде *VD1*, включенном в прямом направлении, на аноде которого поддерживается напряжение 1,2—1,4 В. На транзисторе *VT1* типа КТ315 собран УЗЧ, сигнал с которого модулирует по амплитуде задающий генератор. Постоянное напряжение на коллекторе транзистора *VT1* является напряжением смещения для транзистора *VT2*. Промодулированный ВЧ-сигнал с катушки связи *L2* через конденсатор *C9* поступает в электросеть. В данном случае провода электросети вы-

Рис. 2.33. Принципиальная схема радиопередатчика с питанием от сети 220 В

полняют роль антенны. Источник питания собран по бестрансформаторной схеме. Дроссель *Др1* предотвращает проникновение ВЧ-колебаний в источник питания. На реактивном сопротивлении конденсатора *С8* гасится излишек сетевого напряжения. В отличие от резистора конденсатор не нагревается и не выделяет тепло, что благоприятно сказывается на режиме работы устройства. Выпрямитель собран на диодах *VD3*, *VD4*. Конденсатор *С7* сглаживает пульсации выпрямленного напряжения. Далее напряжение через параметрический стабилизатор, собранный на резисторе *R5* и стабилитроне *VD2*, поступает для питания радиомикрофона.

Конденсатор *С6* уменьшает пульсации выпрямленного напряжения. Такой блок питания обеспечивает стабильную работу радиомикрофона при изменениях сетевого напряжения в интервале от 80 до 260 В.

Микрофон *М1* — любой малогабаритный конденсаторный микрофон со встроенным усилителем (МКЭ-3, М1-Б, «Сосна» и др.). Конденсаторы *С8* и С9 должны быть рассчитаны на рабочее напряжение не менее 250 В. Дроссель *Др1* — типа ДПМ-0,1 номиналом 50—90 мкГн. Дроссель *Др1* может быть изготовлен самостоятельно. Он содержит 100—150 витков провода ПЭВ 0,1 на стандартном ферритовом сердечнике диаметром 2,8 мм и длиной 14 мм (длина сердечника может быть уменьшена в 2 раза). Катушки *L1* и *L2* намотаны на стандартных ферритовых стержнях диаметром 2,8 мм и длиной 14 мм проводом ПЭВ 0,23. Катушка *L1* — 14 витков, *L2* — 3 витка поверх *L1*. Транзистор *VT2* может быть заменен на КТ3102 или КТ368. Светодиод *VD1* — на любой светодиод. Диоды *VD3*, *VD4* заменяются на КД105 или другие на напряжение не ниже 300 В. Конденсаторы *С6* и *С7* могут быть большей емкости и на большее рабочее напряжение, они должны иметь минимальную утечку. Стабилитрон *VD1* может быть заменен на любой стабилитрон с напряжением стабилизации 8—12 В.

Схема сетевого адаптера представлена на рис. 2.34. Конденсатор *С1* исключает проникновение напряжения сети в катушку *L1* и на вход используемого приемника. Катушки *L2*, *L3, L4* и конденсаторы *С2, С3*, *С4* образуют двухконтурный ФСС. С катушки *L4* отфильтрованный сигнал поступает на вход приемника.

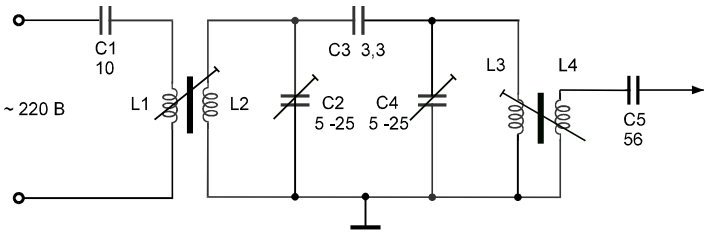


Рис. 2.34. Принципиальная схема сетевого адаптера

Катушки *L1*, *L2*, *L3*, *L4* намотаны на каркасах от КВ-катушек переносных радиоприемников. Катушка *L1* имеет 2 витка, *L2*, *L3* — по 14 витков, *L4* — 5 витков. Все катушки намотаны проводом ПЭВ 0,23. Конденсатор *C1* — на напряжение не ниже 250 В, конденсаторы *C2* и *C4* — подстроечные.

Настройку устройства следует начинать с проверки напряжения питания. Для этого необходимо сделать разрыв в точке *A*. Напряжение на конденсаторе *C6* должно быть 9 В. Если напряжение отличается от указанного, следует проверить исправность элементов блока питания *Др1, C8*, *VD3*, *VD4*, *C7*, *R5*, *VD2*, *C6*.

При исправном блоке питания следует восстановить соединение в точке *A* и подбором сопротивления резистора *R2* установить напряжение на базе транзистора *VT2* равным 3,5 В. Дальнейшая настройка сводится к установке несущей частоты подстройкой контура перемещением сердечника катушек *L1*, *L2*. Настроенную схему нужно залить эпоксидной смолой, предварительно отгородив микрофон. Настройка адаптера сводится к настройке контуров *L2*, *C2* и *L3*, *C4* на частоту передатчика.

ВНИМАНИЕ! При настройке и эксплуатации устройств с бестрансформаторным питанием от сети переменного тока необходимо соблюдать правила и меры безопасности, так как элементы устройств находятся под напряжением 220 В.

Радиопередатчик с ЧМ в диапазоне частот 1—30 МГц

Для питания радиопередатчика (рис. 2.35) используется силовая электросеть 220 В. Она же используется устройством в качестве антенны.

Блок питания устройства собран по бестрансформаторной схеме. Напряжение сети 220 В поступает на дроссели *Др1, Др2* и гасящий конденсатор *C2*, на котором гасится излишек напряжения. Переменное напряжение выпрямляется мостом *VD1*, нагрузкой которого является стабилитрон *VD2* типа КС510. Пульсации напряжения сглаживаются конденсатором *C3*.

Модулирующий усилитель выполнен на транзисторе *VT1* типа КТ315. Сигнал звуковой частоты поступает на базу этого транзистора с электретного микрофона с усилителем *M1* типа МКЭ-3 или М1-Б2 «Сосна». Усиленное напряжение звуковой частоты через резистор *R2* поступает на варикап *VD3* типа

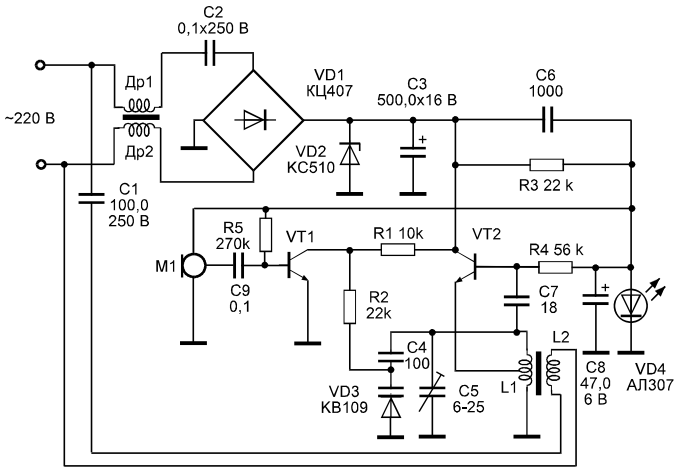


Рис. 2.35. Принципиальная схема радиопередатчика с ЧМ в диапазоне частот 1—30 МГц

КВ109А, изменение емкости которого позволяет осуществлять частотную модуляцию.

Задающий генератор выполнен по схеме индуктивной трехточки на транзисторе *VT2* типа КТ315. Частота генератора определяется элементами колебательного контура *L1*, *C5*, *C4*, *VD3*. Обратная связь осуществляется через конденсатор *C7*.

Режимы транзисторов *VT1* и *VT2* по постоянному току регулируются резисторами *R5* и *R4* соответственно. Напряжения смещения транзисторов *VT1* и *VT2* формируется этими резисторами и параметрическим стабилизатором, выполненным на резисторе *R3*, светодиоде *VD1* типа АЛ307 и конденсаторе *C8*. Этим достигается более высокая стабильность частоты, чем при обычном включении.

Напряжение высокой частоты, промодулированное по частоте звуковым сигналом, с катушки связи *L2* поступает в сеть 220 В через разделительный конденсатор *C1*. Конденсатор *C1* уменьшает влияние напряжения сети на задающий генератор. Дроссели *Др1* и *Др2* исключают проникновение напряжения высокой частоты по цепям питания.

Дроссели *Др1* и *Др2* намотаны на ферритовых стержнях и содержат по 100 витков провода ПЭВ 0,1 каждый. Катушки *L1* и *L2* намотаны на каркасе диаметром 5 мм с подстроечным сердечником. Для диапазона 27 МГц катушка *L1* имеет 10 витков с отводом от середины, намотанных проводом ПЭВ 0,3. Катушка связи *L2* имеет 2 витка того же провода.

Конденсаторы *C1* и *C2* должны быть рассчитаны на рабочее напряжение не ниже 250 В. Диодная сборка КЦ407 может быть заменена на четыре диода КД105, КД102. Вместо стабилитрона *VD2* можно использовать любой другой с напряжением стабилизации 8—2 В. Светодиод *VD4* типа АЛ307 можно заменить на любой светодиод или на два-три кремневых диода, включенных в прямом направлении.

При использовании кондиционных деталей и правильном монтаже настройка заключается в подстройке частоты задающего генератора конденсатором *C5*.

Технические средства обнаружения и подавления радиомикрофонов

Существует достаточно много различных приборов для поиска и обнаружения радиомикрофонов. Однако в силу различных причин (цена, неудобство использования, большие габариты и т. д.) практическое применение нашли далеко не все.

Радиомикрофоны в отличие от других устройств съема информации имеют один ярко выраженный демаскирующий признак — электромагнитное излучение. Ведь радиомикрофон — это миниатюрный радиопередатчик, а любой передатчик, как известно, излучает в окружающее пространство электромагнитную энергию. Именно поэтому мы остановимся на рассмотрении приборов, основанных на исследовании электромагнитного излучения и представленных на российском рынке специальной техники. Прежде всего это такие устройства поиска, как индикаторы (детекторы), частотомеры, приемники-сканеры, анализаторы спектра и т. д. Кроме них существуют специальные комплексы для автоматического обнаружения и подавления радиомикрофонов и нелинейные локаторы, о которых мы расскажем ниже.

Для того чтобы проверить свою квартиру или офис на наличие каких-либо радиотехнических средств, установленных у вас несанкционированно, или убедиться в том, что ваш телефон, компьютер, телевизор и другая бытовая техника не имеют побочных, а значит, нежелательных каналов излучения в радиочастотном диапазоне, совсем необязательно обращаться к специалистам. Эту работу можно выполнить и самостоятельно, достаточно иметь небольшой прибор — регистратор ВЧ-излучений или сканер-обнаружитель. Такие приборы широко представлены в торговых организациях и на радиорынках.

Регистратор ВЧ-излучений представляет собой сканирующий приемник— обнаружитель сигналов маломощных передатчиков с реализацией алгоритма распознавания и селекции сигналов мощных станций радио- и телевизионного вещания, а также связных станций различных служб. Сканер предназначен для обнаружения и локализации места установки акустических, телефонных и телевизионных миниатюрных передатчиков отечественного и зарубежного производства, проверки предметов, которые подозреваются на наличие установленных закамуфлированных микропередатчиков. Наличие возможности автоматического распознавания связных и вещательных станций позволяет максимально повысить относительную чувствительность сканера, что, в свою очередь, позволяет увеличить надежность обнаружения подслушивающих устройств. Небольшие габариты, автономное питание и возможность изменения чувствительности позволяют проводить поисковые мероприятия в максимально сжатые сроки и с высокой надежностью.

Индикаторы (детекторы) электромагнитного поля

Индикатор электромагнитного поля D-006

Предназначен для оперативного обнаружения радиоизлучающих подслушивающих устройств (рис. 2.36). Принцип действия прибора основан на широкополосном детектировании электрического поля, что позволяет обнаруживать излучающие устройства при любом виде модуляции. Радиус обнаружения устройств зависит от излучаемой ими мощности. Он примерно равен 1 м при мощности излучения передатчика 5 мВт. Наличие в приборе аттенюатора позволяет работать с детектором в условиях сложной электромагнитной обстановки, за счет ослабления входного сигнала, и обеспечивает возможность точной локализации радиопередающих устройств. Наличие системы акустической обратной связи позволяет исключить ложные срабатывания детектора и идентифицировать радиопередающие устройства по характерному звуковому сигналу. Восьмисегментная логарифмическая светодиодная шкала и тональный звуковой сигнал обеспечивают наглядность и удобство при работе с прибором.

Основные технические характеристики

Диапазон рабочих частот, МГц ..... 50—1000
Чувствительность, мВ, при *f*:
110 МГц 0,5
800 МГц 3
Динамический диапазон индикатора, дБ ..... –40
Напряжение питания, В 9
Потребляемый ток, мА 30
Габариты (без блока питания), мм ..... 128×63×20

В комплект поставки входят: сам детектор, штатная антенна (ее замена не рекомендуется!!!), зарядное устройство от сети 220 В и руководство по эксплуатации.

Индикатор электромагнитного поля и проверки проводных линий D-008

В отличие от модели D-006 он обладает возможностью проверки проводных линий (силовых — 380/220 В, телефонных, сигнализации) на наличие подслушивающих устройств и позволяет в конкретной обстановке выявить их и локализовать (рис. 2.37).

Индикатор D-008 имеет 2 канала обнаружения:

- радиодетектор для поиска радиопередающих устройств;

- анализатор проводных линий для поиска радиопередающих устройств, использующих для передачи информации проводные линии.

Принцип действия прибора в первом режиме основан на широкополосном детектировании электрического поля, что дает возможность регистрировать радиопередающие устройства независимо от вида модуляции. Радиус обнаружения детектора зависит от излучаемой мощности, частоты, на которой работает радиопередающее устройство, электромагнитной обстановки в обследуемом помещении и составляет при мощности передатчика 5 мВт примерно 1 м.

Аттенюатор, за счет ослабления входного сигнала, позволяет проводить измерения в условиях сложной электромагнитной обстановки, присущей крупным промышленным центрам. Данный режим полезен и при локализации мощных радиопередающих устройств.

Активная антенна облегчит обнаружение передатчиков с частотой передачи выше 400 МГц.

Наличие системы акустической обратной связи в приборе позволяет исключить ложные срабатывания детектора на локальные электромагнитные поля и идентифицировать находящиеся в помещении радиопередающие устройства по характерному звуковому сигналу.

Десятисегментная логарифмическая светодиодная шкала и звуковой сигнал с меняющейся частотой тона обеспечивают наглядность и удобство при работе с прибором.

Рис. 2.36. Индикатор электромагнитного поля D-006

Рис. 2.37. Индикатор электромагнитного поля и проверки проводных линий D-008

Анализатор проводных линий состоит из внешнего проводного адаптера, обеспечивающего подключение к линиям с напряжением до 500 В, и собственно приемника. Контроль звуковой информации осуществляется посредством головных телефонов либо через встроенный громкоговоритель, причем как АМ-, так и ЧМ-сигналов.

Перестройка по частотному диапазону осуществляется регулятором, расположенным на верхней крышке прибора, с одновременным указанием относительного значения частоты на индикаторе.

Основные технические характеристики

Питание, В 9
Потребляемый ток, мА: .....
дежурный режим радиодетектора 20
дежурный режим анализатора проводных линий 30
рабочий режим ..... до 100
Габариты основного блока, мм ..... 148×68×24
Диапазон частот радиодетектора, МГц ..... 50—1500
Чувствительность по входу, мВ, при *f*: .....
100—400 МГц 2
800 МГц 1,5
1500 МГц 6
Ослабление аттенюатора, дБ 20
Диапазон частот активной антенны, МГц ..... 400—1500
Усиление активной антенны, дБ ..... не менее 4
Динамический диапазон индикатора, дБ 20
Диапазон частот анализатора проводных линий, МГц: .....
нижняя граница ..... не более 0,05
верхняя граница ..... не менее 7
Чувствительность при отношении сигнал/шум 20 дБ,
глубине АМ 30 %, мВ 4
Полоса пропускания, кГц 200
Вид модуляции ..... АМ, ЧМ
Максимальное входное напряжение проводного
адаптера, В 500

Многофункциональный приемник широкого диапазона XPLORER

Многофункциональный тестовый и исследовательский приемник ближнего поля XPLORER (рис. 2.38) имеет оптимально подобранную максимальную чувствительность для обнаружения и приема сигнала на расстоянии большем, чем у аналогов (носимая радиостанция — до 400 м).

Рис. 2.38. Многофункциональный приемник XPLORER

Малые габариты, вес, автономная работа от встроенных аккумуляторов в течение 8 ч и широкие функциональные возможности открывают для этого прибора широчайшую сферу применения: тестирование радиопередающего оборудования, исследования радиосигналов, поиск радиопередатчиков и многое другое.

XPLORER проверяет диапазон от 30 МГц до 2 ГГц менее чем за 1 с и позволяет автоматически обнаруживать активные передатчики в ближней зоне, демодулировать ЧМ-сигналы и воспроизводить звук через встроенный громкоговоритель. Приемник имеет двухстрочный дисплей, в одной строке которого отображается частота принятого сигнала, а во второй — одна из характеристик сигнала: значение тона или кода CTCSS, DCS или DTMF, относительный уровень, ЧМ-девиация (1—10; 10—100 кГц), параметры LTR-транкинга, а также широта и долгота в координатах системы GPS. Для удобства работы предусмотрены функции ручного сброса обнаруженной частоты, память на 500 значений частот. В память регистра обнаруженных частот автоматически вносятся не только значение частоты обнаруженного сигнала, но и время, дата, долгота и широта. Прибор имеет встроенные часы с собственной батарейкой и последовательный интерфейс RS-232C. Прибор оборудован гнездом для подключения головных телефонов, а также имеет гнездо управления магнитофоном.

Основные технические характеристики

Диапазон рабочих частот, ГГц ..... 0,030—2
Модуляция:
- тип ..... ЧМ
- девиация не более, кГц 100

Диапазон звуковых частот, кГц ..... 50—3000
Время сканирования всего диапазона частот, с ..... не более 1
Вход:
- сопротивление, Ом 50
- чувствительность на частоте 100 МГц, дБм ..... –59
- чувствительность на частоте 1 ГГц, дБм ..... –25

Индикация ..... захват сигнала; зарядка аккумулятора
Дисплей:
- количество строк 2
- количество символов в строке ..... 16 с подсветкой

Питание:
встроенный никель-кадмиевый аккумулятор, В/мА·ч 7,2/850
универсальный адаптер, В/А 12/2
Последовательный порт ..... CI-V (ТТЛ), RS-232C

Счетчик частоты CUB

Минисчетчик частоты CUB — идеальное средство для поиска активных передатчиков (рис. 2.39).

Данный прибор производства фирмы Optoelectronics является усовершенствованной версией предыдущей модели 3300 MiniCounter, одного из самых популярных и дешевых приборов для измерений и тестирования радиооборудования.

Новый CUB имеет цифровой фильтр и функцию автозахвата. При использовании цифрового фильтра внутренний микропроцессор оценивает полученные результаты и игнорирует случайные результаты измерения, так что при работе на дисплее появляются не случайные числа, а реально измеренные величины. Функция автозахвата удерживает на дисплее значение настолько долго, насколько вам это понадобится, — может пройти несколько дней до тех пор, пока полученное значение будет записано на бумаге.

Прибор имеет высокоскоростной вход 0,001 с и 8 переключаемых значений скорости счета, что делает его более быстрым и точным по сравнению с моделью 3300, имеющей стандартные значения этих параметров: 0,01 с и 6 скоростей счета. Optoelectronics CUB стал более сложным в схемотехническом отношении, но остался таким же простым в управлении, как и его предшественник.

Имея встроенные никель-кадмиевые аккумуляторы, CUB может работать 10 ч без подзарядки, предоставляя вам полную свободу действий. Вы можете практически целый день работать с прибором, будь вы в чистом поле или лаборатории.

Стоит особенно остановиться на чувствительности прибора. При усовершенствовании счетчика модели 3300 была использована так называемая концепция максимальной чувствительности, поэтому CUB имеет предельное для широкодиапазонного прибора значение чувствительности, при котором еще не происходит его самовозбуждения, что дает возможность максимально расширить диапазон частот принимаемых сигналов и дальность их обнаружения. Поэтому в приборе не предусмотрены какие-либо регулировки чувствительности или коэффициента усиления.

Рис. 2.39. Счетчик частоты CUB

Основные технические характеристики

Диапазон рабочих частот, ГГц ..... 0,001—2,8
Входное сопротивление, Ом 50
Максимальный входной сигнал, дБм (мВ) 15 (50)
Частота опорного генератора, МГц 10
Дисплей:
тип ..... жидкокристаллический
организация ..... 9 цифр высотой 4,5 мм
Габариты, мм ..... 94×70×30
Корпус:
материал ..... штампованный алюминий
цвет ..... черный
Встроенные батареи:
тип ..... никель-кадмиевые
количество 4
размер ..... AA
время непрерывной работы, ч 10
Питание:
напряжение, В ..... 9—11
потребляемый ток, мА 110

Тестовый ЧМ-приемник R10 INTERCEPTOR

Мощным средством для обнаружения подслушивающих устройств и перехвата радиопереговоров в ближней зоне является приемник R10 INTERCEPTOR фирмы Optoelectronics (рис. 2.40).

R10 измеряет девиацию сигналов (с широкой и узкой полосой), относительную величину сигнала, а в сочетании с декодером DC440 позволяет измерять сигнальные тоны (CTCSS, DCS и DTMF). R10 может использоваться для любых измерений, требующих ЧМ-демодуляции, и подходит для проверки передатчиков метрового диапазона и сотовой связи, а в некоторых случаях может служить дешевой, малогабаритной заменой для сервисного монитора.

В отличие от приемников и сканеров R10 принимает любые имеющиеся сильные сигналы. Настройка обычных приемников стабилизирована на определенной частоте с помощью внутреннего генератора. Приемник R10 настраивается по принимаемому сигналу. Достоинством этого является то, что для приема сигнала прибор не нужно настраивать на конкретную частоту, он может принимать любой ЧМ-сигнал в диапазоне от 30 МГц до 2 ГГц. R10 работает автоматически и не требует вмешательства оператора.

Лучше всего приемник работает в близлежащей от передатчика зоне, где напряженность электромагнитного поля высока, но быстро падает с увеличением расстояния. В дальней же зоне напряженность поля мала, но сохраняется практически неизменной на огромных расстояниях.

Рис. 2.40. Тестовый приемник R10 INTERCEPTOR

Реальное расстояние, на котором приемник может детектировать радиопередатчик, зависит от фонового радиоизлучения в конкретной области и наличия других сильных сигналов. Проверки показали, что типовыми являются значения 6—250 м от передатчика МВ или ДМВ мощностью 5 Вт. Таким образом, R10 является одним из самых чувствительных приборов для работы в ближней зоне. Это возможно благодаря его отличной чувствительности. Индикатор величины сигнала может служить для обнаружения местоположения скрытых передатчиков или подслушивающих устройств, установленных в комнате или автомобиле.

В отличие от сканеров и приемников, которые должны быть настроены на определенную частоту или должны сканировать заданный диапазон частот, с помощью R10 можно прослушивать близлежащие переговоры по ЧМ-связи благодаря немедленному приему сильных сигналов независимо от их частоты.

Основные технические характеристики

Диапазон рабочих частот, МГц ..... 30—2000
Модуляция:
- вид ..... ЧМ
- девиация, кГц 100

Диапазон звуковых частот, Гц ..... 50—3000
Время настройки, с, ... не более 1
Вход:
- сопротивление, Ом 50
- чувствительность на частоте 100 МГц, дБм 45
- чувствительность на частоте 1 ГГц, дБм 20

Максимальная чувствительность, дБм 15
Питание:
- тип ..... встроенный блок никель-кадмиевый аккумуляторов
- напряжение, В 7,2
- емкость, мА·ч 600
- время непрерывной работы, ч 5

Корпус:
- материал ..... штампованный алюминий
- цвет ..... черный

Габариты, мм ..... 130×70×38

Индикаторы электромагнитного излучения самостоятельного изготовления

Промышленные приборы обнаружения радиозакладок, кратко рассмотренные выше, стоят достаточно дорого (800—1500 USD) и могут оказаться не каждому по карману. В принципе использование специальных средств оправдано лишь тогда, когда специфика вашей деятельности может привлечь внимание конкурентов или криминальных группировок и утечка информации может привести к фатальным последствиям для вашего бизнеса и даже здоровья. Во всех остальных случаях опасаться профессионалов промышленного шпионажа не приходится и нет необходимости тратить огромные средства на специальную аппаратуру. Большинство ситуаций может свестись к банальному подслушиванию разговоров начальника, неверного супруга или соседа по даче. При этом, как правило, используются радиозакладки кустарного производства, обнаружить которые можно более простыми средствами — индикаторами радиоизлучений. Изготовить эти приборы без труда можно самостоятельно. В отличие от сканеров индикаторы радиоизлучений регистрируют напряженность электромагнитного поля в конкретном диапазоне длин волн. Чувствительность их невысока, поэтому обнаружить источник радиоизлучения они могут только в непосредственной близости от него. Низкая чувствительность индикаторов напряженности поля имеет и свои положительные стороны — существенно уменьшается влияние мощных радиовещательных и других промышленных сигналов на качество обнаружения. Ниже мы рассмотрим несколько простых индикаторов напряженности электромагнитного поля КВ-, УКВ- и СВЧ-диапазонов.

Простейшие индикаторы напряженности электромагнитного поля

Рассмотрим простейший индикатор напряженности электромагнитного поля в диапазоне 27 МГц. Принципиальная схема прибора приведена на рис. 2.41. Он состоит из антенны, колебательного контура *L1C1*, диода *VD1*, конденсатора *C2* и измерительного прибора.

Работает устройство следующим образом. Через антенну на колебательный контур поступают ВЧ-колебания. Контур отфильтровывает колебания диапазона 27 МГц из смеси частот. Выделенные ВЧ-колебания детектируются диодом *VD1*, благодаря чему на выход диода проходят только положительные полуволны принимаемых частот. Огибающая этих частот представляет собой НЧ-колебания. Остатки ВЧ-колебаний фильтруются конденсатором *C2*. При этом через измерительный прибор потечет ток, который содержит переменную и постоянную составляющие. Измеряемый прибором постоянный ток примерно пропорционален напряженности поля, действующей в месте приема. Этот детектор можно выполнить в виде приставки к любому тестеру.

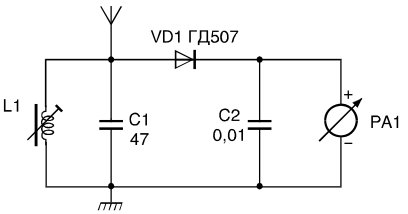


Рис. 2.41. Принципиальная схема простейшего индикатора поля

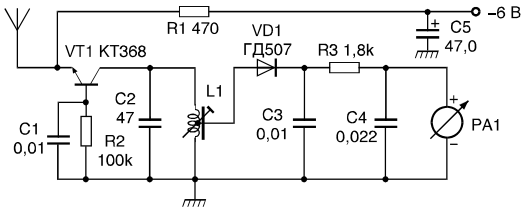


Рис. 2.42. Принципиальная схема индикатора с ВЧ-усилителем

Катушка *L1* диаметром 7 мм с подстроечным сердечником имеет 10 витков провода ПЭВ-1 0,5. Антенна выполнена из стальной проволоки длиной 50 см.

Чувствительность прибора можно значительно повысить, если перед детектором установить ВЧ-усилитель. Принципиальная схема такого устройства представлена на рис. 2.42. Эта схема по сравнению с предыдущей имеет более высокую чувствительность передатчика. Теперь излучение может быть зафиксировано на расстоянии нескольких метров.

Высокочастотный транзистор *VT1* включен по схеме с общей базой и работает в качестве селективного усилителя. Колебательный контур *L1C2* включен в его коллекторную цепь. Связь контура с детектором осуществляется через отвод от катушки *L1*. Конденсатор *C3* отфильтровывает ВЧ-составляющие. Резистор *R3* и конденсатор *C4* выполняют функцию НЧ-фильтра.

Катушка *L1* намотана на каркасе с подстроечным сердечником диаметром 7 мм проводом ПЭВ-1 0,5. Антенна выполнена из стальной проволоки длиной около 1 м.

Для ВЧ-диапазона 430 МГц можно также собрать очень простую конструкцию индикатора напряженности поля. Принципиальная схема такого прибора приведена на рис. 2.43, *а*. Индикатор, схема которого показана на рис. 2.43, *б,* позволяет определить направление на источник излучения.

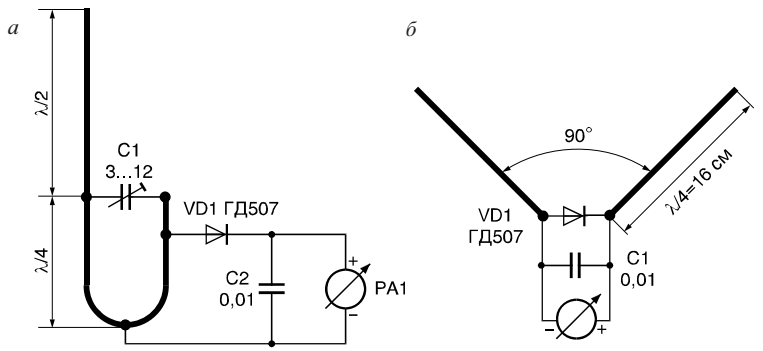


Рис. 2.43. Принципиальные схемы индикаторов диапазона 430 МГц

Индикатор напряженности поля диапазона 1—200 МГц

Проверить помещение на наличие подслушивающих устройств с радиопередатчиком можно при помощи несложного широкополосного индикатора напряженности поля со звуковым генератором. Дело в том, что некоторые сложные «жучки» с радиопередатчиком включаются на передачу только тогда, когда в помещении раздаются звуковые сигналы. Такие устройства трудно обнаружить при помощи обычного индикатора напряженности, нужно постоянно разговаривать или включить магнитофон. Рассматриваемый детектор имеет собственный источник звукового сигнала.

Принципиальная схема индикатора показана на рис. 2.44. В качестве поискового элемента использована объемная катушка *L1*. Ее достоинство, по сравнению с обычной штыревой антенной, заключается в более точной индикации места установки передатчика. Сигнал, наведенный в этой катушке, усиливается двухкаскадным ВЧ-усилителем на транзисторах *VT1, VT2* и выпрямляется диодами *VD1*, *VD2.* По наличию постоянного напряжения и его величине на конденсаторе *C4* (в режиме милливольтметра работает микроамперметр М476-Р1) можно определить наличие передатчика и его местоположение.

Комплект съемных катушек *L1* позволяет находить передатчики различной мощности и частоты в диапазоне от 1 до 200 МГц.

Генератор звука состоит из двух мультивибраторов. Первый, настроенный на частоту 10 Гц, управляет вторым, настроенным на частоту 600 Гц, в ре-

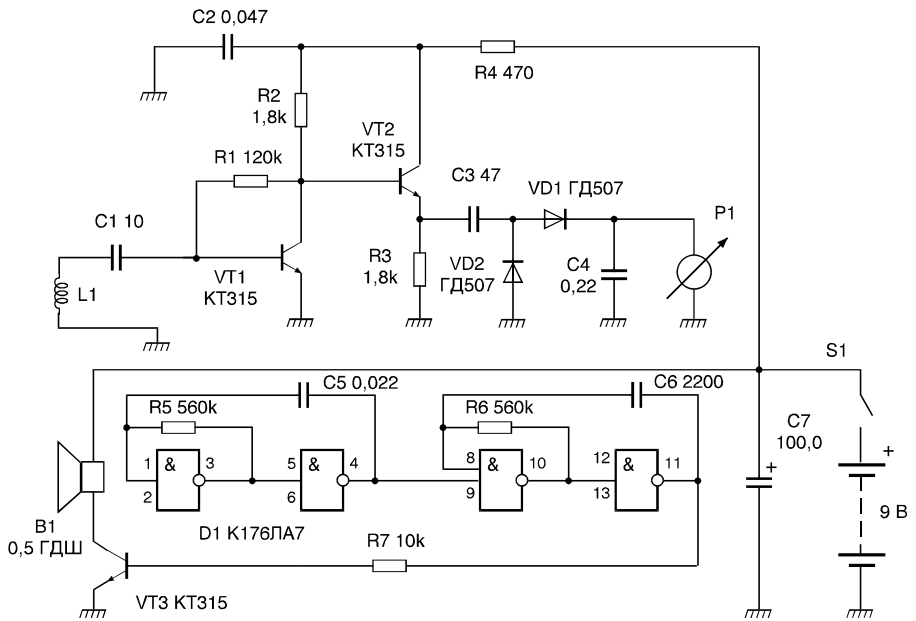


Рис. 2.44. Принципиальная схема индикатора напряженности поля диапазона 1—200 МГц

зультате чего формируются пачки импульсов, следующие с частотой 10 Гц. Эти пачки импульсов поступают на транзисторный ключ *VT3,* в коллекторной цепи которого включена динамическая головка *B1,* размещенная в направленном боксе (пластмассовая труба длиной 200 мм и диаметром 60 мм).

Для более удачных поисков желательно иметь несколько катушек *L1*. Для диапазона до 10 МГц катушку *L1* нужно намотать проводом ПЭВ 0,31 на пустотелой оправке из пластмассы или картона диаметром 60 мм, всего — 10 витков; для диапазона 10—100 МГц каркас не нужен, катушка наматывается проводом ПЭВ 0,6...1 мм, диаметр объемной намотки — около 100 мм, количество витков — 3—5; для диапазона 100—200 МГц конструкция катушки такая же, но она имеет всего один виток.

Для работы с мощными передатчиками можно использовать катушки меньшего диаметра.

Заменив транзисторы *VT1*, *VT2* на более высокочастотные, например КТ368 или КТ3101, можно поднять верхнюю границу частотного диапазона обнаружения детектора до 500 МГц.

Индикатор напряженности поля диапазона 0,95—1,7 ГГц

В последнее время в составе радиозакладок все чаще используются передающие устройства сверхвысокочастотного (СВЧ) диапазона. Это обусловлено тем, что волны этого диапазона хорошо проходят через кирпичные и бетонные стены, а антенна передающего устройства имеет малые габариты при большой эффективности ее использования. Для обнаружения СВЧ-излучения радиопередающего устройства, установленного в вашей квартире, можно использовать прибор, схема которого приведена на рис. 2.45.

Основные характеристики

Диапазон рабочих частот, ГГц	0,95—1,7
Уровень входного сигнала, мВ	0,1—0,5
Коэффициент усиления СВЧ-сигнала, дБ	30—36
Входное сопротивление, Ом	75
Потребляемый ток, мА	не более 50
Напряжение питания, В	+9—20 В

Выходной СВЧ-сигнал с антенны поступает на входной разъем *XW1* детектора и усиливается СВЧ-усилителем на транзисторах *VT1—VT4* до уровня 3—7 мВ. Усилитель состоит из четырех одинаковых каскадов, которые выполнены на транзисторах, включенных по схеме с общим эмиттером, с резонансными связями. Линии *L1—L4* служат коллекторными нагрузками транзисторов и имеют индуктивное сопротивление 75 Ом на частоте 1,25 ГГц. Разделительные конденсаторы *C3*, *C7*, *C11,* имеют емкостное сопротивление 75 Ом на частоте 1,25 ГГц. Такое построение усилителя позволяет добиться максимального усиления каскадов, однако неравномерность коэффициента уси-

ления в рабочей полосе частот достигает 12 дБ. К коллектору транзистора *VT4* подключен амплитудный детектор на диоде *VD5* с фильтром *R18C17*. Продетектированный сигнал усиливается усилителем постоянного тока на микросхеме *DA1*. Его коэффициент усиления по напряжению равен 100. К выходу операционного усилителя подключен стрелочный индикатор, показывающий уровень выходного сигнала. Подстроечным резистором *R26* балансируют операционный усилитель так, чтобы компенсировать его начальное напряжение смещения и собственные шумы СВЧ-усилителя.

На микросхеме *DD1,* транзисторах *VT5*, *VT6* и диодах *VD3*, *VD4* собран преобразователь напряжения для питания операционного усилителя. На элементах *DD1.1, DD1.2* выполнен задающий генератор, вырабатывающий прямоугольные импульсы с частотой следования около 4 кГц. Транзисторы *VT5* и *VT6* обеспечивают усиление по мощности этих импульсов. На диодах *VD3*, *VD4* и конденсаторах *C13*, *C14* собран умножитель напряжения. В результате на конденсаторе *C14* формируется отрицательное напряжение 12 В при напряжении питания СВЧ-усилителя +15 В. Напряжения питания операционного усилителя стабилизированы на уровне 6,8 В стабилитронами *VD2* и *VD6*.

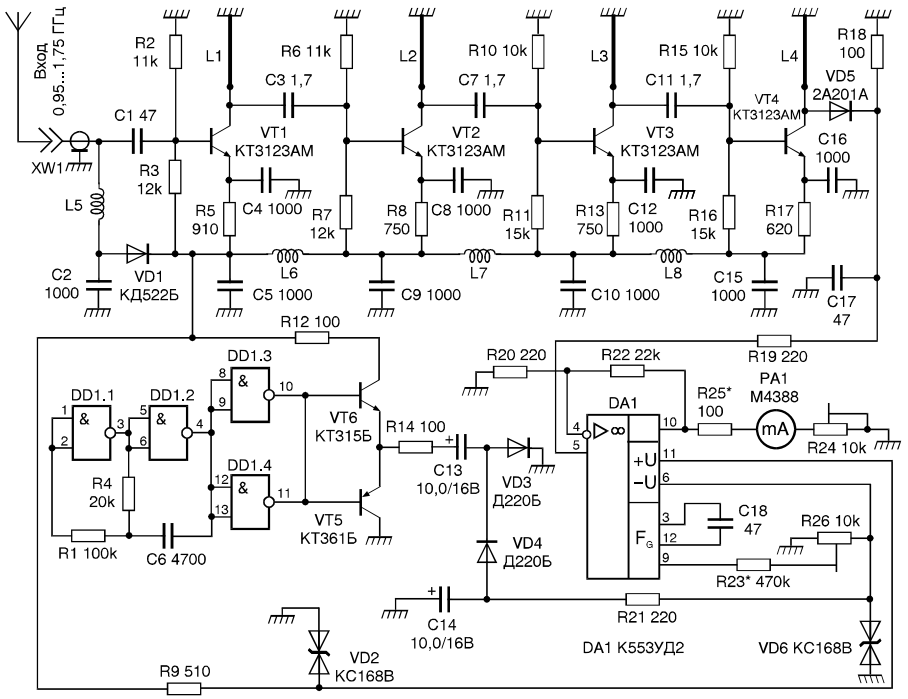


Рис. 2.45. Принципиальная схема индикатора напряженности поля диапазона 0,95—1,7 ГГц

Элементы индикатора размещены на печатной плате из двустороннего фольгированного стеклотекстолита толщиной 1,5 мм. Плата заключена в латунный экран, к которому припаяна по периметру. Элементы находятся со стороны печатных проводников, вторая, фольгированная, сторона платы служит общим проводом.

Линии *L1—L4* представляют собой отрезки медного посеребренного провода длиной 13 мм и диаметром 0,6 мм, которые впаяны в боковую стенку латунного экрана на высоте 2,5 мм над платой. Все дроссели — бескаркасные с внутренним диаметром 2 мм, намотаны проводом ПЭЛ 0,2. Отрезки провода для намотки имеют длину 80 мм. Входным разъемом *XW1* служит кабельный (75 Ом) разъем СГС.

В устройстве применены постоянные резисторы МЛТ и подстроечные СП5-1ВА, конденсаторы КД1 (*C4*, *C5*, С8—*C10, C12, C15, C16*) диаметром 5 мм с отпаянными выводами и КМ, КТ (остальные). Оксидные конденсаторы — К53. Электромагнитный индикатор с током полного отклонения 0,5—1 мА — от любого магнитофона.

Микросхему К561ЛА7 можно заменить на К176ЛА7, К1561ЛА7, К553УД2 — на К153УД2 или КР140УД6, КР140УД7. Стабилитроны — любые кремниевые с напряжением стабилизации 5,6—6,8 В (КС156Г, КС168А). Диод *VD5* 2А201А можно заменить на ДК-4В, 2А202А или ГИ401А, ГИ401Б.

Налаживание устройства начинают с проверки цепей питания. Временно отпаивают резисторы *R9* и *R21*. После подачи положительного напряжения питания +12 В измеряют напряжение на конденсаторе *C14*, которое должно быть не менее –10 В. В противном случае по осциллографу убеждаются в наличии переменного напряжения на выводах *4* и *10 (11)* микросхемы *DD1*. Если напряжение отсутствует, убеждаются в исправности микросхемы и правильности монтажа. Если переменное напряжение присутствует, проверяют исправность транзисторов *VT5*, *VT6*, диодов *VD3*, *VD4* и конденсаторов *C13*, *C14*.

После налаживания преобразователя напряжения припаивают резисторы *R9*, *R21* и проверяют напряжение на выходе операционного усилителя и подстройкой сопротивления резистора *R26* устанавливают нулевой уровень.

После этого на вход устройства подают сигнал напряжением 100 мкВ и частотой 1,25 ГГц с СВЧ-генератора. Резистором *R24* добиваются полного отклонения стрелки индикатора *PA1*.

Индикатор СВЧ-излучений

Прибор предназначен для поиска СВЧ-излучений и обнаружения маломощных СВЧ-передатчиков, выполненных, например, на диодах Ганна. Он перекрывает диапазон 8—12 ГГц.

Рассмотрим принцип работы индикатора. Простейшим приемником, как известно, является детекторный. И такие приемники диапазона СВЧ, состоящие из приемной антенны и диода, находят свое применение для измерения СВЧ-мощности. Самым существенным недостатком является низкая чувстви-

тельность таких приемников. Чтобы резко повысить чувствительность детектора, не усложняя СВЧ-головки, используется схема детекторного СВЧ-приемника с модулируемой задней стенкой волновода (рис. 2.46).

СВЧ-головка при этом почти не усложнилась, добавился только модуляторный диод *VD2*, а *VD1* остался детекторным.

С некоторым приближением можно считать, что когда диод *VD2* закрыт, он не влияет на процессы в волноводе, а когда открыт — полностью закорачивает волновод, т. е. играет роль короткозамкнутой задней стенки.

Рассмотрим процесс детектирования. СВЧ-сигнал, принятый рупорной (или любой другой, в нашем случае — диэлектрической) антенной, поступает в волновод. Поскольку задняя стенка волновода короткозамкнута, в волноводе устанавливается режим стоячих волн. Причем если детекторный диод будет находиться на расстоянии полуволны от задней стенки, он будет в узле (т. е. минимуме) поля, а если на расстоянии четверти волны — то в пучности (максимуме). То есть если мы будем электрически передвигать заднюю стенку волновода на четверть волны (подавая модулирующее напряжение с частотой 3 кГц на *VD2*), то на *VD1*, вследствие перемещения его с частотой 3 кГц из узла в пучность СВЧ-поля, выделится НЧ-сигнал с частотой 3 кГц, который может быть усилен и выделен обычным усилителем НЧ.

Таким образом, если на *VD2* подать прямоугольное модулирующее напряжение, то при попадании в СВЧ-поле с *VD1* будет снят продетектированный сигнал той же частоты. Этот сигнал будет противофазен модулирующему (это свойство с успехом будет использовано в дальнейшем для выделения полезного сигнала из наводок) и иметь очень малую амплитуду.

То есть вся обработка сигнала будет производиться на НЧ, без дефицитных СВЧ-деталей.

Схема обработки приведена на рис. 2.47. Питается схема от источника 12 В и потребляет ток около 10 мА.

Резистор *R3* обеспечивает начальное смещение детекторного диода *VD1*. Принятый диодом *VD1* сигнал усиливается трехкаскадным усилителем на транзисторах *VT1—VT3*. Для исключения помех питание входных цепей осуществляется через стабилизатор напряжения на транзисторе *VT4*.

На микросхеме *DD2* собран генератор импульсов частотой 3 кГц, которыми через резистор *R22* модулируется диод *VD2*. Модулирующее напряжение в прямой (вывод *8 DD2*) и инверсной (вывод *9 DD2*) фазах через *R8* поступает на резистор *R11* «Чувствительность». Этим резистором устанавливается такая фаза и амплитуда компенсирующего напряжения на движке *R11*, чтобы свести к нулю наводки на диод *VD1*. В самом деле, на *VD1*, так или иначе, будет наведено (че-

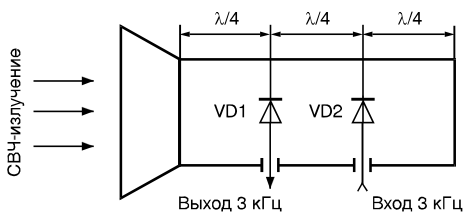


Рис 2.46. Принципиальная схема СВЧ-приемника с модулируемой задней стенкой волновода

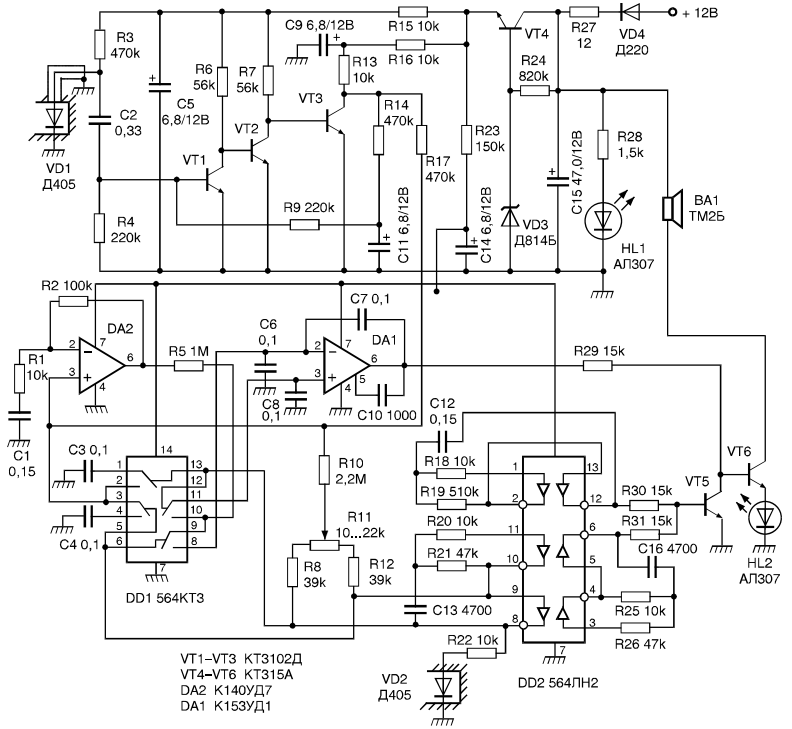


Рис. 2.47. Схема обработки СВЧ-сигнала

рез паразитные связи) модулирующее напряжение 3 кГц (все-таки на *VD2* почти 1 В, а полный сигнал снимается с *VD1* и имеет амплитуду 1 мкВ и менее). Но вспомним, что полезный сигнал (от СВЧ-поля) с диода *VD1* и модулирующее напряжение на диоде *VD2* противофазны. Именно поэтому движок *R11* можно установить в такое положение, при котором наводки будут подавлены. Подключите осциллограф к выходу операционного усилителя *DA2* и, вращая ползунок резистора *R11*, вы увидите, как происходит компенсация.

С выхода предварительного усилителя *VT1—VT3* сигнал поступает на выходной усилитель на микросхеме *DA2*. Обратите внимание на то, что между коллектором VT3 и входом DA2 стоит RC-цепочка *R17C3* (или *C4* в зависимости от состояния ключей *DD1*) с полосой пропускания всего 20 Гц (!). Это так называемый цифровой корреляционный фильтр. Мы знаем, что должны принять прямоугольный сигнал частотой 3 кГц, в точности равной модулирующей и в противофазе с модулирующим сигналом. Цифровой фильтр как раз и использует это знание — когда должен приниматься высокий уровень полезного сигнала, подключается конденсатор *C3*, а когда низкий — *C4*. Таким образом, на *C3* и *C4* за несколько периодов накапливаются верхнее и нижнее значения полезного сигнала, в то время как шумы со случайной фазой отфильтровываются. Цифровой фильтр улучшает соотношение сигнал/шум в несколь-

ко раз, соответственно повышая и общую чувствительность детектора. Становится возможным уверенно обнаруживать сигналы, лежащие ниже уровня шума (это общее свойство корреляционного приема).

С выхода *DA2* сигнал через еще один цифровой фильтр *R5C6* (или *C8* в зависимости от состояния ключей *DD1*) поступает на интегратор-компаратор *DA1,* напряжение на выходе которого при наличии полезного сигнала на входе *(VD1)* становится равным примерно напряжению питания. Этим сигналом включается светодиод *HL2* «Тревога» и головка *BA1.* Прерывистое тональное звучание головки BA1 и мигание светодиода *HL2* обеспечивается работой двух мультивибраторов с частотами около 1 и 2 кГц, выполненными на микросхеме *DD2*, и транзистором *VT5*, шунтирующим базу *VT6* с частотой работы мультивибраторов.

Конструктивно прибор состоит из СВЧ-головки и платы обработки, которая может быть размещена как рядом с головкой, так и отдельно.

Специальные приемники и комплексы обнаружения и пеленгации радиомикрофонов

Для обнаружения радиомикрофонов применяют специальные измерительные приемники, автоматически сканирующие по диапазону. С их помощью осуществляется поиск и фиксация рабочих частот передатчиков, а также определяется их местонахождение. Данная процедура достаточно сложна, она требует соответствующих теоретических знаний, практических навыков работы с разнообразной, весьма сложной измерительной аппаратурой. Пример использования и внешний вид такой аппаратуры представлен на рис. 2.48.

Профессиональный сканирующий приемник AR3000A

Приемник AR3000A (рис. 2.49) является одним из лучших мобильных сканирующих устройств на сегодняшний день. Надежность конструкции, выполненной на металлическом шасси, не оставляет сомнений. Расположение кнопок управления, ручек настройки, размеры жидкокристаллического индикатора — все сделано для удобства управления. Диапазон частот от 100 кГц до 2 ГГц (без вырезов) при скорости сканирования и поиска 50 каналов/с позволяет утверждать, что равных AR3000A по соотношению цена/качество/производительность нет.

По основным параметрам, таким, как чувствительность, избирательность и диапазон приема, AR3000A находится на одной ступени со значительно более дорогими моделями (например, ICOM IC-R9000).

Высокий уровень чувствительности в диапазоне от 100 кГц до 2036 МГц достигается за счет использования 15 полосовых фильтров и 3 ВЧ-усилите-

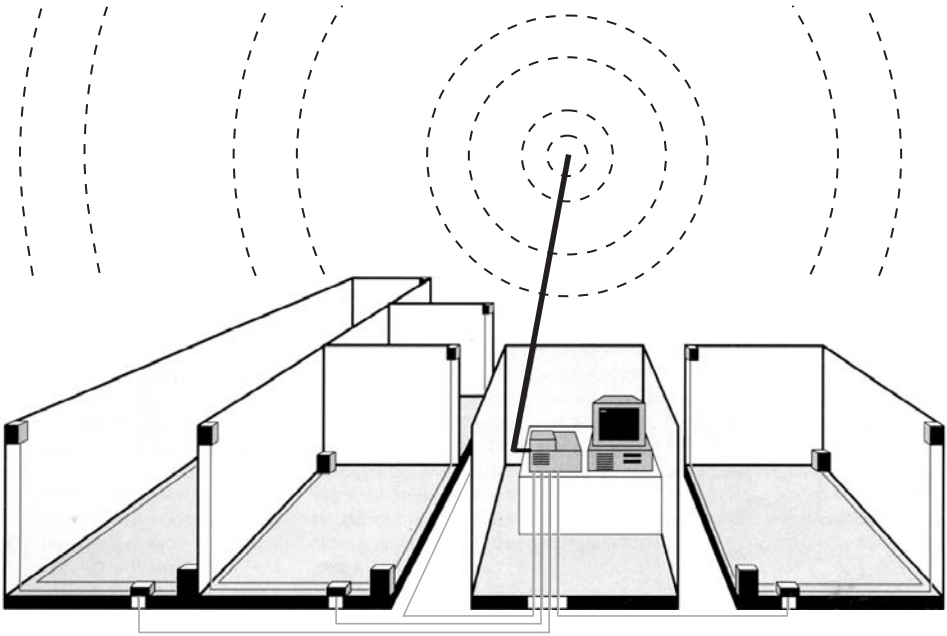


Рис. 2.48. Комплекс для обнаружения и пеленгации радиомикрофонов в помещении и пример его использования

лей, в то время как другие приемники располагают лишь широкополосными усилителями. Это дает высокую чувствительность во всем диапазоне при отсутствии интермодуляционных искажений.

Шаг настройки выбирается в диапазоне от 50 Гц до 999, 95 кГц (кратно 50 Гц) с возможностью быстрого увеличения в 10 или уменьшения в 5 раз нажатием кнопки на панели управления. Вращающаяся ручка плавной настройки удобна при приеме сигнала SSB.

Встроенный интерфейс RS-232 позволяет осуществлять полное ДУ с компьютера основными функциями приемника. Переключение в режим ДУ производится при помощи переключателя на задней панели прибора.

Рис. 2.49. Профессиональный сканирующий приемник AR3000A

Крупный жидкокристаллический индикатор расположен под удобным для наблюдения углом и отражает информацию о частоте, канале памяти, режимах поиска/сканирования, мощности принимаемого сигнала и дополнительных функциях. На дисплее отображается время таймера, позволяющего включать и выключать приемник в установленное время. Для работы в условиях недостаточной освещенности предусмотрена подсветка индикатора.

400 каналов памяти разбиты на 45 банка по 100 каналов в каждом. В каждом канале памяти хранится информация о типе сигнала, частоте, настройке аттенюатора и статусе захвата. Первый канал в каждом банке может быть установлен как приоритетный.

Таблица 2.4. **Характеристика сканирующего приемника AR3000 A**

Характеристика	Значение			
Диапазон рабочих частот, МГц	100—2036			
Тип модуляции	NMF, WFM, AM, USB, LSB,CW			
Тип приемника	Супергетеродин с 3-кратным преобразованием для USB/LSB/CWI/AM/NFM и 4-кратным для WFM			
Число каналов	400 (4 банка по 100 каналов)			
Скорость сканирования, каналов/с	50			
Скорость поиска, каналов/с	50			
Чувствительность приемника, мкВ, в диапазоне частот::	10 дБ S/N		12 дБ S/N	
	SSB/CW	AM	NFM	WFM
100 кГц — 2,5 МГц	1,0	3,2	—	—
2,5 МГц — 1,8 ГГц	0,25	1,0	0,35	1,0
1,8 ГГц — 2,0 ГГц	0,75	3,0	1,25	3,0
Избирательность приемника	2,4 кГц/–6 дБ, 4,5 кГц/–60 дБ (USB/LSB/CW)			
	12 кГц/–6 дБ, 25 кГц/–70 дБ (AM/NFM)			
	180 кГц/–6 дБ, 800 кГц/–50 дБ (WFM)			
Мощность звука, Вт	1,2 при коэффициенте нелинейных искажений 10% (4 Ом) 0,7 при коэффициенте нелинейных искажений 10% (8 Ом)			
Питание, В	13,8 постоянного тока (потребляемый ток 500 мА)			
Габариты, мм	138 80 200			
Вес, кг	1,2			

Прибор оборудован энергонезависимой памятью. Вся информация, находящаяся в ней, остается без изменений даже при выключении питания благодаря встроенной литиевой батарее.

Приемник позволяет осуществлять программируемое сканирование с задержкой до пропадания сигнала и паузой, время которой составляет от 1 до 60 с и задается пользователем. Основные технические характеристики даны в табл. 2.4

Сканирующий приемник с панорамным индикатором AX-700E

Одно из основных достоинств сканирующего приемника AX-700 (рис. 2.50) — наличие панорамного индикатора, позволяющего вести визуальное наблюдение за активностью диапазона шириной 1 МГц (250 кГц или 100 кГц, выбирается программно). Имеется возможность оперативной перестройки сканера на частоту с обнаруженной несущей. Прибор оснащен множеством эксклюзивных функций STANDARD, запоминающим устройством на 100 каналов и на 10 поддиапазонов для сканирования.

В приборе предусмотрено четыре способа сканирования:

- сканирование всего диапазона;
- сканирование любого, заранее оговоренного, поддиапазона;
- сканирование частот, записанных в памяти;
- сканирование определенных частот за вычетом хранящихся в памяти.

Приемник имеет четыре режима сканирования:

- HOLD — при приеме сигнала сканирование прекращается;
- DELAY — при приеме сигнала сканирование останавливается до пропадания сигнала;

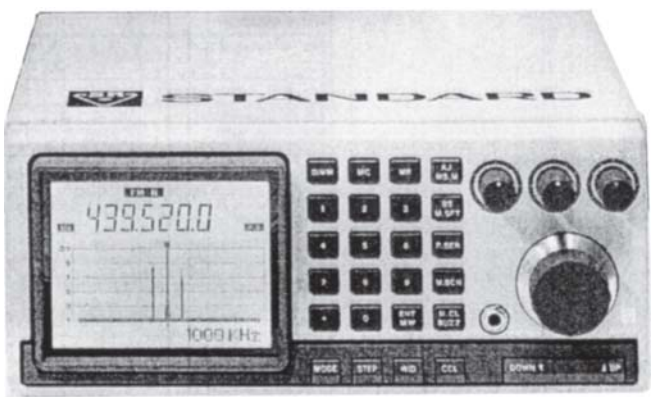


Рис. 2.50. Сканирующий приемник с панорамным индикатором AX-700E

- AUDIO DELAY — при приеме звукового сигнала сканирование останавливается до пропадания сигнала;
- PAUSE — при приеме сигнала сканирование останавливается и возобновляется через 5 с.

Сканер имеет широкий непрерывный частотный диапазон от 50 до 904,995 МГц и шаги настройки частоты 1,5; 10; 12,5; 20; 25 кГц.

Для удобства работы имеются разъемы для подключения внешнего громкоговорителя и головных телефонов (последний размещен на передней панели). При необходимости можно записывать на магнитофон сообщения, передаваемые в контролируемом диапазоне частот.

Наличие энергонезависимой памяти, питание 13,8 В, малый вес делают этот приемник удобным в работе — вы можете использовать его в стационарных условиях и в любой момент взять с собой в дорогу.

Основные технические характеристики

Диапазон рабочих частот, МГц	50—905
Тип модуляции	AM, NFM (±50 кГц), WFM (±75 кГц)
Чувствительность AM, мкВ	3
Чувствительность NFM, мкВ	1,5
Чувствительность WFM, мкВ	1
Стабильность частоты, %	0,0002
Селективность, дБ	не менее 30
Шаг частоты, кГц	10; 12,5; 20; 254
Количество каналов	100
Количество поддиапазонов сканирования	10
Напряжение питания, В	13,8 ±15 %
Потребляемый ток, А	0,3
Диапазон рабочих температур, °С	0—50
Габариты, мм	180×75×180
Вес, кг	2,1

Комплексы автоматизированного радиоконтроля АРК-ПК-3К и АРК-ПК-5К

Предназначены для поиска и пеленгования источников радиоизлучений, оценки и протоколирования загрузки диапазона, контроля радиотелефонных каналов систем связи, автоматического обнаружения радиомикрофонов, контроля проводных сетей, выполнения разнообразных функций радиомониторинга. Работают от аккумулятора 12 В, автомобильной бортовой сети или от сети переменного тока. Размещаются в кейсе в комплекте с компьютером типа Notebook. Внешний вид комплекса представлен на рис. 2.51. Комплексы отличаются друг от друга типом используемого приемного устройства

(AR3000A или AR5000) и контролируемым диапазоном частот 1—2500 МГц и 1—2600 МГц соответственно.

Основные функции комплекса радиоконтроля следующие:

- быстрый панорамный анализ с высокой разрешающей способностью, протоколирование загрузки УКВ-диапазона на момент приема на жесткий диск, поиск работающих радиостанций;
- сканирующий прием в стационарных условиях или в салоне автомобиля с записью на жесткий диск ПЭВМ демодулированных речевых сигналов, их несущих частот, времени обнаружения, длительности и относительного уровня, а также последующее воспроизведение зарегистрированных сигналов (на головные микротелефоны) и служебной информации (на экране монитора);
- прием и регистрация на жесткий диск сигналов пейджерных систем в формате POCSAG.
- отложенная обработка результатов регистрации;
- автоматическое обнаружение радиомикрофонов с АМ, узкополосной и широкополосной ЧМ, с закрытием (инверсией спектра и «частотной мозаикой») и определение их местоположения;
- контроль проводных сетей на наличие посторонних напряжений;
- создание прицельных помех приему сигналов от обнаруженных радиомикрофонов;
- работа в режиме цифрового магнитофона с записью на жесткий диск компьютера речевых сигналов, времени регистрации, длительности и уровня, а также последующее воспроизведение зарегистрированных сигналов (на головные микротелефоны) и служебной информации (на экране монитора).

При панорамном анализе аппаратура позволяет обнаруживать и измерять параметры излучений, отображать на экране монитора спектральный состав радиосигналов и записывать на жесткий диск данные о выявленных излучениях одновременно со служебной информацией.

Для обеспечения панорамного анализа в аппаратуре используется дискретно-шаговая перестройка приемника с шагом, равным полосе широкополосного тракта. Напряжение с выхода широкополосного тракта доработанного приемника обрабатывается процессором БПФ, что обеспечивает параллельный анализ с высокой скоростью перестройки (до 70 МГц) в сочетании с высоким разрешением по частоте.

Рис. 2.51. Комплекс автоматизированного радиоконтроля

Основные технические характеристики АРК-ПК

Чувствительность, мкВ ..... 1—3
Динамический диапазон, дБ ..... 55—60
Скорость панорамного анализа, МГц/с:
в полосе 2 МГц ..... 40—70 (режим «Спектр»)
в полосе до 80 МГц ..... 30 (режим «Спектр»)
в полосе свыше 80 МГц ..... 40 (режим «Панорама»)
Дискретность отсчета частоты, кГц 3
Скорость ввода данных на диск ПЭВМ при регистрации демодулированных сигналов, кб/с 1,7
Мощность обнаруживаемых радиомикрофонов, мкВт 50
Виды модуляции радиомикрофонов ..... $ЧМ_{узк}$, $ЧМ_{шир}$, АМ, частотная инверсия
Скорость перестройки, МГц/с ..... 40—70
Точность определения местоположения, см 20
Диапазон частот передатчика, МГц ..... 65—1000
Шаг перестройки, кГц 12,5
Мощность передатчика, мВт ..... 120—150
Виды модуляции ..... $ЧМ_{узк}$, $ЧМ_{шир}$
Модулирующее сообщение ..... речь, тон, шум
Контроль проводных сетей
максимальное напряжение в сети, В 400
виды модуляции источников ..... $ЧМ_{узк}$, $ЧМ_{шир}$, АМ, частотная инверсия

Комплекс функционирует в реальном масштабе времени (режимы «Панорама», «Спектр») и обеспечивает отложенную обработку результатов регистрации (режимы «Воспроизведение», «Анализ»).

В режимах «Панорама», «Спектр» комплекс обеспечивает:

- возможность панорамного анализа на участках частот общей протяженностью до 80 МГц (до 10 участков шириной 2 или 8 МГц каждый) в пределах общего диапазона 1—2000 МГц;
- панорамное отображение загрузки диапазона максимальными уровнями в диапазоне 1—2000 МГц или на его участках любой протяженности с возможностью дополнения данных;
- накопление на жестком диске и отображение диаграмм загрузки рабочего поддиапазона в координатах «частота — время» и «частота — амплитуда», получаемых в результате выполнения режима аппаратурой;
- отображение в рабочем поддиапазоне спектров с усреднением и экстремальных значений анализируемых сигналов на интервале наблюдения.

В режиме «Анализ» комплекс обеспечивает:

- отображение получаемых в результате выполнения режима «Спектр» диаграмм загрузки рабочих поддиапазонов в координатах «частота — время» и «частота — амплитуда»;
- формирование и представление статистических данных о потоке сигналов в радиоканалах по результатам выполнения режима «Спектр», в том числе оценку частотно-амплитудно-временных характеристик потока поступающих сигналов за время ее работы и (или) на отдельных интервалах времени, накопления и обработки массивов полученных оценок, выдача на экран, печатающее устройство и внешние устройства полученных результатов.

При контроле радиотелефонных каналов комплекс обеспечивает выполнение следующих функций:

- ПОИСК — перестройка в рабочем частотном поддиапазоне с заданным шагом, однократная или многократная запись демодулированных речевых передач и параметров (частоты, времени, относительного уровня) на жесткий диск ПЭВМ;
- СКАНИРОВАНИЕ — перестройка по запрограммированным частотным каналам, запись демодулированных речевых передач и параметров (частоты, времени, относительного уровня) на жесткий диск ПЭВМ;
- ВОСПРОИЗВЕДЕНИЕ — воспроизведение на мониторе персонального компьютера панорамы, регистрируемых параметров (частоты, времени, относительного уровня) с жесткого диска ПЭВМ и прослушивание зарегистрированных сигналов на головные микротелефоны.

При автоматическом обнаружении радиомикрофонов комплекс с высокой скоростью обеспечивает высококачественный анализ частотного диапазона 10—2000 МГц на наличие активных радиозакладных устройств различных типов и определение их местоположения в контролируемом помещении. Использование набора классических и оригинальных алгоритмов анализа позволяет без участия оператора достоверно идентифицировать радиомикрофоны с амплитудной, узкополосной и широкополосной частотной модуляцией, а также со скремблированием (с простой и сложной инверсией спектра) и с высокой точностью определить их местоположение. Благодаря использованию антенной системы обеспечивается обнаружение радиомикрофонов под прикрытием мощных штатных радиосредств. Предусмотрена возможность использования бесшумного коррелятора, активных тестов и внешней опорной антенны.

Нелинейные радиолокаторы

Если радиомикрофоны выключены в момент поиска и не излучают сигналы, по которым их можно обнаружить радиоприемной аппаратурой, то для их поиска (а также для поиска микрофонов подслушивающих устройств и мини-

магнитофонов) применяют специальную рентгеновскую аппаратуру и нелинейные локаторы (детекторы) со встроенными генераторами микроволновых колебаний низкого уровня. Такие колебания проникают сквозь стены, потолки, пол, мебель, портфели, утварь — в любое место, где может быть спрятан радиомикрофон, микрофон, магнитофон. Когда микроволновый луч соприкасается с транзистором, диодом или микросхемой, луч отражается назад к устройству. Таким образом, принцип действия в данном случае похож на миноискатель, реагирующий на присутствие металла.

Нелинейные локаторы, или локаторы нелинейностей, используются для проведения поисковых мероприятий в течение многих лет. Часть специалистов по проведению подобных работ дают очень высокую оценку этой технике, в то время как другие (возможно, из-за малого опыта при использовании нелинейных локаторов) отзываются о них весьма сдержанно.

Большинство людей, незнакомых с возможностями технического шпионажа, представляют подслушивающие устройства в основном как передатчики. Однако «специалисты» в данной области используют массу электронных устройств, которые не имеют ничего общего с радиопередатчиками. Именно в этих случаях нелинейные локаторы просто незаменимы, так как могут обнаруживать и определять местоположение любого электронного устройства, независимо от того включено оно или нет.

Антенна нелинейного локатора облучает объект для определения наличия в нем электронных компонентов. Когда ВЧ-сигнал облучает полупроводниковые соединения (диоды, транзисторы и т. д.), он благодаря их нелинейным характеристикам возвращается к приемнику на гармонических частотах с определенными уровнями.

Наиболее распространенной проблемой, возникающей при использовании нелинейных локаторов, являются ложные срабатывания. Любые обычные бытовые электронные приборы, такие, как телефон или электронные часы, будут вызывать срабатывание прибора, так как они состоят из электронных компонентов. На практике подобные срабатывания, вызванные бытовыми приборами, легко различимы визуально, однако ложные срабатывания могут вызываться металлическими объектами, не содержащими никаких электронных компонентов (места соединения двух различных металлов или коррозийные металлические конструкции).

Из-за различия в нелинейных характеристиках полупроводникового и ложного соединений отклики 2-й и 3-й гармоник будут иметь различную интенсивность. Когда нелинейный локатор облучает полупроводник, отклик на 2-й гармонике сильнее, чем на 3-й. При облучении ложного соединения наблюдается обратный эффект.

При применении нелинейных локаторов в поисковых мероприятиях возможно не только обнаружение электронных устройств, но и их классификация при помощи аудиодемодуляции. Так, например, при обнаружении некоторых записывающих устройств можно услышать аудиосигнал записывающей головки. Более того, если локатор дает хорошую аудиодемодуляцию, то зача-

стую возможно прослушивание синхронизирующих импульсов при обнаружении видеокамер. Используя частотную демодуляцию, иногда возможно прослушать характерные аудиосигналы в электронных устройствах, возникающие из-за фазовых сдвигов. Поэтому очень важно иметь достаточный опыт работы с прибором для распознавания электронных устройств по характерным аудиосигналам.

Кроме того, при обнаружении ложного соединения можно, прослушивая демодулированный аудиосигнал и одновременно производя на это соединение физическое вибрационное воздействие (постукивая по стене кулаком или резиновым молотком), без особого труда отличить его от полупроводника. Ложное соединение отреагирует на подобное воздействие треском в наушниках. Чистый полупроводник при этом будет «молчать».

Портативный нелинейный радиолокатор Orion NJE-4000

Предназначен для обнаружения и поиска устройств, содержащих полупроводниковые компоненты (рис. 2.52). Он обеспечивает автоматический поиск свободной частоты в диапазоне 850—1000 МГц, круговую поляризацию, изменяемую мощность в диапазоне 10 мВт — 1Вт, отсутствие соединительных проводов, новейшие специальные алгоритмы обнаружения.

Особенности функционирования прибора:

- минимальное время, необходимое для подготовки локатора к работе;
- отсутствие проводов или громоздких приемо-передающих устройств;
- большая мощность передатчика, позволяющая обеспечить более быструю по сравнению с другими моделями локацию исследуемой поверхности;
- наличие беспроводных (инфракрасных) наушников и графического дисплея для синхронного отображения аудио- и визуальной информации.

Портативный нелинейный радиолокатор NR-900E

Портативный нелинейный радиолокатор NR-900E (рис. 2.53) американской фирмы *REI* предназначен для поиска и обнаружения устройств, содержащих полупроводниковые компоненты как во включенном, так и в выключенном состоянии. Среди известных в мире аналогов представленного здесь локатора можно назвать, например, локаторы торговой марки *SuperBroom* английской фирмы *Audiotel.*

Модель нелинейного локатора NR-900E относится к четвертому поколению локаторов серии NR. Общими для всех моделей серии являются следующие характеристики:

- высокий энергетический потенциал;
- остронаправленная антенная система;
- наличие режима огибающей.

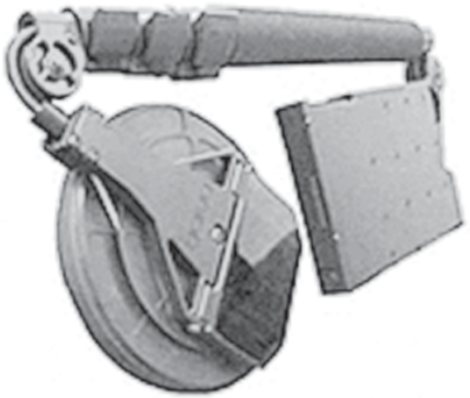


Рис. 2.52. Портативный нелинейный радиолокатор Orion NJE-4000

Рис. 2.53. Портативный нелинейный радиолокатор NR-900E

Сохраняя все достоинства предшествующих моделей, локатор NR-900E, технические характеристики которого представлены ниже, обеспечивает возможность сравнительного анализа сигналов на 2-й и 3-й гармониках зондирующего сигнала, что значительно повышает эффективность его использования.

Другой отличительной особенностью NR-900E является использование специальной микропроцессорной системы обработки сигналов и управления. Все органы управления и ЖКИ-табло отображения информации выведены на пульт управления, размещенный на штанге-держателе антенной системы.

Основные технические характеристики

Вид излучения ..... импульсный
Дальность обнаружения, м ..... 0,5—2
Точность локализации, м 0,1
Несущая частота, МГц ..... 900 ±10
Частоты настройки приемника, МГц ..... 1800 и 2700
Мощность излучаемого сигнала, Вт: .....
в режиме «300» ..... не менее 150
в режиме «20К» ..... не менее 25
Чувствительность приемного блока при соотношении сигнал/шум 10 дБ, дБ/Вт ..... не хуже 115
Динамический диапазон приемника, дБ ..... не менее 25

Регулировка усиления 5-ю ступенями,
в каждой ступени, дБ ..... по 10±2
Коэффициенты усиления, дБ:
приемной антенны ..... не менее 9
передающей антенны ..... не менее 8
Напряжение питания, В:
от сети переменного тока, В ..... 220±22
от аккумулятора 12

Портативный нелинейный радиолокатор «Родник»

Радиолокатор «Родник» (рис. 2.54) предназначен для обнаружения в строительных конструкциях помещений и предметах их интерьера скрытно установленных радиопередающих устройств и других технических средств съема информации, которые содержат в себе полупроводниковые компоненты, и находящихся как во включенном, так и в выключенном состоянии.

Работа аппаратуры основана на принципе нелинейной радиолокации («Родник-2» работает по 2-й гармонике отраженного сигнала, «Родник-23» — по 2-й и 3-й гармоникам). Аппаратура в зоне обследования создает электромагнитное поле с заданными характеристиками. При выявлении в обследуемой зоне радиоэлектронного устройства заданные характеристики электромагнитного поля претерпевают изменения. Эти изменения фиксируются аппаратурой, проводится их анализ и выдается информация о наличии в зоне обследования радиоэлектронного устройства.

Основные технические характеристики

Частота излучения передатчика, МГц 910
Мощность сигнала на выходе «Датчик», Вт ..... не менее 2
Чувствительность приемного блока при
соотношении сигнал/шум 10 дБ, дБ/Вт ..... не хуже –145
Уровень шума на выходе «ТЛФ», мВт ..... не менее 60
Дальность обнаружения, м ..... не менее 1
Напряжение питания, В:
от сети переменного тока 220
от аккумулятора 12
Масса с укладочным чемоданом, кг ..... не более 1

Портативный нелинейный радиолокатор «Обь»

Радиолокатор «Обь» (рис. 2.55) предназначен для обнаружения в строительных конструкциях помещений и предметах их интерьера электронных средств негласного съема информации, взрывных устройств с неконтактными взрывателями и других несанкционированно размещенных устройств, содержащих радиоэлектронные компоненты.

Рис. 2.54. Портативный нелинейный радиолокатор «Родник»

Рис. 2.55. Портативный нелинейный радиолокатор «Обь»

Обнаружение осуществляется путем облучения радиоэлектронных устройств высокочастотным непрерывным излучением и анализа 2-й гармоники отраженного сигнала. Прибор имеет звуковую индикацию принимаемых сигналов на головные телефоны и визуальную — по стрелочному прибору, может работать в помещениях и в полевых условиях от сети переменного тока или от аккумуляторных батарей. Конструктивно выполнен в виде 3 блоков, размещенных в атташе-кейсе стандартного размера. Модификацией прибора является «Обь-АЛ», снабженный лазерным целеуказателем для точного и быстрого определения местоположения электронных устройств.

Основные технические характеристики

Частота излучения передатчика, МГц	1000
Частота приемника, МГц	2000
Мощность излучения, мВт	250
Чувствительность приемника, дБ/Вт	145
Диапазон регулировки чувствительности, дБ	60
Потребляемая мощность, Вт	30
Дальность обнаружения, м	0,5—2,0
Питание	2 аккумулятора типа 6СГ- 6 или сеть 220 В
Индикация	звуковая, визуальная
Вес, кг	около 6

В тех случаях, когда нет приборов для поиска передатчиков либо нет времени на поиск, можно пользоваться генераторами помех для подавления приемников. Они достаточно просты, очень надежны и работают в широком диапазоне частот. Но если передатчик узкополосный, то для его подавления необходим генератор шума очень большой мощности с высокой плотностью излучения, что, в свою очередь, отрицательно сказывается на здоровье находящихся в защищаемом помещении людей.

Низкочастотные сетевые передатчики

Как уже говорилось выше, радиомикрофоны работают в ВЧ-диапазонах. Однако есть и такие устройства, которые работают в НЧ-диапазоне (50—300 кГц). В качестве канала связи они обычно используют сети силовой электропроводки и сигнализации, телефонные и радиотрансляционные линии. Эти устройства практически не излучают сигналы в окружающее пространство, т. е. обладают повышенной скрытностью. Если их вмонтировать в настольную лампу, розетку, тройник, любой электроприбор, работающий от сети переменного тока (рис. 2.56), то они, питаясь от сети, будут долгое время передавать по ней информацию в любую точку здания и даже за его пределы.

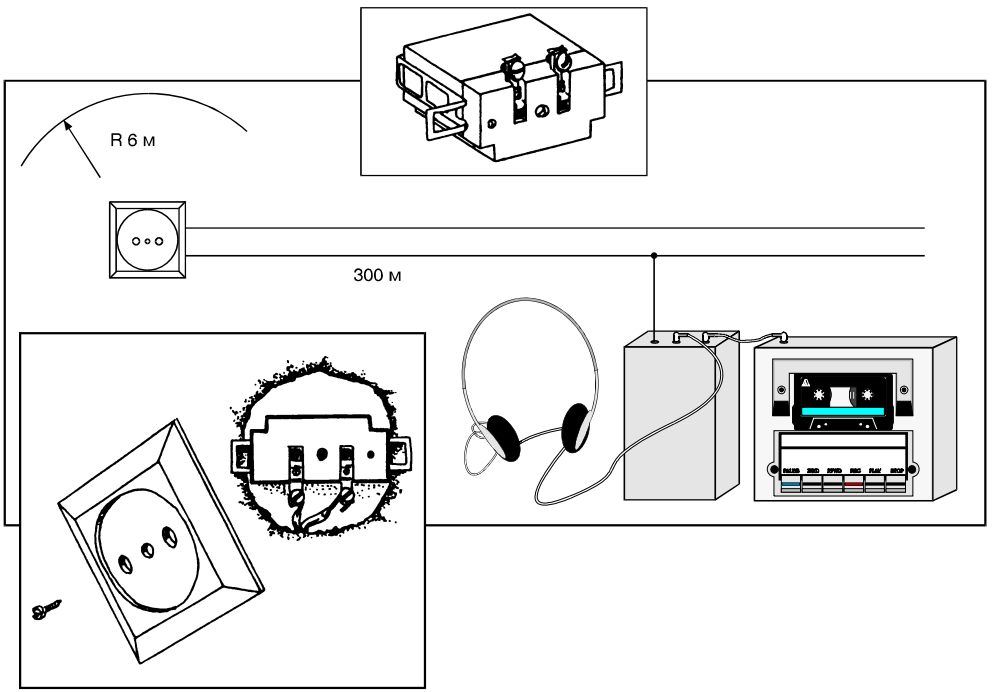


Рис. 2.56. Подключение устройств съема информации к силовой сети

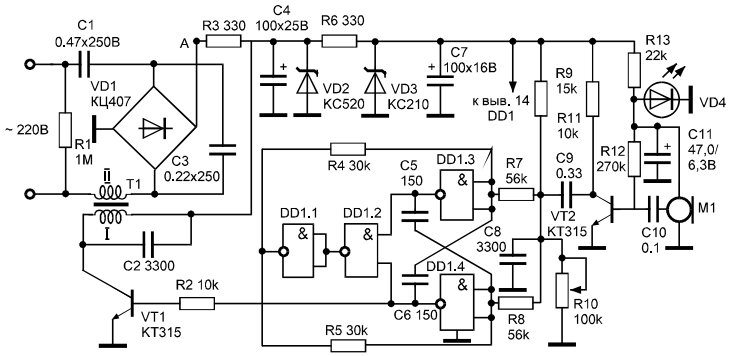


Рис. 2.57. Принципиальная схема сетевого низкочастотного радиопередатчика

Для этого они используют провода электропроводки как линию активной связи и как источник энергии. Отловить передаваемый сигнал можно из электророзетки, однако лишь в пределах действия одного силового трансформатора. Хотя недавно были проведены успешные эксперименты по использованию силовых линий электропередач для передачи информации между компьютерами на большие расстояния и объединения их в информационную сеть.

Сетевой радиопередатчик

Выше приведенные устройства излучают ВЧ-колебания в сеть, используя провода сети в качестве антенны. Но есть и устройства, которые работают в НЧ-диапазоне (50—300 кГц) и также используют в качестве канала связи электросеть или телефонную линию. Такие радиопередатчики имеют повышенную скрытность, так как практически не излучают сигналы в окружающее пространство. Примером передачи сигналов в НЧ-диапазоне может служить трехпрограммное проводное вещание, где 2-я и 3-я программы передаются на частотах 78 и 120 кГц соответственно с использованием амплитудной модуляции. Приборы, питающиеся от сети переменного тока, могут длительное время передавать по ней информацию в любую точку здания и даже за его пределы.

Схема одного из таких устройств приведена на рис. 2.57. Для передачи информации используется частотная модуляция несущей частоты, равной 95 кГц.

Устройство питается от сети через бестрансформаторный блок питания. Излишек напряжения сети гасится конденсатором *C1*. Пониженное напряжение выпрямляется диодным мостом *VD1* типа КЦ407. Резистор *R3* и конденсатор *C4* образуют сглаживающий фильтр, предотвращающий проникновение колебаний несущей частоты в цепи питания устройства. Напряжение ограничивается до необходимой величины стабилитроном *VD2* типа КС520. Данное напряжение используется для питания усилителя мощности. Напряжение, снимаемое с параметрического стабилизатора на резисторе *R6*, стабилитроне *VD3* и конденсаторе *C7*, используется для питания устройства.

Сигнал звуковой частоты, снимаемый с микрофона *M1* типа М1-Б2 «Сосна», усиливается однокаскадным усилителем на транзисторе *VT2* типа КТ315.

ЧМ-модулятор представляет собой управляемый напряжением генератор прямоугольных импульсов. Собран он на микросхеме *DD1* типа К561ЛА7. Начальную частоту следования импульсов генератора (при отсутствии напряжения звуковой частоты) устанавливают при помощи подстроечного резистора *R10*. Она должна равняться 95 кГц. При поступлении напряжения звуковой частоты с делителя *R9*, *R10* частота следования импульсов генератора начинает изменяться, т. е. модулируется напряжением звуковой частоты. Модулированные колебания поступают на усилитель мощности, собранный на транзисторе *VT1* типа КТ315. Нагрузкой этого транзистора служит трансформатор *T1*. Первичная обмотка трансформатора совместно с конденсатором *C2* образуют колебательный контур, настроенный на частоту несущей. В этом колебательном контуре прямоугольные импульсы преобразуются в синусоидальный сигнал, что исключает появление побочных гармоник в выходном сигнале. С обмотки *2* трансформатора *T1* сигнал несущей частоты через конденсаторы *C1* и *C3* поступает в сеть 220 В переменного тока. Такой сигнал необходимо принимать на специальный приемник (см. ниже). В устройстве использованы резисторы типа МЛТ-0,125. Резистор *R10* — любой малогабаритный. Конденсаторы *C1* и *C3* должны быть рассчитаны на рабочее напряжение не ниже 250 В. Стабилитроны *VD2* и *VD3* могут иметь напряжение стабилизации 18—24 В и 6—12 В соответственно. Микросхема *DD1* может быть заменена на К176ЛА7, К564ЛА7, К1561ЛА7.

Трансформатор *T1* намотан на кольцевом ферритовом сердечнике К12×7×3 мм марки 600НН. Первичная обмотка содержит 100 витков провода ПЭВ 0,1, вторичная обмотка — 20 витков провода в изоляции диаметром 0,15—0,3 мм. Сердечник трансформатора изолируется лакотканью или фторопластом. Обмотки также разделяются слоем изоляции.

Настройку лучше начинать с использованием источника постоянного напряжения 30 В, плюсовой провод которого подключают к точке *A* (устройство к сети не подключено!). Проверяют напряжение на стабилитронах *VD2* и *VD3*. Затем закорачивают базу транзистора *VT2* на общий провод и подбором сопротивления резистора *R10* устанавливают частоту генератора на микросхеме *DD1*, равную 95 кГц (контролируется осциллографом или частотомером на резисторе *R2*). Подбором конденсатора *C2* добиваются получения неискаженной синусоиды на коллекторе транзистора *VT1*. После этого снимают перемычку с базы транзистора *VT2* и убеждаются в наличии частотной модуляции.

ВНИМАНИЕ! При настройке и эксплуатации устройств с бестрансформаторным питанием от сети переменного тока необходимо соблюдать правила и меры безопасности, так как элементы этих устройств находятся под напряжением 220 В.

Защита питающих цепей радиоэлектронной аппаратуры

Сетевые фильтры обеспечивают защищенность электронного устройства не только от внешних помех, но и от разного рода сигналов, генерируемых устройствами, которые могут служить источником утечки информации, в том числе и сетевые передатчики.

К защищаемым устройствам относят самую разнообразную аппаратуру: компьютеры, приемники диапазона длинных и средних волн, радиотрансляционные приемники и др. Сетевой фильтр устанавливают между энергетической сетью и устройством потребителя.

Рассмотрим наиболее часто используемые фильтры, выпускаемые нашей промышленностью, и приведем принципиальную схему подобного фильтра, пригодную для самостоятельного изготовления.

Сетевые помехоподавляющие фильтры ФСП-1Ф-7А и ФСП-3Ф-10А

Фильтр сетевой помехоподавляющий ФСП-1Ф-7А предназначен для защиты радиоэлектронных устройств и средств вычислительной техники от утечки информации по сетям электропитания с напряжением 220 В, частотой 50 Гц, а также для защиты их от ВЧ-помех и повышения помехоустойчивости в диапазоне частот от 150 кГц до 1000 МГц. Он применяется для обеспечения электромагнитной развязки по цепям электропитания выше перечисленных устройств и электросетей промышленных и других объектов. Внешний вид фильтра представлен на рис. 2.58, а технические характеристики — ниже.

Этот фильтр представляет собой набор высокочастотных LC-фильтров, включаемых в сеть напряжением 220 В, частотой 50 Гц. Для уменьшения связи между входом и выходом LC-фильтры размещены в трех экранированных отсеках, образованных стенками и шасси фильтра. Соединение цепей между отсеками осуществляется проходными индуктивностями. Подавление помехи осуществляется реактивными LC-элементами фильтра.

Сетевой помехоподавляющий трехфазный фильтр ФСП-3Ф-10А предназначен для защиты трехфазных цепей электропитания напряжением 380/220 В, частотой 50 Гц с номинальным рабочим током до 10 А по каждой фазе. Внешний вид фильтра аналогичен однофазному фильтру типа ФСП-1Ф-7А, а его технические характеристики даны ниже.

Рис. 2.58. Сетевой помехоподавляющий фильтр ФСП-1Ф-7А

Фильтр ФСП-3Ф-10А может использоваться для обеспечения электромагнитной совместимости и увеличения помехоустойчивости радиоэлектронных средств и средств вычислительной техники различного назначения. Допускается использование фильтра в однофазных сетях, параллельное и последовательное подключение двух фильтров.

Основные технические характеристики фильтров ФСП-1Ф-7А и ФСП-3Ф-10А

Величина затухания по напряжению в каждом проводе двухпроводной сети в диапазоне частот от 150 кГц до 1000 МГц, дБ ..... не менее 60
Величина падения напряжения на одном проводе на частоте 50 Гц, В:
при максимальном токе 7 А ..... не более 3
при максимальном токе 10 А 0,3
Электрическое сопротивление между заземляющим зажимом и корпусом фильтра, Ом ..... не более 0,1
Сопротивление изоляции в нормальных климатических условиях между цепями сетевого питания и корпусом фильтра, МОм ..... не менее 20
Диапазон рабочих температур, °С ..... 10—40
Относительная влажность воздуха при 30 °С, % ..... до 90
Габариты, мм ..... 270×150×115
Масса фильтра, кг ..... не более 3,9
Средний срок службы, лет ..... не менее 10
Средняя наработка на отказ, ч ..... не менее 10 000
Класс электрозащиты фильтра по ГОСТ 12.2.007.0—75 01

Примечание. При параллельном и последовательном включении фильтров их соответствующие характеристики суммируются.

Сетевой фильтр для самостоятельного изготовления

Принципиальная схема сетевого фильтра, рассчитанного на мощность нагрузки 100 Вт и предназначенного для самостоятельного изготовления, представлена на рис. 2.59. Его характерная особенность состоит в том, что он обеспечивает питание одновременно двух потребителей.

В данном фильтре использованы два способа подавления помех: фильтрация режекторным дросселем *Др1, Др2* и экранирование сетевой обмотки трансформатора *Т1* и выходной обмотки трансформатора *Т2.* Электростатическим экраном сетевой обмотки трансформатора *Т1* и выходной обмотки трансформатора *Т2* служат магнитопроводы и низковольтные обмотки трансформаторов, расположенные поверх высоковольтных и соединенные с общим проводом фильтра и устройств-потребителей. Так как направление намотки обмоток и индуктивность дросселей *Др1* и *Др2* одинаковы, а токи через обмотки

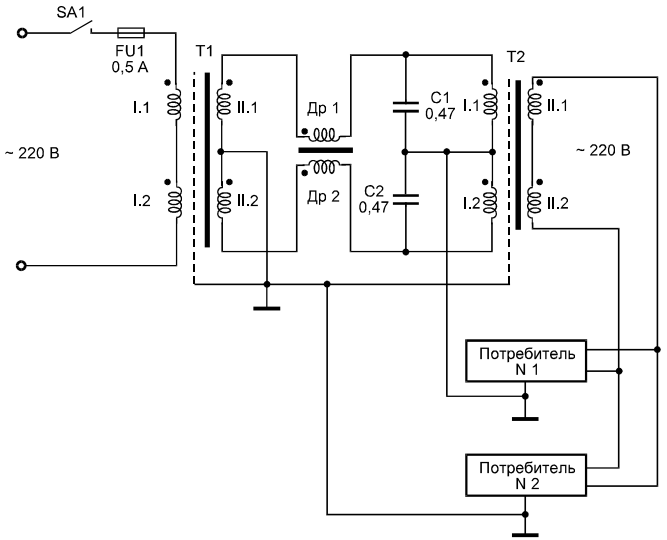


Рис. 2.59. Принципиальная схема самодельного сетевого фильтра

Др1 и *Др2* противофазны, то сумма магнитных полей этих обмоток равна нулю и результирующее сопротивление дросселей переменному току промышленной частоты равно активному сопротивлению обмоток. Следовательно, падение напряжения на дросселях *Др1, Др2* практически равно нулю.

В устройстве использованы два готовых трансформатора *Т1* и *Т2* типа ТПП296-127/220-50. Режекторные дроссели *Др1, Др2* выполнены на ферритовом кольцевом магнитопроводе марки М4000 размером К65×32×8. Две обмотки наматываются в два провода одновременно проводом МГШВ-0,5 и содержат по 20 витков каждая. Намотка должна быть в один слой. Марка феррита и размер сердечника могут быть другими, но индуктивность дросселей должна быть около 1,5 мГн. Конденсаторы *С1* и *С2* должны быть рассчитаны на напряжение более 400 В.

2.3. Диктофоны

Диктофоны — устройства, записывающие голосовую информацию на магнитную ленту (проволоку, внутреннюю микросхему памяти). Время записи различных диктофонов колеблется в пределах от 15 мин до 10 ч. Стандартными аксессуарами хороших диктофонов являются выносной микрофон, пульт дистанционного управления. Режимы записи по голосу (VOX) и автореверс кассеты уже имеют практически все диктофоны. Чувствительность выносного микрофона позволяет произвести хорошую запись разговора с дальности до 5 м. Диктофоны могут комплектоваться и специальными аксессуарами:

- выносными микрофонами с отдельным питанием и усилителем;
- выносными вибромикрофонами (стетоскопными), позволяющими записать разговор через стену;
- микрофонами с достаточно длинным кабелем: применяются для записи разговоров, например, на кухне через вентиляционную шахту.

В качестве магнитного носителя у специальных диктофонов (в особенности у долговременных) может использоваться тонкая стальная проволока.

Последним «писком» на рынке в области скрытной звукозаписывающей техники являются диктофоны с записью информации во внутренний чип памяти, позволяющий производить запись разговора длительностью до нескольких часов. Данные диктофоны практически бесшумны (так как нет ни кассеты, ни механического лентопротяжного механизма, производящих основной шум), имеют возможность сброса записанной информации в память компьютера для ее дальнейшей обработки (повышения разборчивости речи, выделения полезных фоновых сигналов и т. д.).

Не секрет, что не всегда и не всем нравится, когда разговор, особенно деловой, записывается на пленку. С развитием электронной техники и появлением все новых достижений в области миниатюризации стало возможным осуществлять давнюю мечту репортеров и шпионов. Наконец-то появились диктофоны, имеющие весьма малые размеры при обилии вспомогательных устройств и сервисных функций, с помощью которых возможно производить скрытную запись.

Существует несколько стандартов записи для диктофонов. Прежде всего, это запись на стандартную кассету. Такую запись можно «расшифровать» на любом магнитофоне. Однако такой диктофон вряд ли можно использовать скрытно. Другой стандарт — микрокассетный. Такие устройства, несомненно, компактней, но прослушивать запись возможно только с их помощью.

Все диктофоны имеют систему автоматического регулирования уровня записи (АРУЗ). Здесь есть одна тонкость. При записи слабого сигнала встроенный микрофон очень хорошо «слышит» собственные шумы диктофона. Этот недостаток легко исправим при использовании выносного микрофона. Такой микрофон просто незаменим, если ведется скрытная запись собеседника.

Ряд диктофонов имеет систему голосовой активации записи. Это позволяет повысить плотность записи и экономить ленту при записи продолжительной беседы. Кроме того, многие диктофоны, особенно микрокассетные, имеют две рабочие скорости.

В последнее время все более широко стали применяться диктофоны, использующие цифровую запись звука. Запись в них ведется в цифровом виде на мини-диски или на встроенную микросхему памяти (микрочип). Преимущества этих систем перед аналоговыми — быстрый доступ к нужному фрагменту, качество и долговечность записи. Например, диктофон Olympus D-1000 использует для записи аудиоинформации неподвижный электронный носитель — карточку стандарта FTL вместимостью 2 или 4 Мб. Время записи в

стандартном режиме на карточку 2 Мб составляет 16 мин, на карточку 4 Мб — 33 мин, в продолжительном режиме — 34 и 72 мин соответственно. При этом качество записи в стандартном режиме сравнимо с записью на обычный микрокассетный диктофон, а в продолжительном режиме — эквивалентно обычному телефонному разговору. Этот диктофон не содержит каких-либо движущихся деталей и узлов, то есть в процессе работы не создает механических шумов и вибраций, не излучает каких-либо электрических и магнитных колебаний и практически не выявляется существующими системами обнаружения.

Диктофоны можно купить практически в любом магазине или ларьке. Для скрытного получения информации их прячут в дипломатах, свертках, карманах или вмонтируют в различные предметы: настольные часы, вазы и т. д. Тактика применения проста: дипломат «случайно» забывают в кабинете, плащ по «рассеянности» оставляют в приемной, а часы дарят людям, в помещения которых есть доступ после работы своих агентов (уборщиц, сторожей, пожарников) для смены кассет.

Диктофоны с записью на микрокассету

Диктофоны Olympus S713 и S725

Диктофоны Olympus S713 и S725 (рис. 2.60) с записью на микрокассету при невысокой цене и простоте в эксплуатации обеспечивают хорошее качество записи и воспроизведения речи. Они оснащены автореверсом, с помощью которого на 90-минутную пленку в непрерывном режиме можно записать до трех часов беседы (естественно, при использовании пониженной скорости движения ленты). Правда, в этом случае придется немного пожертвовать качеством, так как на пониженной скорости диапазон записываемых частот у́же, чем на стандартной. Однако порой бывает гораздо важнее записать всю беседу полностью с качеством похуже, чем потом довольствоваться только ее половиной.

Особенности диктофонов Olympus S713 и S725:

- запись на микрокассету;
- голосовая система активации записи с регулируемой чувствительностью;
- двухпозиционный переключатель скорости ленты (1,2/2,4 см/с);
- ускоренное воспроизведение; регулировка чувствительности микрофона;
- автостоп;
- функции обзора в прямом и обратном направлении;
- светодиодный индикатор;
- автореверс;
- счетчик ленты (S725);
- встроенные динамик и микрофон;
- гнезда для подключения наушников и сетевого адаптера (S725);

Рис. 2.60. Диктофоны Olympus S713 и S725

- гнездо для подключения внешнего микрофона (S725);
- гнездо для подключения пульта ДУ (S725);
- питание — 2 батарейки типа AA;
- габариты — 121×58×26 мм;
- вес (с батарейками) — 160 г.

Отдельно стоит отметить возможность подключения пульта ДУ в модели S725. Скользящий переключатель ДУ имеет четыре позиции: стоп, воспроизведение, запись и перемотка назад, и подключается к диктофону через специальный разъем. Им удобно пользоваться, когда сам диктофон лежит в кармане, включен режим блокировки кнопок и управление диктофоном осуществляется только с самого пульта.

Диктофон Sony M-100MC

Диктофон с записью на микрокассету Sony M-100MC (рис. 2.61) имеет следующие функции:

- голосовую систему активации записи с регулируемой чувствительностью;
- двухпозиционный переключатель скорости ленты (1,2/2,4 см/с);
- регулировку чувствительности и диаграммы направленности микрофона (3 положения — лекция, совещание, диктовка);
- установка и поиск индексных меток;
- обзор в прямом и обратном направлении;
- быстрое воспроизведение (+20 % к нормальной скорости ленты);
- бесшумный автостоп;
- трехуровневый индикатор разрядки батарей и индикатор записи;
- трехразрядный счетчик ленты;
- встроенный динамик;
- гнезда для наушников и сетевого адаптера;
- питание — 2 батарейки типа AA;
- габариты — 126×68×40 мм;
- вес (с батарейками) — 180 г.

Наиболее выделяющаяся деталь конструкции есть не что иное, как встроенный микрофон. Он, в отличие от обычных, является более универсальным, так как может работать в трех различных режимах (один — направленный и

Рис. 2.61. Диктофон Sony M-100MC

два — ненаправленных). К примеру, для записи лекций лучше всего использовать направленный режим, который позволяет наиболее качественно записывать голос лектора, отсекая посторонние звуки. Режим диктовки можно использовать как по прямому назначению, так и для записей в шумных местах. В этом режиме микрофон имеет минимальную чувствительность и фиксирует только близкие и громкие звуки, оставляя «за кадром» весь ненужный шум. Если же ведется беседа с участием нескольких человек (планерка, переговоры и т. п.), то рекомендуется выбрать режим «совещание». В таком режиме микрофон имеет широкую диаграмму направленности и высокую чувствительность, так что от него не ускользнет ни единое слово, даже сказанное шепотом. При помощи специальных откидных «ножек» можно установить диктофон наиболее оптимальным образом, чтобы обеспечить более качественную запись звука.

Диктофоны с записью на микрочип

Диктофон Panasonic RR-DR60

Цифровой диктофон Panasonic RR-DR60 (рис. 2.62) с записью на микрочип обеспечивает максимальную длительность записи — до 60 мин. Этот диктофон относится к плеяде первенцев цифровой технологии, так как был выпущен примерно в одно время с другими пионерами в этой области — Olympus D1000 и Sony ICD-30. Тогда фирма Panasonic была единственной, выпустившей модель с 60-минутной длительностью записи на встроенную микросхему (Olympus, кстати, для записи использовал сменные мини-карты). Для этого, конечно, пришлось пожертвовать качеством записи (голос записывается не очень четко, с шумами), но, с другой стороны, если диктофон использовать как голосовую записную книжку или личный органайзер, то на такие вещи не особо обращаешь внимание.

Особенности цифрового диктофона Panasonic RR-DR60:

- запись на микрочип (возможность записи до 99 сообщений);
- жидкокристаллический дисплей (отображение всех режимов работы, даты и длительности записи, оставшегося времени и заряда батарейки);
- голосовая система активации записи;

Рис. 2.62. Цифровой диктофон Panasonic RR-DR60

- выполнение различных операций при помощи диска Jog Dial (поиск сообщений и перемотка вперед/назад, выборочное и последовательное воспроизведение, остановка воспроизведения, управление режимами);
- удаление одной или всех записей;
- защита от стирания;
- пошаговая перемотка назад внутри сообщений (шаг — 10 с);
- регулируемая скорость воспроизведения (5 уровней);
- регулируемая чувствительность микрофона (5 уровней);
- блокировка кнопок (Hold);
- встроенные динамик и микрофон;
- гнездо для наушников;
- питание — 2 батарейки типа AAA;
- габариты — 56×92×14 мм;
- вес (с батарейками) — 69 г.

Практически все операции с записями выполняются с помощью элементарных действий (поворотов и нажимов) над специальным диском (Jog Shuttle). С его же помощью регулируются чувствительность микрофона, скорость воспроизведения, выставляются дата и часы. При этом на большом дисплее размещается вся необходимая для пользователя информация (номер сообщения, режимы работы, оставшееся свободное время и т. п.).

Цифровые диктофоны Voice It VX-3400 и VX-2200

Цифровые диктофоны Voice It VX-3400 (рис. 2.63) и VX-2200 — продукт американского концерна Voice It Worldwide Inc., специализирующегося на разработке и производстве исключительно цифровых записывающих устройств. Несмотря на то что в России цифровые диктофоны этой фирмы появились не так давно, во всем мире они не менее известны, чем Olympus и Sony.

В линейке диктофонов Voice IT модели VX-3400 и VX-2200 занимают промежуточную позицию между совсем элементарными голосовыми блокнотами, рассчитанными всего на несколько минут записи, и вполне профессиональными устройствами с длительностью записи до 3,5 ч (при дополнительном использовании флэш-карты на 8 Мб), широким набором функций редактирования и возможностью подключения к компьютеру. Памяти аппа-

Рис. 2.63. Цифровой диктофон Voice It VX-3400

ратов вполне достаточно не только для записи текущей информации (срочные дела, каждодневные домашние обязанности, ценные мысли), но и информации длительного хранения (номера телефонов, адреса и т. п.). Чтобы данные в диктофоне не смешивались, существует 4 папки (директории) для разделения их по категориям. Каждой из папок можно дать определенное название (голосовую метку), записав в диктофон соответствующий комментарий (например, «папка для временных сообщений», «папка для адресов и телефонов» и т. п.). Чувствительности встроенного микрофона вполне достаточно для того, чтобы четко фиксировать человеческую речь средней громкости на расстоянии до 1 м. Для наиболее же качественной записи голоса необходимо следовать стандартным рекомендациям — располагать диктофон в 5—10 см от источника звука.

Особенности цифровых диктофонов с записью на микрочип:

- длительность записи (макс.) — 34/22 мин;
- запись на встроенную микросхему (микрочип);
- четыре директории с возможностью записи в каждую до 99 сообщений;
- режимы записи — стандартный SP (17/11 мин), длительный LP (25/16 мин) и расширенный EP (34/22 мин);
- многофункциональный жидкокристаллический дисплей с отображением режима записи, степени заполнения памяти и заряда батарейки; подсветка дисплея;
- питание — 1 батарейка типа AAA;
- габариты — 85×55×15 мм;
- вес — 56 г.

Цифровой диктофон с записью на микрочип Voice It VTR-32

Цифровой диктофон Voice It VTR-32 (рис. 2.64) — один из самых многофункциональных и разносторонних аппаратов среди выпускаемых под маркой Voice It. В 1998 г. на Всемирной выставке электроники CES этот диктофон был оценен строгим мировым жюри как модель, воплотившая в себе самые последние достижения в области цифровой техники, и получил приз за лучшую инновацию.

Рис. 2.64. Цифровой диктофон с записью на микрочип Voice It VTR-32

Среди его огромного количества различных функций и режимов можно было бы легко запутаться, если бы не удачное меню, с помощью которого выставляются дата и время, режимы записи, чувствительность микрофона и даже перемещаются файлы из одной папки в другую (операции производятся всего двумя кнопками). Но все-таки главной отличительной чертой модели является реализация в ней сразу всех известных на сегодняшний день (для цифровых диктофонов) вариантов хранения записанной информации:

- на встроенной микросхеме «флэш-памяти»;
- на стандартной флэш-карте типа Smartmedia (2, 4 и 8 Мб);
- на жестком диске ПК.

Это позволяет заметно расширить возможности аппарата и обеспечивает практически стопроцентную сохранность записей. Например, на длительное интервью можно вместе с диктофоном захватить 4-мегабайтную флэш-карту, увеличивающую общую память ровно в 2 раза. Причем, чтобы случайно не затереть данные при манипуляциях с диктофоном, рекомендуется наиболее важную информацию переписать на карту и с помощью специальной наклейки защитить ее от уничтожения. Впоследствии данные с диктофона или карты можно перенести на винчестер персонального компьютера. Благодаря применению в модели VTR-32 уникальной технологии сжатия информации записи на диске займут в 10 раз меньше места, чем если бы они были в стандартном для звуковых файлов формате *.vaw. При этом с помощью программного обеспечения Voice It Link звуковые файлы можно преобразовывать из сжатого в стандартный формат и обратно, снабжать их текстовыми комментариями, прослушивать прямо на компьютере (при наличии у него звуковой карты и динамика), переписывать обратно на диктофон и, наконец, переводить записанную речь в текст. Для таких целей существуют специальные программы (производства IBM или Dragon Systems).

Цифровой диктофон с записью на микрочип Voice It VTR-32 имеет следующие особенности:

- максимальную длительность записи — 74 мин;
- запись на встроенную микросхему (4 Мб);
- 99 директорий с возможностью записи в каждую до 99 сообщений;

- режимы записи — специальный VT (40 мин, используется для записи речи с последующим переводом в текст), стандартный SP (55 мин) и длительный LP (74 мин);
- многофункциональный жидкокристаллический дисплей с отображением количества сделанных записей, длины и режима записи, даты, степени заполнения памяти и оставшегося заряда батареек;
- подсветку дисплея;
- возможность редактирования сделанных записей (вставка фрагмента внутрь сообщения, вставка комментариев в конце записи, удаление фрагментов записи);
- паузу во время воспроизведения и записи;
- ускоренное и замедленное воспроизведение;
- поиск внутри записи;
- беспрерывное воспроизведение всех записей;
- выставление меток в режиме записи с возможностью поиска или воспроизведения по ним; удаление отдельных сообщений и целых папок;
- установку режимов работы диктофона при помощи меню (выбор чувствительности микрофона — диктовка/конференция, режима записи — VT/SP/LP);
- перемещение записей из папки в папку;
- цифровую индикацию громкости;
- встроенный динамик;
- гнезда для наушников и выносного микрофона;
- слот для флэш-карт;
- питание — 2 батарейки типа AAA;
- габариты — 120×53×20 мм;
- вес — 108 г.

Диктофон Olympus V-90

Дизайн диктофона Olympus V-90 (рис. 2.65) сразу дает понять, что это модель нового поколения цифровых аппаратов. Полтора часа записи, а также огромное количество различных функций — и все это при совершенно миниатюрных размерах.

Красивая форма (в виде «капли») — это не столько дань моде, сколько удобство в управлении диктофоном. Благодаря ей модель V-90 словно «срастается» с рукой, при этом все часто используемые клавиши (запись, воспроизведение, остановка) оказываются в аккурат под самыми активными пальцами — указательным и большим.

На внешней панели под дисплеем располагаются еще три клавиши, с помощью которых осуществляются операции по выбору папок и сообщений, а также поиск по ним. Все остальные режимы работы диктофона задаются путем пролистывания меню. Среди них: выбор скорости записи, регулировка чувствительности при голосовой активации записи, установка часов и будильника.

Стоит особо отметить интересные дополнительные функции, связанные с составлением расписания. Для этого существует специальная папка (S), в которую, как в ежедневник, можно вносить, например, планы на будущее, причем необязательно ближайшее: можно составить даже годовое расписание (ограничившись, правда, только 15 записями). Все сообщения в папке S хранятся строго под установленными для них датами, так что в режиме «листания» найти необходимую дату и воспроизвести соответствующее ей расписание не составляет труда.

Чтобы не забыть о важных делах, можно воспользоваться будильником, который запищит в установленное время, причем после нажатия на любую кнопку диктофон вашим же голосом напомнит о запланированной встрече или совещании.

К особенностям этой модели можно отнести следующие:

- максимальную длительность записи — 90 мин;
- запись на микрочип;
- голосовую систему активации записи с регулируемой чувствительностью (высокая/низкая);
- две папки (A и B) с возможностью записи в каждую до 99 обычных сообщений;
- папку S для записи 99 обычных сообщений или 15 сообщений для будильника и расписания; режимы записи — стандартный SP (33 мин) и длительный LP (90 мин);
- многофункциональный жидкокристаллический дисплей (отображение номера папки, сообщения, режимов работы, даты и времени записи, оставшегося времени для записи, заряда батарейки);
- быстрое воспроизведение (увеличение скорости на 30 %);
- перемотка вперед/назад внутри сообщений;
- стирание одного или всех сообщений в папке;
- перемещение сообщений между папками;
- запись расписания (папка S);
- воспроизведение по установленному будильнику;
- блокировку кнопок (Hold);
- встроенные динамик и микрофон;
- гнездо для наушников;
- питание — 1 батарейка типа AAA;
- габариты — 116×40×16 мм;
- вес (с батарейкой) — 45 г.

Диктофоны Samsung SVR-P350 и SVR-P700

Samsung Electronics, давно и успешно работающая на рынке цифровой техники, решила попробовать себя в амплуа производителя цифровых диктофонов. В 1999 году она выпустила на рынок сразу несколько моделей звукозапи-

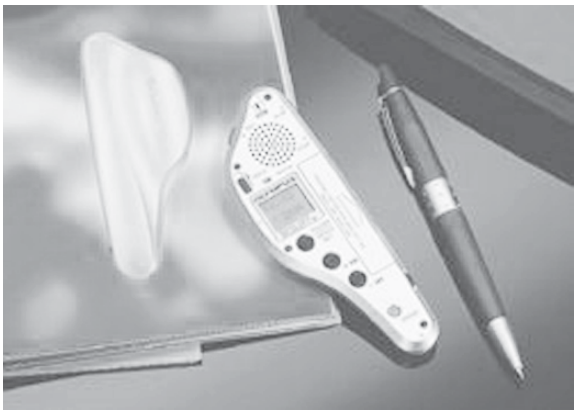


Рис. 2.65. Цифровой диктофон Olympus V-90

Рис. 2.66. Диктофоны Samsung SVR-P350 и SVR-P700

сывающих аппаратов, которые удивили всех своим дизайном и миниатюрными размерами. Модели SVR-P350 и SVR-P700 наиболее соответствуют названию всей серии «Voice Pen» (что переводится как «голосовая ручка»), так как выполнены в стиле дорогих авторучек (рис. 2.66). Имеется даже специальный зажим для крепления к нагрудному карману рубашки. Управлять диктофонами не составляет никакого труда: модели имеют всего три сенсорные клавиши, с помощью которых выполняются все элементарные операции — запись, поиск вперед/назад, воспроизведение или удаление нужного сообщения. Несмотря на то что на одну из клавиш приходится сразу три операции, путаницы, как правило, не возникает. Впрочем, здесь как нельзя кстати приходится сенсорный дисплей — с его помощью намного проще ориентироваться в сделанных записях, контролировать объем свободной памяти и заряд батарейки. Диктофонам вполне по плечу выполнение «шпионских» функций: компактные размеры и маскировка «под ручку» делают их практически незаметными, а отсутствие кассеты и лентопротяжного механизма — еще и бесшумными.

Особенности диктофонов Samsung SVR-P350 и SVR-P700:

- длительность записи на микрочип 35/70 мин;
- возможность записи до 99 сообщений;
- жидкокристаллический дисплей с отображением длительности записи, оставшегося времени и заряда батарейки;
- поиск вперед/назад;
- удаление одной или всех записей;
- встроенные динамик и микрофон;
- гнездо для наушников;
- питание — 1 батарейка типа AAA;
- габариты — 18×143 мм;
- вес (с батарейкой) — 41 г.

Диктофон Samsung SVR-240

Цифровой диктофон с записью на микрочип Samsung SVR-240 (рис. 2.67) на сегодняшний день является безусловным рекордсменом по максимальной длительности непрерывной записи среди цифровых аппаратов. Остается только догадываться, как конструкторам фирмы удалось при использовании стандартной 8-мегабайтной микросхемы флэш-памяти добиться такой длительности при довольно приемлемом качестве записи (до сих пор на 8 мегабайтах удавалось разместить максимум 2,5 ч голосовой информации). Правда, полоса записываемых частот у модели немного у́же, чем у выше описанных (500—3500 Гц у SVR-240 против 300—4000 Гц у SVR-P350 и SVR-P700), но на слух такая разница фактически не ощущается. Зато заметна повышенная чувствительность встроенного микрофона: он хорошо улавливает речь даже на расстоянии нескольких метров от говорящего.

Функционально SVR-240 отличается от других диктофонов Samsung тем, что позволяет регулировать громкость при воспроизведении и делать паузы при записи (длительностью до 30 мин). Последнее свойство особенно пригодится при записи беседы или лекции, проходящей с перерывами (можно все записать в один файл, а не разбивать его на несколько, как у диктофонов без паузы). Это облегчает последующее прослушивание записи и упрощает процесс перенесения и обработки информации на персональный компьютер. Кстати, все диктофоны Samsung имеют возможность сохранения записанных сообщений на внешних устройствах (магнитофонах с линейным входом, компьютерах со звуковой картой и т. п.). Для этого у них предусмотрен стандартный выход и соответствующий соединительный кабель для перезаписи. Возможность записать на такой миниатюрный диктофон до 4 ч информации делает его привлекательным практически для всех категорий потенциальных пользователей. Например, журналисты могут его использовать для записи интервью (с последующим перенесением информации на компьютер и редактированием там), а студенты — для фиксирования лекций (памяти с лихвой хватит для записи двух лекций и еще своих комментариев к ним). Кроме того, модель SVR-240 прекрасно справляется с обязанностями весьма вместительной голосовой записной книжки.

Особенности диктофона Samsung SVR-240:

- максимальная длительность записи — 238 мин;
- запись на встроенную микросхему (микрочип);
- возможность записи до 199 сообщений;
- режимы записи: стандартный SP (118 мин) и длительный LP (238 мин);

Рис. 2.67. Цифровой диктофон Samsung SVR-240

- жидкокристаллический дисплей с отображением длительности записи, оставшегося времени и заряда батарейки;
- пауза при записи;
- поиск вперед/назад;
- удаление одной или всех записей;
- регулировка громкости (10 уровней);
- блокировка кнопок (Hold);
- встроенные динамик и микрофон;
- гнезда для наушников и внешнего микрофона;
- шнур для перезаписи;
- питание — 2 батарейки типа AAA;
- габариты — 15,5×25×125 мм;
- вес (с батарейками) — 56 г;
- дополнительно: наушник; внешний микрофон; адаптер для подключения к телефонной сети.

Обнаружители и подавители диктофонов

Стационарный обнаружитель диктофонов PTRD-016

Стационарный обнаружитель диктофонов PTRD-016 (рис. 2.68) предназначен для выявления попыток несанкционированной регистрации конфиденциальных переговоров диктофонами и другими портативными приборами магнитной записи с электромеханическим приводом. Информативным сигналом для обнаружителя служит электромагнитное поле, создаваемое работающим мотором портативных звукозаписывающих устройств.

Специальная схема адаптивной фильтрации повышает надежность регистрации сигнала на фоне стационарных помех. Модель отличается повышенной помехоустойчивостью, что позволяет использовать обнаружитель в условиях сложной электромагнитной обстановки. Базовая модель прибора состоит из

Рис. 2.68. Стационарный обнаружитель диктофонов PTRD-016

основного блока и четырех датчиков. Датчики устанавливаются стационарно (например, в стол, за которым ведутся наиболее важные переговоры) и через соединительные кабели подключаются к основному блоку. Предусмотрены различные варианты сигнализации, в том числе передача сигнала тревоги по радиоканалу на специальный приемник.

Основные технические характеристики

Дальность обнаружения для каждого датчика, м ..... 0,5—1,2
Количество датчиков, шт. 4
Тип датчиков ..... индукционные преобразователи градиентного типа
Чувствительность датчиков, Тл ..... 10^{-11}
Питание, В 220
Потребляемая мощность, Вт 0,6
Габариты, мм: .....
датчика ..... 230×18×18 или 170×16 (диаметр)
основного блока ..... 180×170×25

Стационарный обнаружитель диктофонов PTRD-018

Стационарный обнаружитель диктофонов PTRD-018 (рис. 2.69) предназначен для охраны помещений от несанкционированного использования портативных звукозаписывающих устройств — диктофонов и им подобной аппаратуры. Система обеспечивает обнаружение работающего в режиме записи прибора, определение его местоположения и времени работы с выводом текущей информации на жидкокристаллический дисплей либо через интерфейс RS-232 на экран монитора. Принцип действия устройства основан на регистрации электромагнитных полей, создаваемых работающим мотором записывающего устройства путем последовательного опроса каждого канала (датчика).

Основные технические характеристики

Дальность обнаружения (в зависимости от типа обнаруживаемого прибора), м ..... 0,5—1,5
Время обнаружения, с ..... 20—30
Количество каналов (в зависимости от варианта поставки) 4, 8, 16
Скорость отображения состояния, с 1,25
Скорость опроса одного канала, с ..... 2—30
Количество градаций уровня сигнала 3
Питание, В 220
Потребляемая мощность, Вт ..... не более 0,8
Габариты чемодана-упаковки, мм ..... 550×350×165
Вес (в зависимости от варианта поставки), кг ..... 9,5—13,5

Рис. 2.69. Стационарный обнаружитель диктофонов PTRD-018

Рис. 2.70. Портативный обнаружитель диктофонов TRD-800

Портативный обнаружитель диктофонов TRD-800

Портативный обнаружитель диктофонов TRD-800 (рис. 2.70) предназначен для обнаружения заукозаписывающих и радиопередающих устройств. Он предоставляет возможность двойного обнаружения: предупреждает об опасности в присутствии активного ВЧ-передатчика (радиомикрофона) корпусного типа, или магнитофона (диктофона), или обоих этих приборов вместе. Реагирует на них TRD-800 также двойственным образом: он снабжен бесшумным вибрационным сигналом тревоги и визуальным предупреждением об опасности, состоящим из трех светодиодных индикаторов. Прибор, в отличие от других устройств обнаружения, не требует постоянного и явного наблюдения за ним, так как вибратор бесшумно и скрытно предупреждает о ВЧ-радиопередачах или записывающих устройствах.

Основные технические характеристики:

Диапазон рабочих частот, МГц ..... 1—1000
Обнаруживаемые устройства ..... разведывательные магнитофоны, видео-, аудиокамеры и электронные подслушивающие ВЧ-устройства
Габариты, мм ..... 222×89
Вес, г 170

Подавитель диктофонов УПД-02

Подавитель диктофонов УПД-02 (рис. 2.71) предназначен для предотвращения несанкционированной записи конфиденциальных переговоров аппаратами магнитной звукозаписи (диктофонами, в том числе с цифровой записью, магнитофонами).

Рис. 2.71. Подавитель диктофонов УПД-02

Изделие представляет собой кейс с вмонтированным в него блоком подавления со встроенной направленной антенной. В результате воздействия излучения изделия на скрытый аппарат магнитной записи на ленту вместо разговора записывается шумовой сигнал.

Устройство рассчитано на работу как в переносном, так и в стационарном варианте, имеет вид обычного кейса, что дает возможность использовать его незаметно для собеседника. Прибор оборудован пультом ДУ.

Основные технические характеристики

Зона подавления ..... сектор с углом не менее 80° и радиусом до 4 м по диктофонам в металлическом корпусе
Время непрерывной работы от встроенных аккумуляторов, ч ..... до 1,5
Питание, В:
50 Гц 220
от аккумуляторов 12
Потребляемая мощность в режиме подавления, Вт ..... не более 60
Габариты, мм ..... 550×450×110
Вес, кг ..... не более 7

2.4. Защита информации от утечки по оптическому каналу

Использование лазерной техники

Для скрытности проведения перехвата речевых сообщений из помещений могут быть применены устройства, в которых передача информации осуществляется в оптическом диапазоне. Чаще всего используется невидимый для простого глаза инфракрасный диапазон излучения. Характеризуются такие изделия крайней сложностью их обнаружения. Срок непрерывной работы — 1—3 суток. Используют эти устройства, как правило, для увеличения дальности передачи информации и размещают у окон, вентиляционных отверстий и т. п., что может облегчить задачу их поиска. Для приема информации применяют специальный приемник ИК-диапазона, который обеспечивает надежную связь на расстоянии 10—15 м.

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 модулирующие колебания.

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 подобных устройств.

Простейший модулятор 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. 2.72.

В качестве модулятора с частотой 50 Гц используется обычное малогабаритное реле постоянного тока *P1*. Питается реле *P1* от сети переменного тока частотой 50 Гц и напряжением 220 В через понижающий трансформатор *T1*. На выводы обмотки реле *P1* подается напряжение со вторичной обмотки трансформатора *T1* немного ниже порога срабатывания. В качестве трансформатора используется любой, желательно малогабаритный, понижающий трансформатор. Напряжение на обмотке *II* выбирается в зависимости от используемого реле. Реле *P1* может быть типа РЭС22, РЭС9 и им подобные. Корпус реле приклеивается к стеклу клеем «Момент» или аналогичным (рис. 2.73).

Если подходящего трансформатора подобрать не удалось, то можно воспользоваться бестрансформаторной схемой устройства (рис. 2.74).

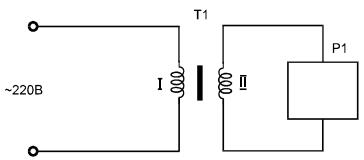


Рис. 2.72. Принципиальная схема простейшего модулятора оконного стекла

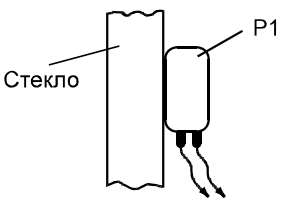


Рис. 2.73. Установка модулятора

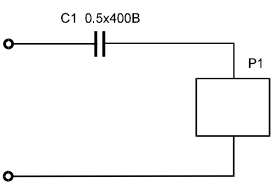


Рис. 2.74. Бестрансформаторная схема модулятора

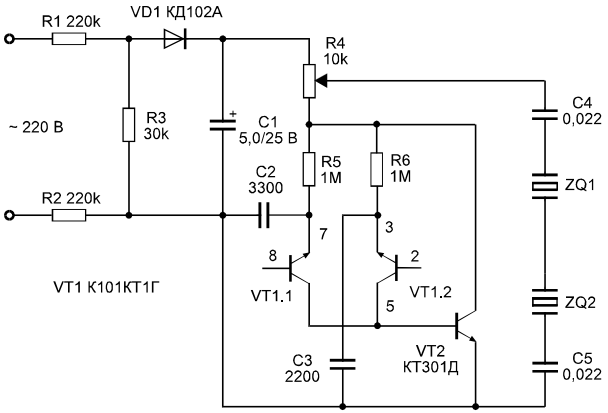


Рис. 2.75. Принципиальная схема модулятора с питанием от сети 220 В

Конденсатор *C1* гасит излишек напряжения, он подбирается под определенную нагрузку. При монтаже его можно разместить прямо в штепсельной вилке.

Этот модулятор позволяет получать сигналы, которые имеют хаотический характер, так как частота следования импульсов не стабильна. Устройство представляет собой два генератора импульсов, частоты которых не стабилизированы и отличаются друг от друга. Оба генератора работают на общую нагрузку. Принципиальная схема модулятора приведена на рис. 2.75.

Питание устройства осуществляется от сети переменного тока напряжением 220 В. Напряжение питания снимается с делителя напряжения на резисторах *R1—R3* и выпрямляется диодом *VD1* типа КД102А. Выпрямленное напряжение сглаживается конденсатором *C1*. Так как у конденсатора *C1* небольшая емкость, то напряжение питания имеет большие пульсации. Оба генератора импульсов собраны на транзисторной сборке *VT1* типа К101КТ1Г, содержащей два идентичных транзистора *VT1.1* и *VT1.2*. Микросборка представляет собой транзисторные прерыватели для коммутации слабых сигналов переменного и постоянного токов. Транзисторы микросборки имеют общий коллектор. Работают генераторы следующим образом. Через резисторы *R5* и *R6* происходит заряд конденсаторов *C2* и *C3*, соответственно, от источника питания. При достижении напряжения на конденсаторах *C2* и *C3* напряжения пробоя транзисторов *VT1.1* и *VT1.2* последние открываются и происходит разряд конденсаторов через базовый переход транзистора *VT2* типа КТ301. Это приводит к открыванию транзистора *VT2,* и короткие импульсы (щелчки, следующие с частотой в сотни герц) поступают на пьезокерамические излучатели *ZQ1* и *ZQ2.* Период времени между импульсами постоянно изменяется, в связи с чем считывание информации со стекол в условиях апериодических акустических полей даже с использованием специальных фильтров сильно затруднено. Громкость звукового сигнала можно плавно регулировать резистором *R4*.

Транзистор *VT2* можно заменить на КТ3102, КТ315. Пьезокерамические преобразователи могут быть любыми, количество — от одного до четырех. Диод *VD1* можно заменить на КД105. Пьезоизлучатели наклеиваются в центре стекла внутренних рам и соединяются с генератором тонким проводом.

Модулятор на одной микросхеме

Этот модулятор тоже питается от сети переменного тока напряжением 220 В. Принципиальная схема модулятора приведена на рис. 2.76.

Напряжение сети гасится резисторами *R1* и *R2* и выпрямляется диодом *VD1* типа КД102А. Конденсатор *C1* 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 *R5*С4. При этом конденсатор *C4* то заряжается через резистор *R5*, то разряжается через него. Поэтому на конденсаторе *C4* получается напряжение треугольной формы, которое используется для управления генератором на элементах *DD1.1, DD1.2*. Этот генератор собран по схеме симметричного мультивибратора. Конденсаторы *C2* и *C3* 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. Нагрузкой генератора служат пьезокерамические излучатели *ZQ1* и *ZQ2* типа ЗП-1.

Микросхему *DD1* можно заменить на К561ЛА7 и даже на К561ЛН1, К561ЛН2 либо на микросхемы серий 564, 1561.

Излучатели *ZQ1* и *ZQ2* могут быть любыми, их количество — от одного до четырех. Они могут быть соединены последовательно или параллельно-последовательно.

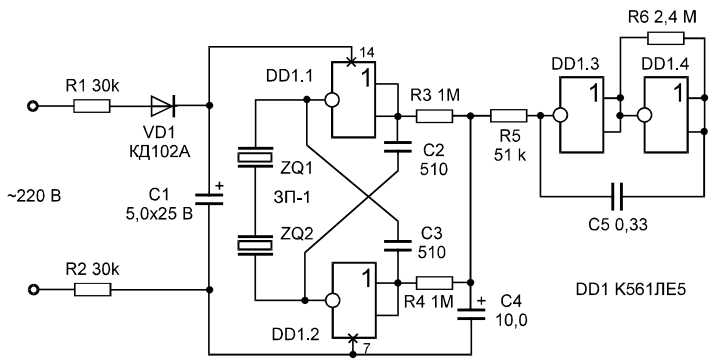


Рис. 2.76. Принципиальная схема модулятора на одной микросхеме

Многочастотный генератор

Фильтрация периодического сигнала не представляет особого труда и может быть выполнена с помощью простого режекторного фильтра. А вот использование многочастотной помехи увеличивает вероятность закрытия полезной информации, так как необходимо применение нескольких, в зависимости от количества используемых частот, точно настроенных фильтров. И чем больше количество частот в многочастотной помехе, тем более сложно выделить необходимую информацию.

Многочастотный генератор, схема которого изображена на рис. 2.77, можно использовать в качестве генератора шума и устанавливать на стекла и рамы (выходным элементом здесь является пьезокерамический излучатель *ZQ1*). Практически это RC-мультивибратор на элементах *DD3.1, DD3.2*, частота которого регулируется включением дополнительных резисторов *R2—R9* параллельно основному *R1*. Таким образом, частота на выходе увеличивается соответственно уменьшению общего сопротивления резисторов.

Изменение тональности происходит циклически с периодом в 8 тактов, при этом с каждым тактом частота может не обязательно последовательно уменьшаться или увеличиваться, значение ее для каждого такта выбирается произвольно, подбором номиналов *R2—R9* соответствующим образом.

Переключение резисторов обеспечивает мультиплексор *DD1* в соответствии с двоичным кодом, поступающим на его входы *1, 2, 4* со счетчика *DD2.*

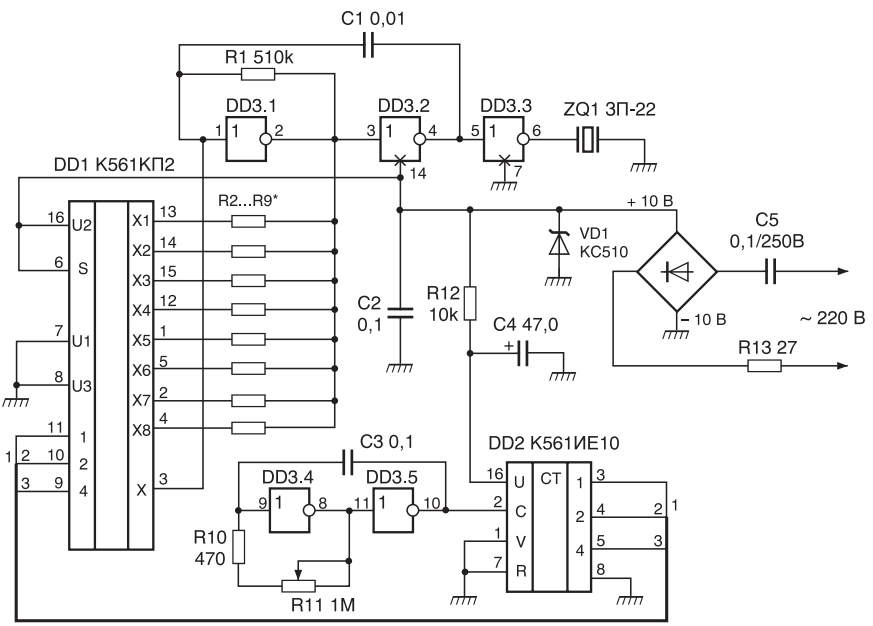


Рис. 2.77. Принципиальная схема многочастотного модулятора

Длительность звучания каждого такта и скорость смены тактов определяется быстротой работы мультиплексора, а следовательно — частотой тактового генератора на элементах *DD3.4, DD3.5,* импульсы от которого поступают на счетный вход счетчика *DD2*. Скорость изменения тактов можно регулировать резистором *R11*.

Если требуется в определенном такте сделать паузу (во время действия этого такта на выходе устройства будет логический нуль), нужно соответствующий вывод мультиплексора соединить не с одним из резисторов *R2—R9*, а с плюсом питания, а соответствующий резистор не устанавливать.

Устройство модуляции стекла на цифровых микросхемах

Данное устройство вызывает вибрацию стекла с различной частотой, тем самым устраняя основной недостаток простейшего модулятора. Оно выполнено на двух цифровых схемах серии 561. В качестве вибропреобразователя используется пьезокерамический преобразователь. Принципиальная схема устройства приведена на рис. 2.78.

Модулятор выполнен 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* (вывод *4*). 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

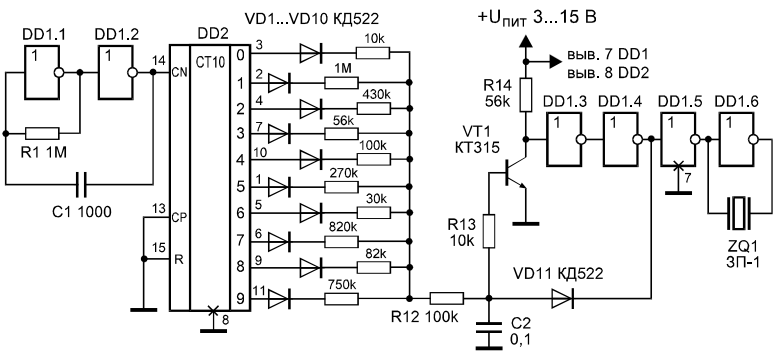


Рис. 2.78. Принципиальная схема устройства модуляции стекла на цифровых микросхемах

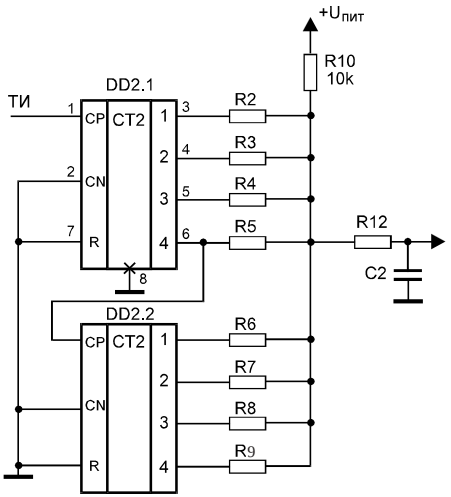


Рис. 2.79. Использование микросхемы К561ИЕ10

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* (вывод *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 «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 (рис. 2.79) 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* в этом случае из схемы исключаются. При подаче тактовых импульсов на вход *CP* микросхемы *DD2.1* в точке соединения резисторов *R2—R12* появляется изменяющееся ступенчато напряжение. Количество градаций напряжения, а следовательно — и число частот, можно варьировать путем использования определенного количества разрядов счетчика DD2.

Скрытая фото- и видеосъемка при помощи специальной оптики

Не нужно обращаться к истории разведки, чтобы сделать вывод о том, что визуальное наблюдение является самым древним и очень эффективным методом сбора информации. В настоящее время для сбора информации могут использоваться миниатюрные скрытые и специальные (камуфлированные под обычные предметы) фото- и видеокамеры:

- миниатюрные (скрытые). Встраиваются в бытовую технику и передают видеоинформацию по кабелю или ВЧ-каналу при помощи телевизионного передатчика;
- специальные, т. е. замаскированные под бытовые предметы, например пачку сигарет, кейс, книгу, наручные часы и т. п.

Аппаратура для скрытой фото- и видеосъемки, как правило, оборудуется специальными объективами и насадками:

- миниатюрными объективами, предназначенными для съемки через отверстия небольшого диаметра (до 5 мм);
- телескопическими объективами, позволяющими вести съемку с дальних расстояний. Такие объективы обладают высокой кратностью увеличения (до 1,5 тыс. крат);
- комуфляжными объективами, используемыми для скрытой съемки из различных бытовых предметов, например из кейсов;
- объективами, совмещенными с приборами ночного видения (с инфракрасной подсветкой) и предназначенными для проведения съемки в темное время суток.

Получение видовых характеристик объекта постоянно совершенствуется благодаря новой аппаратуре наблюдения (телевизионной, инфракрасной видовой, визуально-оптоэлектрической, фотографической). Глаз человека является конечным прибором восприятия визуальной информации. Его возможности существенно повышаются за счет использования различных приборов наблюдения как в видимом диапазоне (бинокли, монокуляры, перископы, телескопы), так и приборов визуализации изображений объекта в ИК-диапазоне, радиолокационных, тепловых и рентгеновских изображений (приборов ночного видения, тепловизоров, рентгеновских аппаратов, РЛС бокового обзора и т. п.)

Объекты получения визуальной информации — самые разные, определяемые заказчиком информации: от сцен неверности супругов, изображений новой техники и ее составных частей до глобального наблюдения за всей поверхностью Земли с целью получения данных по возможному урожаю этого года или расположению войск и средств доставки ядерного оружия.

Получение видовых характеристик объекта является результатом решения трех задач:

- обнаружения — это стадия зрительного восприятия, когда наблюдатель выделяет из окружающего фона объект, характер которого остается для него неясным;

- различения — когда наблюдатель способен определить крупные детали объекта, раздельно воспринимать два объекта, расположенные рядом;
- опознавания (идентификации) — когда наблюдатель, различая отдельные мелкие детали, выделяет существенные признаки объекта и может отличить этот объект от других, имеющихся в его поле зрения.

Видовые характеристики объектов наблюдения могут быть получены либо непосредственно в световом диапазоне, либо путем визуализации изображений в ИК-диапазоне, радиолокационном диапазоне за счет теплового излучения объектов.

Возможность образования визуального канала утечки информации зависит от определенных психофизиологических особенностей восприятия наблюдателем объекта, таких, как:

- угловые размеры объекта;
- уровни адаптационной яркости;
- контраст объект/фон;
- время восприятия;
- зашумленность изображения.

Существенные ограничения могут быть наложены условиями временных характеристик восприятия, что связано с инерциальными свойствами зрения и имеет большое значение при наблюдении за движущимися объектами или объектами кратковременного попадания в поле зрения оператора. При таком наблюдении эффект кратковременности усиливается эффективной яркостью объекта, которая при коротких раздражениях может быть существенно меньше действительной яркости. В этом случае яркостный контраст движущегося объекта может быть значительно меньше неподвижного.

Существенное влияние на получение визуальной информации оказывает состояние трассы наблюдения — от чистого воздуха до очень сильного тумана, что определяет дальность возможного обнаружения и наблюдения объектов.

Много легенд появилось о возможностях спутников видеоразведки. Например, в период американо-иракского кризиса в американской печати много писалось о том, что характеристики их последних спутников видеоразведки позволяют различать членов иракского правительства по формам бороды. Однако в действительности предельная разрешающая способность таких систем ограничивается тем, что съемка ведется через атмосферу Земли, с ее запыленностью и турбулентностью, и поэтому физический предел разрешающей способности лежит от 10—15 см (при «хорошей» атмосфере) и 30 см (при «плохой» атмосфере).

Несмотря на эти ограничения возможности несанкционированного получения информации по визуально-оптическому каналу исключительно важны. Так, например, длиннофокусные фотоаппараты позволяют осуществлять съемку документов, расположенных на стене офиса или столе, на расстоянии до 5 км.

Телескоп РК 6500, выполненный по схеме Шмидта, позволяет опознать автомобиль на расстоянии 10 км. Приборы с электронной стабилизацией изображения позволяют вести наблюдение с рук из движущихся автомобилей и вертолетов.

На рынке технических средств разведки появились в большом количестве миниатюрные фотоаппараты в обычном исполнении и закамуфлированные под различные бытовые предметы — наручные часы, зажигалки и т. п., в том числе фотоаппараты с ДУ. Эти аппараты позволяют снимать копии с документов формата А4—А6, переснимая до 800 документов. А ведь первый миниатюрный фотоаппарат, получивший название «Минокс», был создан всего в 1936 г. в Эстонии. Для него же была изготовлена и первая в мире микропленка.

Такое значительное количество технических средств получения визуальных характеристик объектов и носителей информации, располагаемых на различных носителях, начиная от пуговицы пиджака и заканчивая многотонными спутниками-шпионами, требует от специалистов применения комплекса защитных мероприятий по исключению возможности утечки видовой информации.

Появление и широкое практическое использование световодов позволило получить принципиально новые приборы визуального наблюдения. При их применении приборы наблюдения отходят от традиционной схемы «линии зрения», т. е. наблюдения только за теми объектами, которые находятся на линии видимости глаза или оптической оси прибора. Появилась возможность получения информации из замкнутых помещений — зонд пропускается в замочную скважину или отверстие в стене, и его поворот обеспечивает визуальный обзор внутри помещения.

Расположенная на спутниках-разведчиках аппаратура обеспечивает обзор и получение информации, содержащейся в изображениях различных объектов с разрешающей способностью от 15—30 см до 1 м в зависимости от типа используемой аппаратуры (фотографической, оптико-электронной, в том числе телевизионной, инфракрасной, видовой и т. п.). При разрешающей способности порядка 1—2 м из космоса можно различить типы самолетов, кораблей, автомобилей. Обеспечение же разрешающей способности в 30 см позволяет прочитать бортовые номера самолетов и рассмотреть подвешенное к ним вооружение, сосчитать количество солдат в строю.

Существенно новые возможности раскрываются при использовании зональной фотосъемки в различных частях спектра (как видимого, так и инфракрасного). Появляется возможность выявления замаскированных объектов в лесных массивах.

То, что раньше было уделом спецслужб и новых русских, теперь доступно и простому россиянину. Сегодняшнее состояние российской экономики вынудило как поставщиков, так и торгующие организации снизить цены на оборудование видеонаблюдения.

В качестве примера оборудования для скрытого наблюдения рассмотрим миниатюрную телевизионную камеру JT-241s (рис. 2.80), которая позволяет сделать это наблюдение абсолютно незаметным, информативным и безопас-

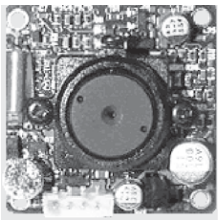


Рис. 2.80. Миниатюрная видеокамера JT-241s

ным. Наиболее эффективно ее использование в системах охраны, системах телевизионного наблюдения, системах скрытого аудиовидеопротокола и т. п.

Сверхминиатюрный зрачок объектива позволяет вести наблюдение через отверстие диаметром 0,3—1,2 мм при угле поля зрения 110°, а высокая чувствительность (0,04 лк) — видеть в темноте лучше, чем человеческий глаз.

Малые габариты телекамеры (39×39×20 мм) позволяют установить ее в любые элементы интерьера: часы, книгу, картину, входную дверь, стену и т. п. На самом деле область применения видеокамер скрытого наблюдения очень широка. Это и возможность следить за детьми в ваше отсутствие, ведь никто не захочет, чтобы его ребенок баловался наркотиками и приводил сомнительных друзей. Особо сомневающимся в лояльности своих подчиненных начальникам не помешает камера, скрыто установленная, например, в офисных часах. Ну а если вы — начальник службы безопасности, то вы поймете, что саботаж против видеокамеры, которую невидно, не возможен. Для органов правопорядка просто незаменима носимая система скрытой видеозаписи.

Преобразователи света для CCTV телекамер NiteMate 1305/1306

Преобразователи света для CCTV телекамер NiteMate 1305/1306 (рис. 2.81) — это революционное решение задач скрытого наблюдения в ночное время. При работе этого прибора с существующими типами телекамер достигается разрешение в 425 TVL при полном отсутствии освещения (0,00001 люкс).

Видеоизображение с выхода прибора поступает в телекамеру с матрицей 1/2" или 2/3" через преобразующий объектив, находящийся внутри корпуса

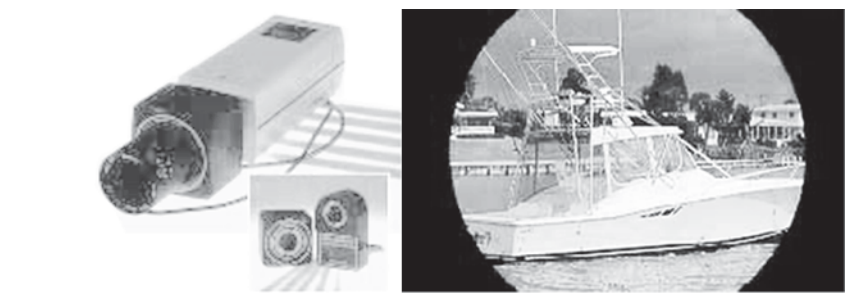


Рис. 2.81. Преобразователи света NiteMate 1305/1306 и пример их использования

прибора. Для улучшения показателей работы рекомендуется использование телекамер с разрешением по горизонтали в 550 TVL и чувствительностью в 0,1 люкс.

Обе модели преобразователя NiteMate 1305 и 1306 имеют сверхкомпактный дизайн, легкий вес и скомпонованы для работы в экстремальных внешних условиях. Содержащийся в приборе высоковольтный блок питания требует всего 12 В постоянного тока при потребляемой мощности 600 мВт.

Модификация 1305 легко крепится к любой стандартной CCD-камере формата 2/3" с креплением C или CS. Таким же образом 1306 крепится к любой камере формата 1/2". Разработанный первоначально для ночного наблюдения, прибор NiteMate можно также использовать в дневное время при использовании объектива формата 1" T1500 с автозатвором.

Преобразователь NiteMate чувствителен в области дневного и инфракрасного спектра света и позволяет получать усиление света на выходе, превышающее входное в 25 000 раз. В результате NiteMate позволяет намного увеличить радиус обзора даже при низкой освещенности.

Основные технические характеристики NiteMate

Рабочий температурный режим, °C	–19...+50
Температурный режим хранения, °C	–34...+69
Допустимая влажность, %	95
Питание:	
источник постоянного тока, В	12
потребляемая мощность, мВт	600
Вес, г	369

Карманный монокуляр ночного видения NiteMate NAV-3

Карманный монокуляр ночного видения NiteMate NAV-3 (рис. 2.82) основан на использовании фотокатодной технологии арсенида галлия. Имеет встроенную инфракрасную подсветку, чувствительность до 0,00001 люкс, автоматический контроль яркости. Полный комплект включает адаптеры для работы прибора с 35-миллиметровыми фотокамерами и видеокамкордерами.

В комплект прибора входят:

- защитный резиновый видоискатель;
- стандартный объектив с фокусным расстоянием 25 мм F1,4;
- ремень с креплением для ношения;
- адаптер для 35-миллиметровых фотокамер SLR с диаметром резьбы 49 мм;
- адаптер для видеокамкордеров с диаметром резьбы 37 мм;
- одна алкалиновая батарея AA-типа;
- футляр для хранения;

Рис. 2.82. Монокуляр ночного видения NiteMate NAV-3 и его использование

дополнительное оборудование:

- шлемофон-комплект для крепления прибора на голове и работы со свободными руками;
- конверсионный объектив для работы прибора с CCTV (CCD) телекамерами.

Основные технические характеристики

Тип фотокатода	GaAs
Чувствительность, нА/люм	1100
Угол обзора, град.	40
Эквивалентная яркость на входе, л/см2	$3{,}0\times10^{-11}$
Выходная яркость (FL/FC),	20 000—30 000
Крепление объектива	С-типа
Предельное разрешение, lp/мм мин	36
Фокусное расстояние, мм	25
Внешняя матрица	оптоволокно,180° инвертор
Фосфорный экран	П20/П43
Питание	одна алкалиновая батарея АА-типа
Время беспрерывной работы, ч	8
Габариты, мм	95×50×73
Вес, г	260

Лазерный локатор ночного видения SEA LYNX

Системы SEA LYNX работают в пассивном, активном и импульсном режимах, что, в отличие от известных аналогов, позволяет наблюдать выделенные объекты на определенных расстояниях, в том числе с отсечением яркого фонового света, в условиях тумана, пурги и т. п.

Лазерный локатор ночного видения SEA LYNX (рис. 2.83) обеспечивает значительное улучшение контроля обстановки и охраны территорий, в том числе в условиях полного отсутствия освещения, в условиях снега, дождя, тумана. Прибор имеет CCIT ТВ-выход, воз-

Рис. 2.83. Лазерный локатор ночного видения SEA LYNX

можность видеодокументирования и сопряжения с другими техническими и навигационными системами, а также позволяет автоматически определять расстояния. Возможность полного компьютерного контроля и работы в автоматическом режиме позволяют реализовать автоматическую защиту от ослепления случайными вспышками света.

Таблица 2.5. **Режим работы лазерного локатора ночного видения**

Режим работы	Активный	Пассивный	Импульсный
Дистанция обнаружения лодки, м	500	700	1000
Дистанция идентификации лодки, м	150	300	600

Основные технические характеристики

Глубина зоны подсветки, м ..... 50—350
Горизонтальный угол обзора, град ..... 506×4,8 (9×6,5)
ТВ-разрешение, ТВ-линий 450
Рабочее напряжение ..... 24 В (DC) или 220 V (AC)
Потребляемая мощность, Вт 60
Габариты и вес, мм/кг:
электронно-оптического блока ..... 190×430×370/15
9-дюймового монитора ..... 230×250×220/6
блока ручного управления ..... 95×350×305/10

Перечень техники фото- и видеосъемки можно было бы продлить, но вероятность ее использования частными лицами очень мала из-за сложности в эксплуатации и большой стоимости.

ГЛАВА ТРЕТЬЯ

ПОЛУЧЕНИЕ ИНФОРМАЦИИ ИЗ СРЕДСТВ СВЯЗИ

3.1. Контроль телефонных каналов связи

Ежедневно, говоря по телефону, вы даже не задумываетесь о том, что вас могут подслушивать. В результате содержание самых важных разговоров (деловая, стратегически ценная, компрометирующая информация) становится известно именно тем людям, которые не должны ничего о нем знать. Как только ваши телефонные переговоры заинтересуют кого-либо, находится простое решение — подслушать их. Каждый раз, когда вы поднимаете трубку телефона у себя дома или в офисе, на телефонной линии включаются специальные радиопередатчики или диктофоны; для того чтобы прослушать ваш разговор, достаточно просто подключить к ней параллельный аппарат или телефонную трубку.

Телефон, будучи самым используемым инструментом при человеческом общении, предоставляет уникальные возможности для незаметного проникновения в личную и деловую жизнь своего владельца. Он является одним из основных способов несанкционированного доступа к информации частного и коммерческого характера. Ценность информации, передаваемой по телефонным линиям, вызывает наибольшее беспокойство у организаций и частных лиц за сохранение конфиденциальности своих переговоров именно по телефонным каналам. Для защиты своих секретов необходимо знать методы, с помощью которых могут быть осуществлены операции по перехвату. Но при этом нужно учесть, что организация массового прослушивания (в существовании которой убеждены очень многие) невозможна по причинам технического и финансового характера — для анализа записанных сообщений нужно держать огромное количество людей и техники. Как утверждал бывший глава КГБ В. Бакатин, 12-й отдел КГБ прослушивал в Москве примерно 300 абонентов. Но с 1994 г. на наших телефонных станциях, станциях сотовой связи и других стала внедряться система СОРМ. Что же это за зверь такой? СОРМ — это система технических средств по обеспечению оперативно-розыскных мероприятий на отечественных и импортных электронных телефонных станциях, предназначенная для оперативного контроля соединений определенных абонентов из удаленного пункта управления правоохранительных органов, который имеет абсолютный приоритет даже перед оборудованием АТС, путем вза-

имодействия этого пункта с оборудованием станций. Максимальное количество номеров телефонов контролируемых абонентов на ЭАТС определяется из расчета 128 для станции емкостью 10 000 номеров, но не должно превышать 1024 при увеличении емкости станции до максимальной. Количество номеров телефонов контролируемых абонентов сети не превышает 1024 при любой емкости станции, при этом СОРМ на ЭАТС должна обеспечивать одновременный контроль 168 абонентов.

Если говорить вкратце, то эта система позволяет:

- контролировать исходящие и входящие вызовы (местных, внутризоновых, междугородных и международных) к/от определенных абонентов данной станции;
- контролировать вызовы при предоставлении абонентам дополнительных видов обслуживания, изменяющих направление вызовов (переадресация) или номерную информацию по ним (сокращенный набор номера);
- по команде из пункта управления осуществлять разъединение установленного соединения абонента, блокировку входящих и (или) исходящих соединений;
- по команде из пункта управления конспиративно подключаться к любым абонентским линиям (каналам), в том числе находящимся в состоянии установленного соединения, и осуществлять запись разговоров;
- по каждому контролируемому вызову иметь/получать данные:
  порядковый номер контролируемого абонента;
  категорию контроля;
  номер контрольной линии (канала) при полном контроле;
  отметку о полуавтоматической входящей связи;
  цифры номера телефона вызываемого абонента;
  номер телефона вызывающего абонента до ответа вызываемого абонента при внутристанционной связи;
  номер телефона вызывающего абонента после ответа вызываемого абонента при входящей связи от других станций;
  номер входящего пучка соединительных линий (при невозможности определения номера вызывающего абонента);
  время начала разговора;
  время разъединения и др.

Однако для организации такого прослушивания в настоящее время требуется санкция прокуратуры. Более вероятна организация прослушивания без санкции в коммерческих или других целях. По американским данным, вероятность утечки информации по телефонным каналам составляет от 5 до 20 %.

Прослушивать удается как ведущиеся телефонные переговоры, так и все беседы в комнате при положенной на рычаг трубке, с регистрацией содержания переговоров как «на слух», так и с применением автоматической записи на магнитную ленту.

Способы, которыми может вестись прослушивание телефонных линий и какая при этом используется аппаратура, наглядно представлены на рис. 3.1. Рассмотрим кратко эти способы.

Общепринятые способы подслушивания контролируемого телефона следующие:

- непосредственное подключение к телефонной линии:
  - контактное — последовательное или параллельное (прямо на АТС, где-нибудь на линии, в произвольном месте между телефонным аппаратом и АТС);
  - бесконтактное (индукционное) подключение к телефонной линии;
- помещение радиоретранслятора («жучка») на телефонной линии:
  - последовательное включение;
  - параллельное включение;
- прослушивание через звонковую цепь;
- внутрикомнатное прослушивание с применением ВЧ-накачки;
- встраивание в аппарат «жучка», активизируемого по коду через любой дальний телефон;
- встраивание в аппарат «жучка», временно блокирующего рычаг трубки в ходе опускания ее после ответа на обычный телефонный звонок.

Непосредственное подключение к телефонной линии осуществляется на телефонной станции либо на любом участке линии от телефона до АТС, причем чаще всего в распределительной коробке в зоне дома, где обычно производится разводка кабеля. Чтобы обнаружить нужные провода, подсоединяют переносную телефон-трубку к любой паре промежуточных контактов и набирают номер объекта, проскользив кончиками пальцев, завалявшейся монеткой, неоновой лампой или светодиодным пробником по отдельным клеммам, регистрируют (через удар током, сильное искрение, вспыхивание светодиода) явно повышенное (до 100 В и более) напряжение вызова. Отыскав подобным образом требуемую линию, от нее пробрасывают к близлежащему посту прослушивания либо установленному невдалеке магнитофону неприметную отводку, причем в качестве последней можно задействовать всегда имеющиеся в кабеле неиспользованные провода.

Так как АТС переключает линию на разговор при шунтировании ее сопротивлением порядка 1000 Ом, применение для подслушивания аппаратуры с низкоомным входом вызывает перегрузку телефонной сети и падение напряжения с вероятностью обнаружения подключения. Поэтому параллельный телефон подсоединяют через сопротивление номиналом в 600—1000 Ом. Заурядные демаскирующие признаки плохо выполненного подключения проявляются прежде всего в щелчках и перепадах громкости, возникающих при разговоре в контролируемом телефоне.

Индукционное подсоединение к телефонной линии позволяет уклониться от непосредственного контакта с телефонной сетью, поэтому его довольно трудно обнаружить. Принцип действия такой отводки строится на том, что

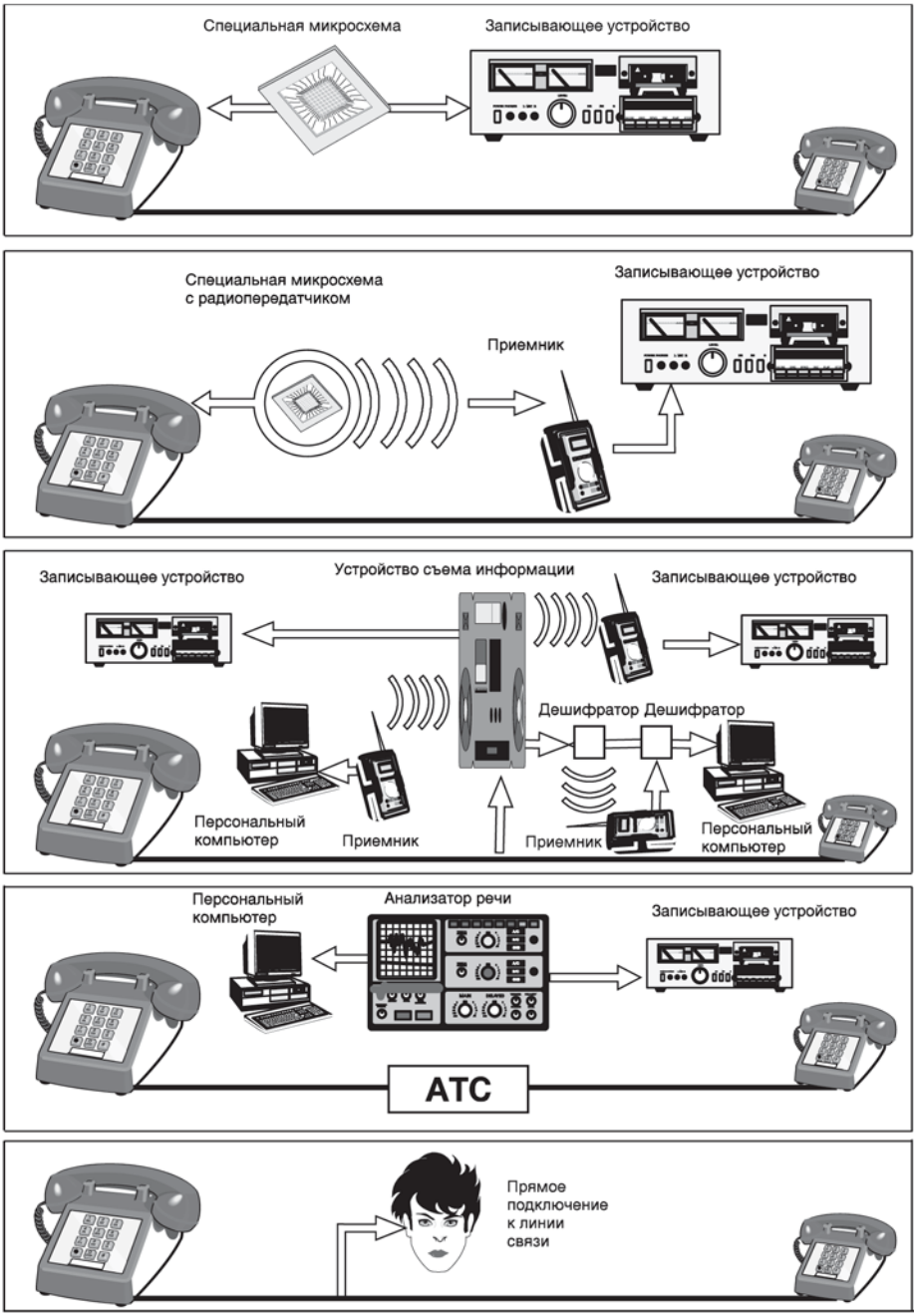


Рис. 3.1. Способы прослушивания телефонных линий

вокруг обычных проводов при проходе по ним электрического тока возникает электромагнитное поле, наводящее индукционный ток в расположенном поблизости проводнике. Для реализации этого эффекта один из проводов наружной линии обматывают вокруг миниатюрной многовитковой катушки с ферромагнитным сердечником либо размещают его вблизи подобной же катушки в броневом сердечнике. Выводы импровизированного трансформатора подсоединяют к усилителю низкой частоты, диктофону или микропередатчику. Недостаток подобного приема заключается в довольно незначительной величине засекаемого сигнала, требующего обычно дополнительного усиления, и в явной склонности такого датчика реагировать на посторонние электромагнитные влияния. Радиопередатчик (радиомикрофон, радиоретранслятор), подключенный к телефонной линии, часто используют, когда применение демаскирующих отводок вызывает некоторые затруднения. Он превосходно ретранслирует циркулирующую информацию в место, где установлен приемник. Различают два способа такого подключения, известные как последовательное и параллельное.

В первом случае миниатюрный передатчик включают в разрыв линии и питают его электроэнергией линии только в момент разговора. Это позволяет ретранслятору действовать неограниченно долго, но вот напряжение в сети несколько снижается, что может привести к его обнаружению.

Во втором стандартном варианте передатчик подсоединяется параллельно линии и обеспечивается, в зависимости от тока потребления, питанием от линии или своим автономным источником питания. Данный образец сложнее обнаружить (передается бросок тока в линии только в момент подсоединения), но период его автономной работы может ограничиваться емкостью применяемых батарей (которая, впрочем, тратится лишь в периоды использования телефона). В конструктивном исполнении все эти устройства представляют маломощные, преимущественно транзисторные генераторы ультракоротких волн (27—900 МГц), несущие которых модулированы перепадами тока, возникающими в линии при телефонном разговоре. Действуют они нередко на частотах радиовещательного диапазона (66—74 и 88—108 МГц), что дает возможность принимать их передачи на обычный УКВ-радиоприемник в радиусе десятков-сотен метров, хотя в этом случае передаваемую информацию могут слушать и другие, совершенно посторонние люди.

При возможности миниатюрный передатчик вмонтируется прямо в телефонный аппарат, с тем чтобы он нагло перехватывал не одни лишь телефонные переговоры, но и прочие беседы в данной комнате.

Не мешает знать, что многочисленные телефоны с кнопочным набором номера сами являются источниками паразитных радиоизлучений, так что разговоры, проводимые, к примеру, с применением аппарата ВЭФ ТА-12, можно пробовать засечь на частоте ДВ-диапазона (около 150 кГц) на дистанции в сотню-другую метров.

Весьма распространенным способом раскрытия ваших секретов является подкуп обслуживающего персонала на АТС. Особенно это касается неболь-

ших городов, где до сих пор используются старые декадно-шаговые АТС. Скорее всего, таким способом могут воспользоваться преступные группы либо конкурирующие фирмы.

Непосредственное подключение к телефонной линии

Непосредственное подключение к телефонной линии — наиболее простой и надежный способ получения информации. В простейшем случае применяется трубка ремонтника-телефониста, подключаемая к линии в распределительной коробке, где производится разводка кабелей. Чаще всего это почерк «специалистов» нижнего звена уголовного мира (верхнее звено оснащено аппаратурой не хуже государственных секретных служб). Необходимо помнить, что АТС переключает линию на разговор при шунтировании ее сопротивлением около 1 кОм. Применение аппаратуры подслушивания с низкоомным входным сопротивлением можно достаточно быстро обнаружить. Если вы услышите щелчки в линии или перепады громкости, есть вероятность того, что вас пытаются прослушать не совсем профессиональным способом. Кроме того, существуют различные электронные устройства, позволяющие контролировать состояние телефонной линии. Принципиальные схемы некоторых из них мы рассмотрим ниже.

Эти устройства в лучшем случае засекают изменения напряжения в цепи, но не могут определить однозначно — установлено устройство съема информации или нет. Для того чтобы убедиться в том, что ваша линия чистая, вам потребуется помощь профессионала с хорошей репутацией и современным оборудованием. Этот процесс дорогой и занимает много времени, но даже в этом случае нет абсолютной уверенности в том, что у вашего противника нет еще более современной техники, чем у того человека, которого вы наняли. Как говорится в недавнем заключении одной государственной организации, «не существует оборудования по борьбе со средствами электронной борьбы, которое могло бы определить наличие хорошо установленного подслушивающего устройства на линии». Тем не менее хорошей идеей будет регулярная проверка ваших телефонных линий.

Прослушивание через электромагнитный звонок

Телефонные аппараты, где в качестве вызывного устройства используется электромагнитный звонок, пока еще широко распространены в нашей стране. Звонок обладает свойством дуальности, т. е. если на электромагнитный звонок действуют звуковые волны, он начнет вырабатывать соответствующим образом модулированный ток. При разговоре в помещении акустические колебания воздействуют на маятник звонка, соединенного с якорем электромаг-

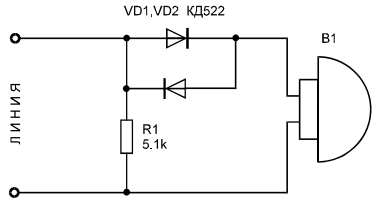


Рис. 3.2. Схема защиты звонковой цепи

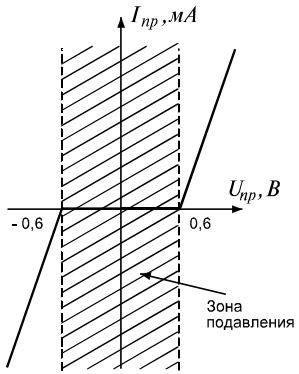


Рис. 3.3. Вольт-амперная характеристика диодов

нитного реле. Под воздействием звуковых сигналов якорь совершает микроколебания, что, в свою очередь, вызывает колебания якорных пластин в электромагнитном поле катушек, следствием чего является появление микротоков, промодулированных звуком. Амплитуда его достаточна для дальнейшей обработки. Корпус аппарата является дополнительным резонирующим устройством.

Эксперименты показали, что амплитуда ЭДС, наводимая в линии, для некоторых типов телефонных аппаратов может достигать нескольких милливольт. Для приема используется НЧ-усилитель с частотным диапазоном 300—3500 Гц, который подключается к абонентской линии. Для защиты от такого канала утечки информации используется схема, представленная на рис. 3.2.

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 (вольт-амперная характеристика диодов представлена на рис. 3.3).

Поэтому низкочастотные токи, наводимые в схеме аппарата, не пройдут в линию. В то же 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.

Вместо указанных на схеме диодов можно использовать диоды Д226, КД105, КД102.

Прослушивание через микрофон телефонного аппарата

Этот способ не является синонимом непосредственного подключения к линии. Он гораздо сложнее. Микрофон — часть электронной схемы телефонного аппарата: он либо соединен с линией (через отдельные элементы схемы) при разговоре, либо отключен от нее, когда телефонный аппарат находится в готовности к приему вызова (трубка находится на аппарате). На первый взгляд, когда трубка лежит на аппарате, нет никакой возможности использовать микрофон в качестве источника съема информации. Но это только на первый взгляд. На рис. 3.4 приведена схема прослушивания помещения способом, называемым ВЧ-навязыванием.

Промодулированный высокочастотный сигнал демодулируется амплитудным детектором и после усиления готов для прослушивания или записи. Дальность действия такой системы из-за затухания ВЧ-сигнала в двухпроводной линии не превышает нескольких десятков метров.

Суть этого способа состоит в следующем. На один из проводов телефонной линии, идущий от АТС к телефонному аппарату *TA2*, подаются колебания частотой 150 кГц и выше от генератора *Г*. В этом случае ВЧ-колебания проходят через микрофон или элементы схемы телефонного аппарата *TA2,* обладающие «микрофонным эффектом», и модулируются акустическими сигналами прослушиваемого помещения. К другому проводу линии подключается детектор, выполненный на элементах *C1*, *C2*, *VD1*, *VD2* и *R1*. Детектор приемника выделяет речевую информацию, которая усиливается до необходимого уровня и обрабатывается. Корпус передатчика (генератор *Г*) и приемника (детектор) соединены между собой или с общей землей, например с водопроводной трубой.

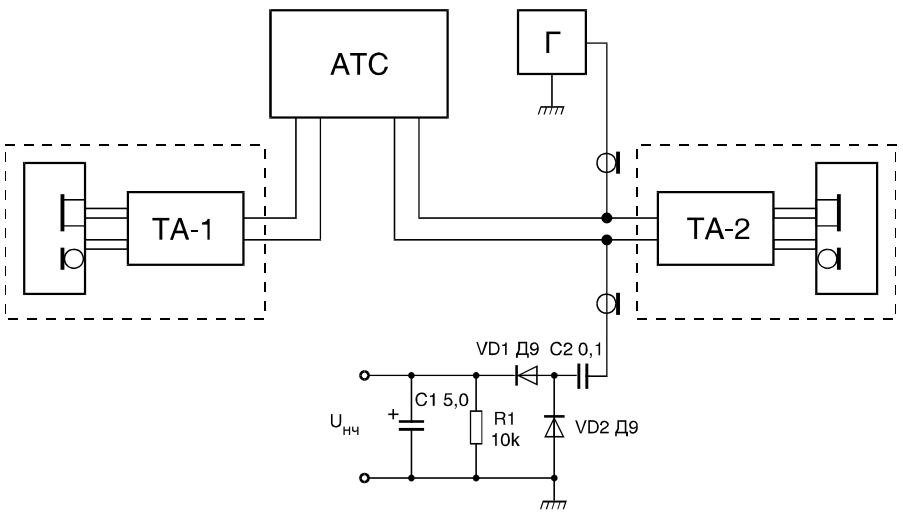


Рис. 3.4. Схема прослушивания способом высокочастотного навязывания

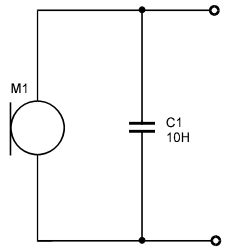


Рис. 3.5. Схема защиты телефонного аппарата

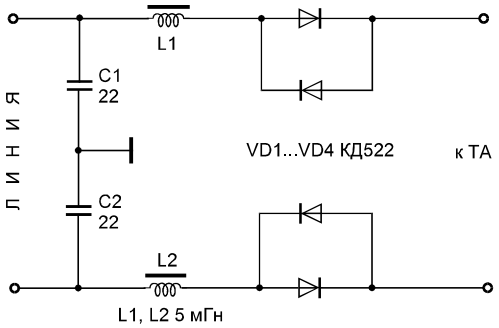


Рис. 3.6. Комплексная схема защиты

Схема защиты телефонного аппарата от этого метода съема информации представлена на рис. 3.5.

Так как модулирующим элементом является микрофон *M1* телефонного аппарата, то для его защиты достаточно подключить параллельно микрофону *M1* конденсатор *C1* емкостью 0,01—0,05 мкФ. При этом конденсатор *C1* шунтирует по высокой частоте микрофонный капсюль *M1*. Глубина модуляции ВЧ-колебаний уменьшается более чем в 10 000 раз, что делает практически невозможной дальнейшую демодуляцию сигнала.

Комплексная схема защиты представляет собой сочетание двух схем, приведенных ранее. Кроме конденсаторов и резисторов схема, представленная на рис. 3.6, содержит катушки индуктивности.

Диоды *VD1—VD4*, включенные встречно-параллельно, защищают звонковую цепь телефона. Конденсаторы и катушки образуют фильтры *C1*, *L1* и *C2*, *L2* для подавления напряжений высокой частоты.

Детали монтируются в отдельном корпусе навесным монтажом. Устройство не нуждается в настройке. Однако оно не защищает пользователя от непосредственного подслушивания путем прямого подключения в линию.

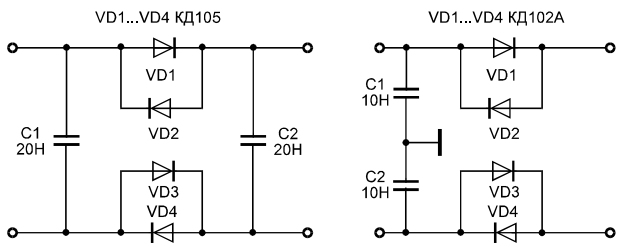


Рис. 3.7. Практические схемы комплексной защиты телефонных аппаратов и линий связи

Кроме рассмотренной схемы существует и ряд других, которые по своим характеристикам близки к ранее описанным устройствам. На рис. 3.7 приведены схемы, предназначенные для комплексной защиты телефонных аппаратов и линий связи и часто используемые в практической деятельности.

Анализаторы телефонных линий

Анализаторы телефонных линий можно разделить на индивидуальные сигнализаторы и тестовые комплекты. Индивидуальные сигнализаторы устанавливаются на заранее проверенную линию и служат для контроля ее параметров. Часто такие сигнализаторы называют «телефонными стражами». Телефонный страж обычно выполняется в виде розетки с двумя светодиодами (рис. 3.8): зеленый — «Линия чиста», красный — «Тревога! Параметры линии изменились». Плюсом таких стражей является простота эксплуатации, минусом — высокая вероятность «ложной тревоги». Эти устройства обычно контролируют только напряжение в линии.

Тестовые комплекты предназначены для проверки линии специалистами. Такой комплект посылает в линию зондирующий сигнал и анализирует ответный сигнал, по которому определяет наличие в линии каких-либо радиоэлементов, присущих цепям съема и передачи информации.

Существуют различные системы для предотвращения несанкционированного прослушивания телефонных переговоров, факсов и модемной связи. Принцип действия таких систем заключается в том, что они подавляют нормальную работу телефонных закладок всех типов (последовательных и параллельных) и диктофонов, установленных на вашей телефонной линии от места установки до АТС. Результатом работы устройств является «размывание спектра» излучения телефонной закладки, что делает невозможным прием информации от нее, а также «забивание» системы АРУЗ и выведение из строя системы VOX (система автоматического включения при наличии на линейном входе сигнала определенного уровня) диктофонов, подключенных к линии.

В результате становится крайне затруднительно перехватить ваши телефонные разговоры обычными средствами прослушивания как зарубежного, так и отечественного производства.

Устройства контроля напряжения линии

Устройства контроля напряжения линии образуют наиболее многочисленную группу приборов обнаружения, представленных на рынке спецтехники. Приборы данной группы регистрируют изменение напряжения линии с помощью компараторов или вольтметров. При этом если напряжение на линии изменяется на достаточную величину, то делается вывод о гальваническом подключении к линии. Основным недостатком всех приборов данной группы является то, что они должны быть установлены на «чистую» линию, т. е.

Рис. 3.8. Телефонный страж

выявляются только новые гальванические подключения к линии. Например, все приборы данной группы успешно выявляют «поднятие» трубки параллельного телефона в момент проведения переговоров по линии или подключение к линии «новых» телефонных закладок с питанием от линии (последовательных — с сопротивлением более 0,1 кОм, параллельных — с сопротивлением менее 100 кОм). При измерении напряжения линии с помощью вольтметров или компараторов следует учитывать «естественные» колебания напряжения линии в пределах до 1 В, зависимость параметров линии от температуры, влажности, состояния оборудования АТС, сопротивления переходных колодок и других факторов. На рынке спецтехники широко представлены недорогие анализаторы напряжения линии на основе компараторов: ЛСТ-1007, АЛ-2, АТЛ-2, АТЛ-3, АТ-21, «Скат-3», «Скат-4» и др. Часто анализаторы напряжения линии встраивают как составные части в более сложные приборы защиты переговоров по телефонной линии (например, в генераторы помех). К таким приборам можно отнести: «Атолл», АТ-23, «Барьер-3», КЗОТ-06, «Прокруст», «Протон», SI-2020, УЗТ-01 и т. д. В любом случае чувствительность приборов контроля напряжения линии невысока и ограничена нестабильностью параметров телефонной линии. Замена телефонного аппарата требует перенастройки прибора, а при первом подключении необходима проверка линии на «чистоту» другими техническими средствами. Ниже приведены практические схемы подобных телефонных стражей — анализаторов линии.

Световой анализатор телефонной линии

Данное устройство 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 (включается красный светодиод). Схема такого устройства приведена на рис. 3.9.

Устройство состоит из анализатора линии, собранного на стабилитроне *VD2* типа КС530 и транзисторе *VT1* типа КТ503, и усилителя тока, выполненного 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.

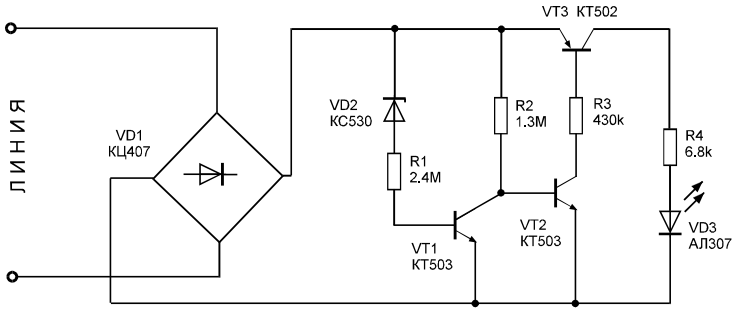


Рис. 3.9. Принципиальная схема светового анализатора телефонной линии

При свободной линии постоянное напряжение в ней около 60 В. Стабилитрон *VD2* «пробивается» (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.

Индикатор 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. Принципиальная схема индикатора приведена на рис. 3.10.

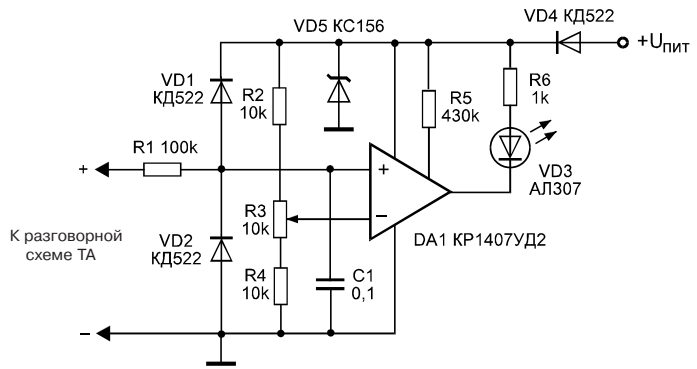


Рис. 3.10. Принципиальная схема индикатора линии на микросхеме

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 КС156 параметрический стабилизатор напряжения. Одновременно напряжение поступает через резистор *R1* на неинвертирующий 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 неинвертирующем 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 ВЧ-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 В. Микросхему *DA1* можно заменить на КР140УД1208, а также на любой операционный усилитель с током потребления не более 5 мА.

Устройство настраивают по методике, приведенной ниже. Сняв трубку телефонного аппарата и установив разговорное соединение (позвонив, например, знакомым), 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. Светодиод снова гаснет, прибор настроен. Он будет реагировать как на параллельное подключение к линии, так и на последовательное подключение.

Необходимо соблюдать полярность включения прибора!

Устройство защиты от несанкционированного подключения к телефонной линии

Устройство защиты от несанкционированного подключения к телефонной линии предназначено для кодирования линии индивидуальным одно-, двух-, трехзначным кодом и применяется в тех случаях, когда имеется возможность установить устройство защиты в щитке, колодце, т. е. как можно дальше от охраняемого телефонного аппарата (в идеальном случае — на выходных клеммах АТС). Система охраняет линию «за собой». При этом все посылки вызова, пришедшие с АТС, беспрепятственно допускаются к телефону, но для подключения к линии (ведения разговора, набора номера) на диске телефона (клавиатуре) необходимо набрать индивидуальный код.

Схема системы приведена на рис. 3.11. Устройство собрано на дискретных общедоступных элементах и микросхеме серии 561 с микропотреблением в статическом режиме. Вся схема питается от телефонной линии. В режиме ожи-

дания потребление не превышает 10—20 мкА, в режиме приема вызова или обработки кода — 150—200 мкА.

В состав устройства входят:

- узел обработки импульсов вызова на элементах *DD1.1, DD1.2;*
- узел приема кода на элементах *DD1.3, DD1.4;*
- ключ включения телефона *A1;*
- дешифратор кода *A2;*
- узел питания на элементах *VD7, R3, C6, VD8;*
- узел питания напряжением 60 В на элементах *VD10, R8, VD9, C7, R7, VD11—VD13.*

Рассмотрим работу системы защиты.

Исходящая связь

При снятии трубки с телефона, подключенного в любом месте охраняемой части линии, в телефоне будет отсутствовать сигнал готовности станции (425 Гц). После набора соответствующего кода на диске (клавиатуре) телефона и обработки его узлом приема кода *DD1.3, DD1.4* на выходе *4* дешифратора *A2* появится уровень логической единицы, который через ключ *A1* подключит телефон к линии (если код набран правильно).

Если код набран неправильно, система защиты блокируется на время 15—30 с, после чего можно повторить набор кода. При включении ключа *A1* телефон работает в обычном режиме, обеспечивая набор номера и связь. Система вновь входит в режим охраны через 10—20 с после того, как трубка будет опущена на аппарат.

Входящая связь

Любая посылка вызова частотой 25 Гц и напряжением 90—120 В, пришедшая от АТС, напрямую на телефон не поступает, так как ключ *A1* в исходном состоянии заперт. После обработки сигнала вызова элементами

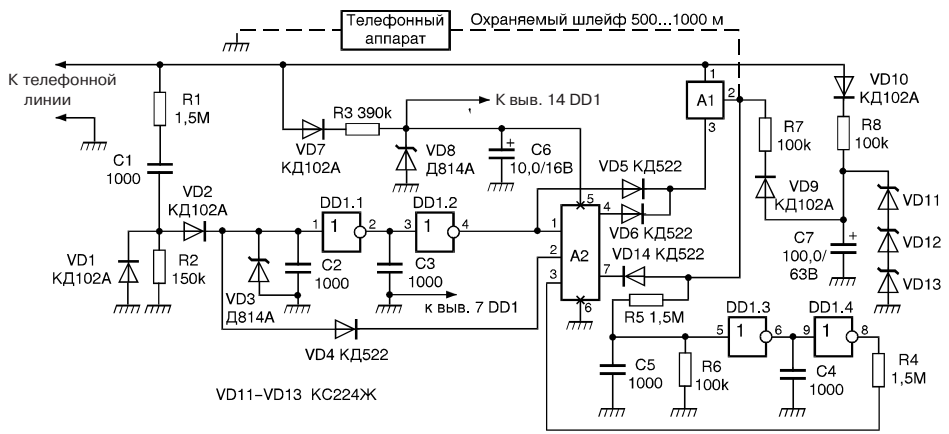


Рис. 3.11. Принципиальная схема устройства защиты телефонной линии

DD1.1, DD1.2 с небольшой задержкой, определяемой номиналами элементов *C2*, *C3*, на выходе *4 DD1.2* появится логическая единица, которая через диод *VD5* открывает ключ *A1* только на время вызова. При снятии трубки с телефонного аппарата входной узел запирается через диод *VD4*, и далее для подключения телефона к линии и ведения разговора необходимо вновь набрать индивидуальный код.

Таким образом, система защиты блокирует подключение к охраняемому участку линии любых телефонных аппаратов без знания кода. Дешифратор может быть выполнен одно-, двух-, трехзначным.

Размер платы — 100×60 мм, подключение к линии осуществляется тремя разъемами. Единственным условием является использование телефонных аппаратов II и III группы сложности (с потреблением от линии не более 50—80 мкА).

Активный индикатор состояния линии

В отличие от выше приведенных устройств 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. Принципиальная схема такого устройства представлена на рис. 3.12.

Устройство собрано на 4 микросхемах и 4 транзисторах. Опишем работу прибора. 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 *a*). 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 высокого напряжения. С движка подстроечного резистора *R2* напряжение высокого уровня поступает на вход элемента *DD1.1* микросхемы К561ЛЕ5, запрещая проход импульсов с генератора, выполненного на элементе *DD2.1* микросхемы К561ТЛ1. Этот генератор собран на основе триггера Шмидта. При заряде и разряде конденсатора *C1* на выходе генератора появляются прямоугольные импульсы. Поскольку заряд конденсатора *C1* 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 *C4*, *R4* и элемент *DD2.2,* устанавливает триг-

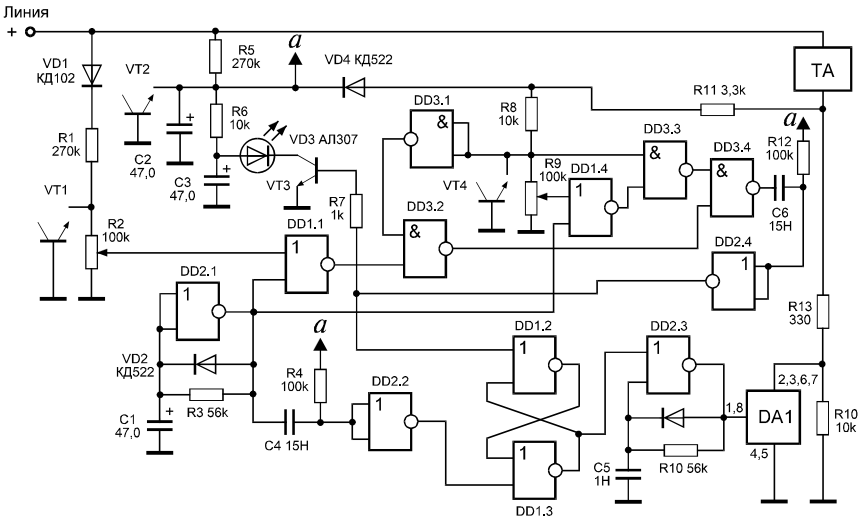


Рис. 3.12. Принципиальная схема активного индикатора состояния линии

гер, 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, так как 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 движке 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 *C6*, *R12* и элементом *DD2.4* поступают на базу транзистора *VT3.* Транзистор открывается, и конденсатор *C3* быстро разряжается через открытый транзистор VT3 и светодиод *VD3*, который ярко вспыхивает с частотой 0,5—1 Гц. В перерывах между импульсами конденсатор *C3* подзаряжается через резистор *R6*. Так как оценка состояния линии про-

исходит под управлением импульсов с генератора *DD2.1*, то некоторое изменение напряжения в линии в момент заряда конденсатора *C3* 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, так как нагрузкой линии будут телефонный аппарат, резистор *R13* и резистор *R14*, зашунтированный малым (около 10 Ом) сопротивлением микросхемы *DA1.* Напряжение, снимаемое с резистора *R13*, обеспечивает питание 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 *C6*, *R12* и элемента *DD2.4* они поступают на базу транзистора *VT3,* включая световую индикацию. Одновременно первый же импульс переводит триггер на *DD1.2* и *DD1.3* 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 данной 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 *C1*, *C2* и *C3* 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,

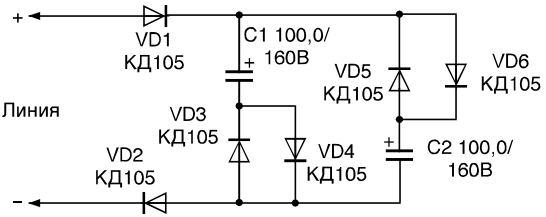


Рис. 3.13. Схема простейшего защитного устройства

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!

Простейшее защитное устройство

В тех случаях, когда вы хотите защититься от несанкционированного подключения к телефонной линии более простым способом, можно воспользоваться схемой, представленной на рис. 3.13.

Это устройство блокирует как набор номера, так и вызывной сигнал. Его удобно выполнить в виде отдельной вилки, подключаемой вместо телефонного аппарата (например, при длительном вашем отсутствии).

Блокировка параллельного телефона

Предлагаемое релейно-конденсаторное устройство позволяет исключить прослушивание телефонного разговора с параллельно включенного телефонного аппарата. Работа его основана на использовании постоянного тока, протекающего через телефонный аппарат при снятой трубке (рис. 3.14).

Контакты *K2.1* и *K1.1* — нормально замкнутые. Конденсаторы *C1* и *C2* обеспечивают прохождение переменной составляющей тока при вызове и во время разговорного соединения. При выборе номиналов конденсаторов важно не допустить, чтобы резонансная частота колебательного контура обмотки реле-конденсатора была равной 25 Гц (частота сигнала вызова) и 450 Гц (частота сигнала зуммера станции).

В качестве реле *K1* и *K2* подойдут любые с током срабатывания 25—30 мА, имеющие нормально замкнутую контактную пару, например РЭС49.

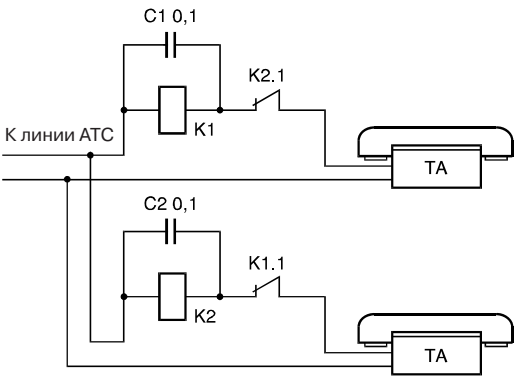


Рис. 3.14. Принципиальная схема релейно-конденсаторного блокиратора

Блокиратор параллельного телефона

Во многих офисах и квартирах телефонные аппараты подключают параллельно к одной линии. Поэтому разговор между двумя абонентами легко может прослушать и третий. Чтобы исключить такую возможность, используют устройство, обычно именуемое блокиратором. Схема блокиратора приведена на рис. 3.15.

Принцип действия данной схемы предельно прост. Допустим, что снята трубка с телефонного аппарата *TA2*. В цепи задействованного аппарата *TA2* 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 (в нашем случае *TA2*) 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.

Аналогичное устройство по принципу действия можно собрать на другой элементной базе по схеме, приведенной на рис. 3.16.

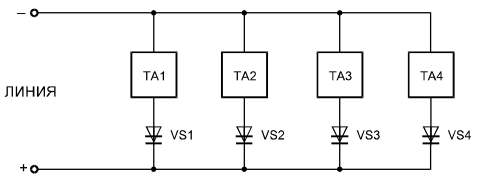


Рис. 3.15. Принципиальная схема блокиратора на динисторах

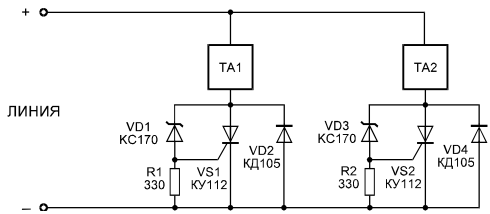


Рис. 3.16. Принципиальная схема блокиратора на аналоге динистора

Устройство содержит два аналога динисторов. Диоды и тиристоры могут быть любыми с допустимым напряжением не менее 100 В и рассчитанными на ток до 0,1 А. Стабилитроны *VD1* и *VD3* могут быть на напряжение стабилизации от 5,6 до 20 В.

Устройства контроля сигналов на телефонной линии

Принцип действия устройств контроля сигналов на телефонной линии основан на частотном анализе сигналов, имеющихся на проводной линии (электросеть, телефонная линия, кабельные линии сигнализации и т. д.). Как правило, приборы этой группы работают в диапазоне частот 40 Гц —10 МГц, имеют высокую

чувствительность (на уровне 20 мкВ), различают модуляцию принимаемого сигнала, имеют возможность контроля принимаемой информации. С помощью данных приборов можно легко установить факт передачи информации по линии связи, ВЧ-навязывание и др. К таким приборам можно отнести Scanner-3, SELSP-31/C, ТСМ-03, ПСЧ-4, РТО-30 и др. Основным недостатком приборов данной группы применительно к телефонной линии является обнаружение узкого класса устройств прослушивания. Поэтому контроль сигналов на телефонной линии часто выполняют более сложные многофункциональные приборы.

Устройства анализа неоднородности телефонной линии

Устройства анализа неоднородности телефонной линии определяют сосредоточенные резистивные или реактивные проводимости, подключенные к линии. Производится это путем измерения параметров сигнала (чаще всего мощности), отраженного от неоднородности линии. Периодически появляющиеся на рынке опытные образцы приборов, реализующие этот принцип (например, БОР-1), позволяют определить расстояние до неоднородности. Это, несомненно, является преимуществом данного способа. Однако небольшая дальность обнаружения (реально до 500 м), низкая достоверность (чаще всего за неоднородность принимаются контактные соединения в линии) полученных результатов измерений делают приборы этой группы эффективными только для регистрации «новых» подключений к линии при небольших измеряемых расстояниях. Высокая цена и сложность реализации данного способа обнаружения, ограниченные функциональные и технические возможности опытных образцов приборов препятствуют их распространению на рынке.

Устройства анализа несимметрии линии

Наиболее распространенным из устройств анализа несимметрии линии является прибор типа ТПУ-5. Принцип действия прибора основан на определении разности сопротивлений проводов линии по переменному току и определении утечки по постоянному току между проводами линии. Измерения проводятся относительно нулевого провода электросети. Прибор не требует «чистой» линии при работе. Чувствительность его довольно высока для обнаружения практически любых закладок, контактно подключенных к линии. Прибор обнаруживает последовательно включенные прослушивающие устройства с внутренним сопротивлением более 100 Ом, параллельные с током потребления более 0,5 мА. Прибор имеет и ряд недостатков. При изначальной несимметрии линии (например, за счет продолжительной и разветвленной проводки внутри здания, наличия скруток, отводов, контактных соединений и т. п.) приборы данной группы ошибочно указывают на наличие последовательно

подключенного прослушивающего устройства. Изменение параметров линии из-за смены климатических условий, неидеальность телефонной линии, утечки за счет устаревшего оборудования АТС и т. д. приводят к ошибочному «определению» параллельно подключенного прослушивающего устройства. И, наконец, использование в качестве «третьего» провода нулевой шины электросети при неисправности в приборе может привести к выходу из строя оборудования АТС, телефонной линии.

Устройства анализа нелинейности параметров линии

В последние несколько лет на отечественном рынке спецтехники появились устройства анализа нелинейности параметров линии, принцип действия которых основан на анализе нелинейности импеданса телефонной линии. В свою очередь, в этой группе приборов существуют две подгруппы. Это приборы:

- определяющие нелинейность двухпроводной обесточенной линии;
- работающие на реальной телефонной линии.

Приборы, определяющие нелинейность двухпроводной обесточенной линии (АТ-2, «Визир» и др.), обладают высокой чувствительностью и позволяют определять практически любые нелинейные устройства съема информации, подключенные к линии. Существенным недостатком таких приборов применительно к телефонной линии является небольшая дальность обнаружения, ограниченная физической доступностью к проводам линии и необходимостью отключения телефонной линии от АТС на время проверки. Эти особенности эксплуатации не позволяют производить оперативный контроль телефонной линии и ограничивают дальность проверки. Приборы наиболее пригодны для периодических проверок обесточенных отрезков линий (телефонных, электросети, сигнализации) внутри здания. Приборы, работающие на реальной телефонной линии (SELSP-18/T, КТЛ-400), обладают меньшей чувствительностью по сравнению с приборами предыдущей подгруппы. Происходит это из-за того, что помехи, специальные сигналы АТС, наводки промышленной частоты, присутствующие на линии, реально не позволяют получить такую же чувствительность. Однако их чувствительность вполне достаточна для обнаружения практически всех известных прослушивающих устройств с питанием от телефонной линии, имеющих нелинейный характер импеданса. С другой стороны, возможность работы на реальной телефонной линии, оперативность проведения контроля (не более 5 мин) без нарушения нормального функционирования линии, максимально возможная дальность обнаружения прослушивающих устройств (непосредственно от телефонного аппарата до АТС), необязательность «чистой» линии на момент подключения прибора, отсутствие зависимости результатов проверки линии от реактивных неоднородностей, некачественных контактов (скруток), утечек тока делают приборы второй подгруппы наиболее привлекательными при

эксплуатации. К несомненным достоинствам приборов следует отнести их многофункциональность. Анализатор SELSP-18/T выполнен как поисковый прибор с автономным питанием и в качестве дополнительных функций определяет ВЧ-навязывание и наличие аудиосигналов на линии. В отличие от SELSP-18/T контроллеры КТЛ-3, КТЛ-400 кроме функции поиска выполняют функцию защиты переговоров по линии от утечки информации. Например, КТЛ-400 полностью автоматизирован, имеет цифровой генератор шума с автоматически перестраиваемым спектром. Прибор оказывает эффективное противодействие параллельным телефонным аппаратам, телефонным закладкам с питанием от линии или внешним питанием, диктофонам, подключенным к линии через контактные или индуктивные съемники, микрофонам и радиомикрофонам с питанием от линии. Кроме этого, прибор защищает телефоны от аппаратуры ВЧ-навязывания, обнаруживает и отключает аппаратуру типа «телефонное ухо». В КТЛ-400 также реализован новый эффективный способ защиты — компенсация постоянного напряжения линии при разговоре, что позволяет полностью отключить параллельные прослушивающие устройства с питанием от линии. Прибор может эксплуатироваться как на городских, так и на местных линиях (с мини-АТС). И, наконец, прибор можно использовать для проверки любых двухпроводных обесточенных линий (электросеть, сигнализация и т. д.).

Таким образом, можно сказать, что на сегодняшний день, несмотря на развитие рынка спецтехники для проверки телефонной линии, не существует универсальной аппаратуры, позволяющей определить подключение к телефонной линии. Более того, индуктивные и емкостные съемники без радиоканала не определяются ни одним прибором из перечисленных групп. Следует учитывать, что наибольшее распространение (до 95 %) получили контактно подключенные устройства прослушивания переговоров с радиоканалом и питанием от линии и устройства типа «телефонное ухо». Распространено прослушивание с помощью параллельных телефонных аппаратов, АОНов и автоответчиков. Значительно более организационно сложным, дорогостоящим и менее вероятным следует считать бесконтактное подключение к линии устройств без радиоканала, контактное подключение устройств с высоким входным сопротивлением и внешним питанием без радиоканала, использование аппаратуры ВЧ-навязывания. Что касается выбора из всех выше перечисленных приборов для проверки телефонной линии, то в каждом конкретном случае пользователь должен исходить из того, какие типы устройств наиболее вероятно могут быть подключены к линии. Следует учитывать место, где они могут быть установлены, и ориентировочную продолжительность их работы. С нашей точки зрения, наиболее эффективными в настоящее время являются приборы радиоконтроля и приборы, анализирующие нелинейность линии. Это вызвано тем, что основная масса прослушивающих устройств работает с питанием от телефонной линии (т. е. содержит нелинейный импеданс) и передает информацию по эфиру, используя радиоканал. Причем для оперативной проверки лучше использовать приборы, анализирующие нелинейность импеданса линии. При оценке приборов необходимо учитывать их дополнительные функции. С этой точки зрения наиболее предпочти-

тельными являются приборы, обеспечивающие как функции поиска, так и функции защиты переговоров по телефону. В этом смысле наиболее выигрышным по критерии «поиск — защита» является контроллер телефонной линии КТЛ-400, обладающий мощными защитными функциями. Прибор позволяет эффективно подавлять практически любые прослушивающие устройства, включая индуктивные и емкостные съемники, параллельные телефоны, «телефонное ухо», ВЧ-навязывание и т. д. на всей протяженности телефонной линии

Многофункциональные устройства защиты телефонных линий

В настоящее время российский рынок изделий специальной техники представлен широким выбором приборов, позволяющих с той или иной степенью достоверности обнаруживать наличие прослушивающих устройств, установленных на телефонной линии. Кратко рассмотрим некоторые из них.

Многофункциональный поисковый прибор ST031 «Пиранья»

Многофункциональный поисковый прибор ST031 «Пиранья» (рис. 3.17) предназначен для проведения оперативных мероприятий по обнаружению и локализации технических средств негласного получения информации, а также для выявления и контроля естественных и искусственно созданных каналов утечки информации.

Прибор состоит из основного блока управления и индикации, комплекта преобразователей и позволяет работать в следующих режимах:

Рис. 3.17. Многофункциональный поисковый прибор ST031 «Пиранья»

- высокочастотный детектор-частотомер;
- сканирующий анализатор проводных линий;
- детектор ИК-излучений;
- детектор низкочастотных магнитных полей;
- виброакустический приемник;
- акустический приемник.

Переход прибора ST031 в любой из режимов осуществляется автоматически при подключении соответствующего преобразователя. Информация отображается на графическом ЖКИ-дисплее, акустический контроль осуществляется через головные телефоны либо через встроенный

громкоговоритель. Управление прибором производится с помощью 16-кнопочной клавиатуры. Аппаратура ST031 позволяет обрабатывать поступающие НЧ-сигналы в режиме осциллографа либо спектроанализатора с индикацией численных параметров.

Основные технические характеристики

Полоса пропускания, кГц	22
Чувствительность по входу, мВ	10
Погрешность измерений (от верхнего предела), %	1
Скорость вывода осциллограммы, с	0,2
Скорость вывода спектрограммы, с	0,3
Разрешение графического дисплея, точек	128×64
Возможность сохранения и вызова из энергонезависимой памяти отображений	15—60

Устройство защиты телефонных линий «Барьер-3»

Система безопасности телефонной линии «Барьер-3» разработана специально для того, чтобы исключить любую возможность подслушивания телефонных переговоров. Это полностью автоматизированное устройство (рис. 3.18) подавляет любые телефонные подслушивающие и звукозаписывающие устройства. Представляя минимальную сложность в использовании, «Барьер-3» просто включается между телефонным аппаратом и линией (телефонной розеткой) и автоматически обеспечивает максимальную защиту от подслушивающих и записывающих устройств любого типа. Кроме того, с помощью специальной системы индикации потребителю станет известно о попытках подключить что-либо к его телефонной линии. Система обеспечивает защиту переговоров от телефонного аппарата до АТС, т. е. там, где обычно устанавливаются устройства для подслушивания переговоров.

Функциональные возможности устройства защиты телефонных линий «Барьер-3»:

- подавление подслушивающих устройств (телефонных радиозакладок), несанкционированно подключенных к телефонной линии, вне зависимости от их типов и способов подключения (в том числе с индуктивным съемом);
- подавление автоматических звукозаписывающих устройств, подключенных к телефонной линии и активизируемых поднятием телефонной трубки;

Рис. 3.18. Устройство защиты телефонных линий «Барьер-3»

- подавление звукозаписывающих устройств с ручным управлением записи;
- запуск диктофонов, активируемых голосом, при положенной телефонной трубке;
- защита телефонного аппарата (в режиме «опущенной трубки») от съема информации методами ВЧ-навязывания, микрофонного эффекта;
- блокирование работы микрофонов, работающих по телефонной линии;
- блокирование работы подключенного к телефонной линии параллельного телефона или трубки;
- цифровая индикация напряжения линии и напряжения отсечки при поднятой и положенной трубке, что позволяет обнаружить любое подключение к линии;
- возможность подключения к линии звукозаписывающей аппаратуры (диктофоны) для архивации телефонных переговоров;
- аудиовизуальная индикация несанкционированного подключения устройств съема информации, изменяющих параметры телефонной линии.

Основные технические характеристики

Защищаемый участок ..... от ТА до АТС
Уровень маскирующего шума, В ..... до 40
Напряжение отсечки, В ..... до 50
Напряжение питания, В 220
Габариты, мм ..... 220×110×50
Потребляемая мощность, Вт ..... не более 5

Устройство защиты телефонных переговоров от прослушивания и записи СТО-24 «Вьюга»

Устройство защиты телефонных переговоров от прослушивания и записи СТО-24 «Вьюга» (рис. 3.19) предназначено для исключения прослушивания телефонных переговоров при помощи специализированных электронных средств.

Устройство позволяет:

- подавить последовательные прослушивающие устройства;
- снизить эффективность применения параллельных прослушивающих устройств за счет снижения отношения сигнал/шум не менее чем в 3 раза в прослушивающих устройствах со стабилизацией частоты и смещения рабочей частоты в устройствах без стабилизации несущей на 2—4 МГц;
- включать прослушивающие устройства, управляемые по сигналу звукового диапазона, на передачу и запись шума вместо информации за счет создания активной шумоподобной помехи в полосе частот 10—25 кГц при снятой телефонной трубке и в полосе 40—1000 Гц при положенной трубке;

Рис. 3.19. Устройство защиты телефонных переговоров СТО-24 «Вьюга»

- устанавливать пассивное заграждение приему сигналов речевого диапазона с телефонной линии при помощи индукционных датчиков путем уменьшения отношения сигнал/шум не менее чем в 3 раза;
- устанавливать пассивное заграждение распространению в линии ВЧ-сигналов несущих частот от закладок;
- контролировать состояние телефонной линии:
  напряжение номинальное в режиме ожидания вызова (60 В) с точностью не хуже ±0,2 В, что позволит обнаруживать параллельно подключенные радиозакладки с сопротивлением до 300 кОм;
  напряжение срабатывания формирователя сигнала «Ответ станции» (длинный гудок) при снятии трубки (40 В) в автоматическом режиме;
  ток в линии при ее замыкании в режиме набора номера (35 мА), что позволит обнаруживать последовательные радиозакладки с сопротивлением от 100 Ом и выше.

На передней панели прибора расположены индикатор и ручка управления. Прибор имеет четыре режима работы. В первом режиме прибор выключен и не влияет на телефонную линию. Во втором режиме обеспечивается возможность защиты переговоров при помощи активных и пассивных помех. Третий и четвертый режимы являются измерительными.

В третьем режиме при снятой трубке прибор автоматически моделирует процесс «постепенного снятия» телефонной трубки и показывает текущее значение напряжения телефонной линии. В этом режиме определяется значение напряжения срабатывания сигнала «Ответ АТС» (длинный гудок).

В четвертом режиме прибор измеряет ток в линии при наборе номера. Этот режим используется для обнаружения последовательных радиозакладок.

Универсальное устройство защиты телефонных линий KZOT-06

Универсальное устройство защиты телефонных линий KZOT-06 — представитель семейства так называемых «телефонных подавителей», использующих принцип: «Лучшая оборона — это нападение». Телефонный подавитель KZOT-06 (рис. 3.20) осуществляет зашумление верхнего звукового диапазона, ухудшая тем самым соотношение сигнал/шум на входе устройств съема информации. В реальности подавитель шумит в линию так, что говорить порой просто невозможно.

Они также устанавливаются на «чистую» линию, работают в двух режимах — обнаружение и подавление. При любом контактном подключении к линии

Рис. 3.20. Телефонный подавитель KZOT-06

прибор подаст сигнал тревоги, после чего можно включить режим подавления. Помеха, подаваемая в линию, действует на участке от прибора до АТС, выводя все средства съема из рабочего состояния. Данный класс устройств защиты является наиболее приемлемым для обеспечения безопасности телефонных переговоров. Главный минус таких приборов — неспособность защитить разговор абонента от СОРМ — системы оперативно-розыскных мероприятий, проводимая субъектами ОРД: ФСБ, СВР, МВД.

Скремблеры

От СОРМ частично могут спасти такие устройства защиты телефонных переговоров, как скремблеры. Телефонные скремблеры — это устройства шифрации-дешифрации речевых переговоров. Так как любой код и шифр можно вскрыть и в конце концов добраться до необходимой информации, то скремблеры только снижают оперативную ценность расшифрованного разговора. К примеру, вы накануне обсуждали по телефону важную встречу, используя скремблирующее устройство. Ваш разговор был перехвачен, но результаты дешифрации конкуренты получили на следующий день после встречи. Таким образом, для них потеряна оперативная ценность информации, за которую они так боролись.

Сам скремблер (рис. 3.21) представляет собой коробочку (черную, серую, белую), размещаемую рядом с телефонным аппаратом. Такая же коробочка должна быть у всех абонентов, разговоры с которыми необходимо засекретить. Порядок действий со скремблером такой: вы дозваниваетесь до абонента, оба включаете свои скремблеры, ждете, пока они настроятся друг на друга, и после этого начинаете разговаривать.

Работа таких систем делится на несколько этапов. На первом этапе речевое сообщение абонента обрабатывается по какому-либо алгоритму (кодируется) так, чтобы злоумышленник, перехвативший обработанный сигнал, не смог разобрать смысловое содержание исходного сообщения. Затем обработанный сигнал направляется в канал связи (телефонную линию). На последнем этапе сигнал, полученный другим абонентом, преобразуется по обратному алгоритму (декодируется) в речевой сигнал. Для того чтобы раскрыть смысловое содержание защищенного криптографическим способом телефонного разговора, злоумышленнику потребуются:

- наличие криптоаналитика;
- дорогостоящее оборудование;
- время для проведения криптоанализа.

Последний фактор, как уже говорилось, может свести на нет все усилия, поскольку к моменту раскрытия сообщения высока вероятность того, что оно уже устарело. Кроме того, момент раскрытия может вообще не наступить.

Принято считать, что скремблеры обеспечивают наивысшую степень защиты телефонных переговоров. Это действительно так, но только в том случае, если алгоритм кодирования/декодирования имеет достаточную криптостойкость. Аналоговые алгоритмы кодирования, которые используются в недорогих скремблерах, более просты и поэтому менее стойки, чем у систем с цифровой дискретизацией речи и последующим шифрованием (вокодеров). Но стоимость последних выше, как минимум, в 3 раза. К достоинствам криптографических систем следует отнести то, что защита происходит на всем протяжении линии связи. Кроме того, безразлично, какой аппаратурой перехвата пользуется злоумышленник. Все равно он не сможет в реальном масштабе времени декодировать полученную информацию, пока не раскроет ключевую систему защиты и не создаст автоматический комплекс по перехвату. К недостаткам криптографической защиты телефонных переговоров относятся:

- необходимость установки совместимого оборудования у всех абонентов, участвующих в закрытых сеансах связи. В последнее время появились «одноплечевые» скремблеры, которые, решая в некоторой степени указанный недостаток, порождают ряд других. Вместо установки второго скремблера у противоположного абонента он устанавливается на городской АТС. Теперь сообщение расшифровывается на середине пути, и появляется возможность перехвата информации с телефонной линии противоположного абонента. При этом вы становитесь заложником финансовых аппетитов и неповоротливости служащих телефонной компании в случае выхода защитного оборудования из строя, а также несете тактические потери от того, что появляется третье лицо, знающее о том, что вы пользуетесь защитой телефонных переговоров;
- потеря времени, необходимого для синхронизации аппаратуры и обмена ключами в начале сеанса защищенного соединения;
- невозможность противостоять перехвату речевой информации из помещений в промежутках между переговорами.

В настоящее время на рынке спецтехники появились приборы, называемые односторонними маскираторами (скремблерами) речи. Принцип их действия основан на том, что при приеме важного речевого сообщения от удаленного абонента владелец маскиратора сам включает режим защиты.

Рис. 3.21. Внешний вид скремблера

При этом в телефонную линию подается интенсивный маскирующий шумовой сигнал в полосе частот, пропускаемых телефонным каналом, который распространяется по всей протяженности канала связи. Поскольку характеристика шумового сигнала известна, то в маскираторе происходит автоматическая компенсация помехи в поступившей на вход смеси полезного речевого и шумового сигналов с помощью адаптивного фильтра.

Для того чтобы противодействовать одностороннему маскиратору, злоумышленник может попытаться:

- записать смесь полезного и шумового сигнала;
- проанализировать характер шумового сигнала и определить расположение пауз в речевом сообщении;
- определить характеристики шумового сигнала в паузах речевого сообщения;
- воспользоваться адаптивным фильтром для очистки речевого сигнала от помехи по полученным характеристикам шумового сигнала.

Как видно из вышесказанного, задача эта трудоемкая и требует значительных материальных затрат и времени. Маскиратор использует для компенсации шума адаптивный фильтр, имеющий некоторое время адаптации. Чем больше время адаптации, тем лучше компенсация помехи. Отсюда следует, что для уменьшения времени адаптации при маскировке следует использовать более однородный шумовой сигнал, характеристики которого легче вычислить злоумышленнику. Если для маскировки использовать шумовой сигнал, характеристики которого будут динамически изменяться, то соответственно снизится уровень компенсации помехи в трубке владельца маскиратора (будет хуже слышно), но при этом задача злоумышленника серьезно осложнится.

Положительные стороны применения односторонних маскираторов:

- достаточно высокая степень защиты входящих сообщений;
- возможность работы с мобильным абонентом.

Недостатки односторонних маскираторов:

- невозможность закрытия исходящих сообщений. Для преодоления этого ограничения потребуется установить маскираторы обоим абонентам, причем вести разговор в дуплексе им не удастся, поскольку каждому абоненту по очереди придется вручную включать режим маскировки и это вряд ли целесообразно, так как проще, дешевле и надежнее воспользоваться комплектом скремблеров;
- наличие высокого уровня шума в трубке абонента, передающего сообщение. Услышав шум в трубке, «нетренированный» абонент может начать передавать сообщение громким голосом, при этом соотношение амплитуд помехи и полезного сигнала на его плече телефонной линии снизится, что облегчит конкуренту задачу по очистке сообщения от помехи.

Использование радиоретрансляторов

Радиоретранслятор — это радиопередающее устройство, передающее (ретранслирующее) без искажений звуковой сигнал, снимаемый с телефонной линии. Радиоретрансляторы, так же как и радиомикрофоны, работают в различных частотных диапазонах. Для прослушивания телефонных переговоров используются следующие способы (рис. 3.22) подключения радиоретрансляторов:

- параллельное подключение к телефонной линии. В этом случае телефонные радиоретрансляторы труднее обнаруживаются, но требуют внешнего источника питания;
- последовательное включение телефонных радиоретрансляторов в разрыв провода телефонной линии. В этом случае питание телефонного радиоретранслятора осуществляется от телефонной линии и в эфир он выходит (т. е. начинает передачу) с момента подъема телефонной трубки абонентом;
- индуктивное подключение к линии подразумевает использование отдельного источника питания.

Подключение телефонного радиоретранслятора может осуществляться как непосредственно к телефонному аппарату, так и на любом участке линии от телефона абонента до АТС. В настоящее время существуют телефонные радиоретрансляторы, позволяющие прослушивать помещение через микрофон лежащей трубки.

Существуют системы прослушивания телефонных разговоров, не требующие непосредственного электронного соединения с телефонной линией. Эти системы используют индуктивный способ (при помощи катушек) съема информации. Они достаточно громоздки, поскольку содержат несколько каскадов усиления слабого НЧ-сигнала и обязательный внешний источник питания. Поэтому такие системы не нашли широкого практического применения.

Для приема информации от телефонных радиоретрансляторов используются такие же приемники, как в акустических устройствах съема информации по радиоканалу.

В настоящее время появились системы перехвата факсовой и модемной связи, которые при использовании персонального компьютера со специальным программным обеспечением позволяют получить расшифровку информации. Однако такие системы очень дорогие и пока не нашли широкого применения в нашей стране.

Телефонный радиоретранслятор с АМ в диапазоне частот 27—28 МГц

Устройство представляет собой телефонный радиоретранслятор. Последний позволяет прослушивать телефонный разговор на радиоприемник диапазона 27—28 МГц с амплитудной модуляцией.

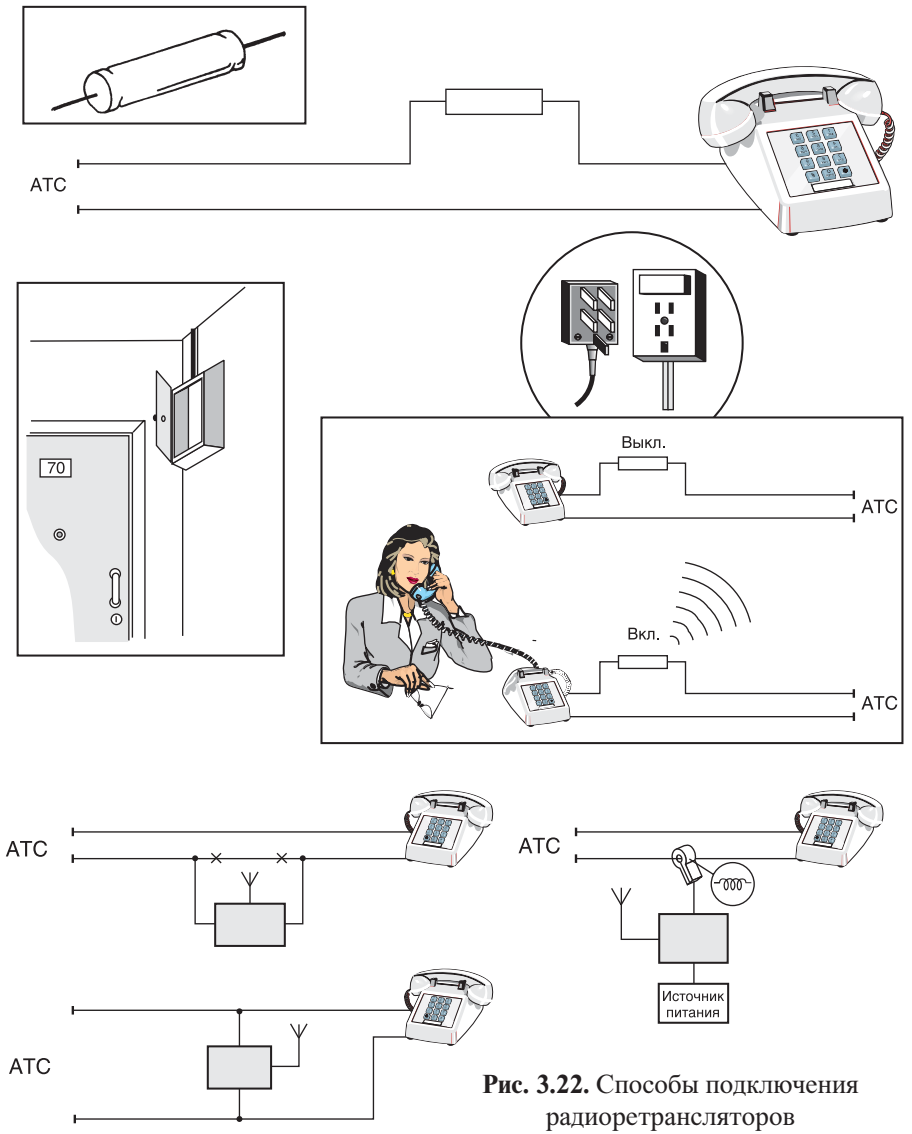


Рис. 3.22. Способы подключения радиоретрансляторов

Принципиальная схема этого устройства изображена на рис. 3.23.

Устройство представляет собой маломощный однокаскадный передатчик с АМ и кварцевой стабилизацией несущей частоты.

Задающий генератор выполнен по традиционной схеме на транзисторе *VT1* типа КТ315. Режим транзистора по постоянному току задается резисторами *R2* и *R3*. Кварцевый резонатор *ZQ1* включен между коллектором и базой транзистора *VT1*. Он может быть любым на одну из частот диапазона 27—28 МГц.

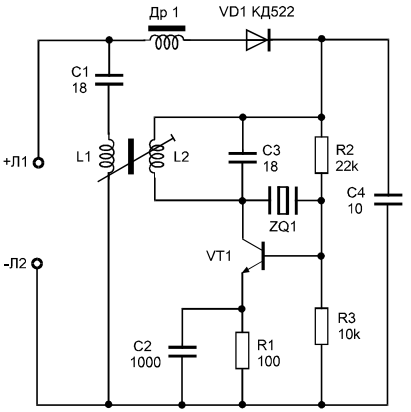


Рис. 3.23. Принципиальная схема телефонного радиоретранслятора с АМ в диапазоне частот 27—28 МГц

Контур, состоящий из катушки *L2* и конденсатора *C3*, настроен на частоту кварцевого резонатора. С катушки связи *L1* сигнал поступает в антенну, в качестве которой используются телефонные провода.

Дроссель *Др1* служит для разделения ВЧ- и НЧ-сигналов. Диод *VD1* предохраняет устройство от выхода из строя в случае неправильного подключения. Схема подключения устройства представлена на рис. 3.24.

Передатчик подключается параллельно телефонной трубке. Когда трубка положена на рычаг, разговорный узел отключен от линии. Подключена к линии в этот момент только цепь вызывного устройства. Таким образом, до тех пор пока трубка не снята, напряжение питания на передатчик не поступает. Как только трубку снимают, к линии подключается разговорная часть. Во время разговора ток через разговорную часть меняется синхронно с речью, соответственно изменяется и напряжение в точках *+Л1* и *–Л1*. Изменение напряжения питания приводит к соответствующему изменению амплитуды генерируемых ВЧ-колебаний, т. е. имеет место АМ. В результате разговор можно слушать на расстоянии до 50 м на приемник диапазона 27—28 МГц, работающий на прием АМ-сигнала.

Транзистор *VT1* может быть типов КТ316, КТ3102, КТ368. Диод *VD1* — КД521, КД510, Д220. Дроссель *Др1* намотан на ферритовом стержне марки 600НН диаметром 2,8 мм и длиной 14 мм, он содержит 150—200 витков провода ПЭВ 0,1.

Катушки *L1* и *L2* намотаны на полистироловом каркасе от КВ-приемников диаметром 8 мм с подстроечным сердечником. Катушка *L2* содержит 12 витков провода ПЭВ 0,31. Катушка связи *L1* наматывается поверх катушки *L2* и содержит 3 витка того же провода.

Настройка устройства осуществляется путем настройки контура *L2*, *C3* на несущую частоту. При подключении следует учитывать полярность напряжения линии.

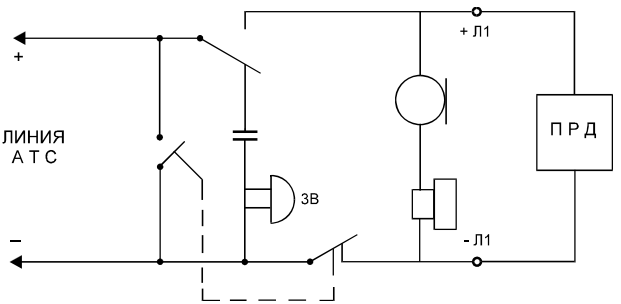


Рис. 3.24. Схема подключения телефонного радиоретранслятора

Телефонный ретранслятор У-диапазона с ЧМ

Данное устройство имеет сходство с предыдущим по способу подсоединения к телефонной линии. Оно представляет собой маломощный передатчик, работающий в диапазоне УКВ с использованием частотной модуляции. Дальность действия передатчика — около 100 м.

Принципиальная схема устройства представлена на рис. 3.25. Особенность схемы состоит в том, что передатчик, собранный на транзисторе *VT1* типа КТ315, питается от телефонной линии, используя ее в качестве антенны, а ЧМ осуществляется путем изменения емкостей переходов этого транзистора при изменении питающего напряжения.

Задающий генератор выполнен на транзисторе *VT1* по схеме с общей базой. Напряжение обратной связи поступает на его эмиттер с делителя, состоящего из конденсаторов *C2* и *C3*. Частоту задающего генератора определяют конденсаторы *C2*, *C3*, катушка *L1* и межэлектродные емкости транзистора *VT1*. С коллектора транзистора *VT1* сигнал через конденсатор *C1* поступает в линию, провод которой используется в качестве антенны. Дроссель *Др1* служит для разделения ВЧ- и НЧ-составляющих сигналов.

Подключение данного устройства к линии аналогично подключению устройства, описанного выше (см. рис. 3.24).

Катушка *L1* бескаркасная, диаметром 4 мм, содержит 6—7 витков провода ПЭВ 0,3. Дроссель *Др1* — индуктивностью не менее 30 мкГн типа ДПМ 0,1.

Настройка передатчика заключается в подборе сопротивления резисторов *R2* или *R3* для получения максимального излучения. Контур передатчика настраивают растяжением или сжатием витков катушки *L1* на свободный участок УКВ ЧМ-диапазона.

Телефонный ретранслятор с питанием от телефонной линии

Устройство, схема которого представлена ниже, представляет собой УКВ ЧМ-передатчик в радиовещательном диапазоне частот. Питается оно от телефонной линии и имеет выходную мощность около 20 мВт. Основное отличие этого устройства от описанных выше заключается в способе подсоединения к телефонной линии. В данном случае устройство подключается в разрыв одного из проводов линии в любом месте по всей длине кабеля.

Принципиальная схема радиоретранслятора представлена на рис. 3.26. Резистор *R1* включается

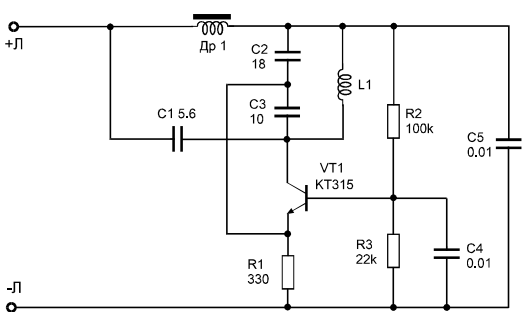


Рис. 3.25. Принципиальная схема телефонного ретранслятора УКВ-диапазона с ЧМ

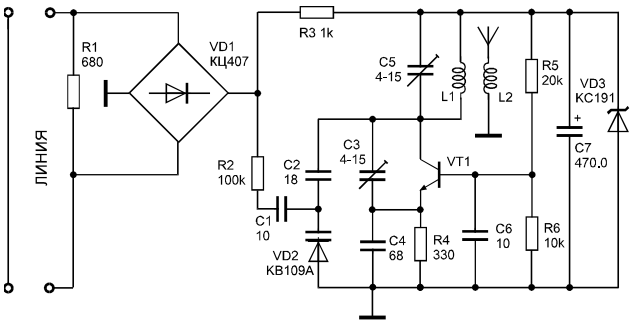


Рис. 3.26. Принципиальная схема телефонного ретранслятора с питанием от телефонной линии

в разрыв одного из проводов телефонной сети. При снятии трубки телефонного аппарата в цепи появляется ток, который, в зависимости от типа аппарата и состояния линии, находится в пределах 10—35 мА. Этот ток, протекая через резистор *R1*, вызывает на нем падение напряжения порядка 4—25 В. Напряжение поступает на выпрямительную диодную сборку типа КЦ407, благодаря которой устройство может подключаться в линию без соблюдения полярности. Высокочастотная часть схемы запитывается от параметрического стабилизатора, собранного на резисторе *R3*, стабилитроне *VD3* типа КС191 и конденсаторе *C7*. Стабилизатор ограничивает излишек напряжения, поступающего с диодной сборки *VD1*.

Задающий генератор выполнен на транзисторе *VT1* типа КТ315. Работа такого генератора подробно была описана при рассмотрении схемных решений радиомикрофонов. Частотная модуляция осуществляется путем изменения емкости варикапа *VD2* типа КВ109А. Модулирующее напряжение поступает из линии через последовательно включенные резистор *R2* и конденсатор *C1*. Первый ограничивает уровень НЧ-сигнала, второй — исключает проникновение постоянного напряжения линии в цепь модулятора. Частотно-модулированный сигнал с катушки связи *L2* поступает в антенну, в качестве нее используется отрезок монтажного провода длиной, равной четверти длины волны, на которой работает передатчик.

Транзистор *VT1* можно заменить на КТ3102, КТ368. Диодную сборку *VD1* можно заменить на четыре диода КД102 или КД103. Стабилитрон *VD3* можно использовать любой с напряжением стабилизации 6,8—10 В. Конденсатор *C7* должен быть рассчитан на рабочее напряжение, большее напряжения стабилизации *VD3*. Катушка *L1* намотана на корпусе подстроечного конденсатора *C5* и содержит 7 витков провода ПЭВ 0,31. Катушка *L2* намотана поверх катушки *L1* тем же проводом — 2 витка.

При настройке конденсаторы *C3* и *C5* подстраивают так, чтобы в нужном диапазоне (65—108 МГц) передавался сигнал максимально возможной мощности. Дальность действия собранного радиоретранслятора в зависимости от условий приема составляет 30—150 м.

Телефонный радиоретранслятор с ЧМ на одном транзисторе

Принципиальная схема передатчика на рис. 3.27 имеет много общего со схемой, представленной на рис. 3.26. Основное отличие состоит в том, что ЧМ осуществляется не варикапом, а путем изменения параметров транзистора в зависимости от протекающего тока. Радиоретранслятор работает в диапазоне частот 65—108 МГц и обеспечивает дальность передачи до 200 м.

Задающий генератор выполнен на транзисторе *VT1* типа КТ315. Частота генератора определяется параметрами колебательного контура — индуктивностью катушки *L1* и емкостью конденсатора *C3*. Конденсатор *C4* обеспечивает оптимальные условия возбуждения генератора. Дроссели *Др1* и *Др2* разделяют ВЧ- и НЧ-составляющие сигнала. С коллектора транзистора *VT1* сигнал через конденсатор *C2* поступает в антенну. В качестве антенны используется отрезок монтажного провода.

В качестве антенны можно использовать и саму линию связи (рис. 3.28). Для этого ВЧ-сигнал с коллектора транзистора *VT1* через конденсаторы *C7* и *C8* поступает в точки *A* и *B* схемы соответственно. Конденсатор *C2* при этом из схемы исключается. Вместо *VD1* можно использовать четыре диода типов КД102, КД510, КД522 и др.

Транзистор КТ315 можно заменить на КТ3102, КТ368 и другие высокочастотные. Катушка *L1* намотана на корпусе конденсатора *C3* и содержит 4 витка провода ПЭВ 0,5. Дроссели — любые с индуктивностью 50—100 мкГн. Настройка аналогична настройке схемы на рис. 3.26.

Телефонный радиоретранслятор большой мощности с ЧМ

Передатчик, собранный по схеме, приведенной на рис. 3.29, обеспечивает большую дальность действия — до 300 м. Работает он в диапазоне 65—108 МГц с частотной модуляцией.

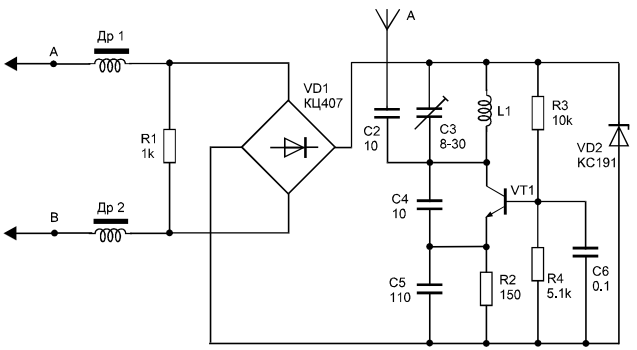


Рис. 3.27. Принципиальная схема телефонного радиоретранслятора с ЧМ на одном транзисторе

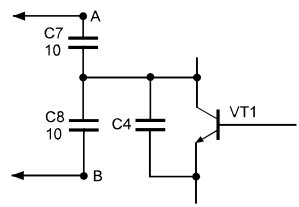


Рис. 3.28. Использование линии связи в качестве антенны

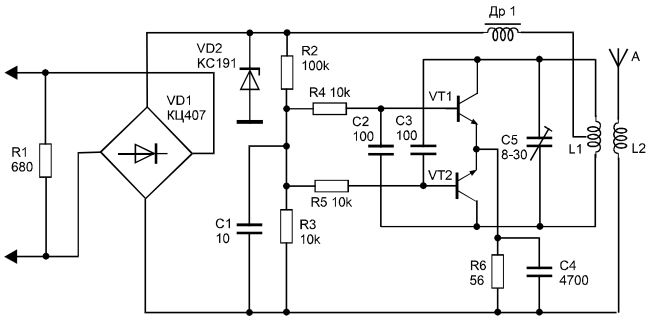


Рис. 3.29. Принципиальная схема телефонного радиоретранслятора большой мощности с ЧМ

Автогенератор собран по обычной двухтактной схеме на транзисторах *VT1* и *VT2* типа КТ315. Частотная модуляция происходит за счет изменения напряжения в линии и, как следствие, изменения напряжения на базах транзисторов *VT1* и *VT2*. Частота задается параметрами контура *L1*, *C5*. При изменении емкости конденсатора *C5* в пределах от 8 до 30 пФ диапазон возможного изменения частоты генератора находится от 65 до 108 МГц при постоянной индуктивности катушки *L1*. Дроссель *Др1* — любой индуктивности в диапазоне от 50 до 100 мкГн. Катушка *L1* наматывается на корпусе подстроечного конденсатора *C5* и содержит 4 витка провода ПЭВ 0,5 с отводом от середины. Катушка *L2* намотана поверх *L1* и имеет 2 витка того же провода. В качестве транзисторов *VT1*, *VT2* можно использовать любые ВЧ-транзисторы. Стабилитрон *VD2* — на напряжение 6—12 В. От него зависит мощность и диапазон девиации частоты передатчика.

Настройка производится при занятой телефонной линии путем подстройки контура *L1*, *C5*.

Радиомикрофон-радиоретранслятор с питанием от телефонной линии

Существуют радиоретрансляторы, которые позволяют прослушивать не только телефонный разговор при снятой трубке, но и разговор в помещении, где они установлены, при положенной трубке. Эти устройства маломощные, так как используют питание от линии и не могут потреблять ток более 1 мА.

Принципиальная схема такого устройства представлена на рис. 3.30.

Выпрямительный мост *VD1* типа КЦ407 подключается параллельно телефонной линии независимо от полярности напряжения в линии. Напряжение в линии при положенной трубке имеет значение около 60 В. Это напряжение прикладывается к блоку питания, который выполнен на микросхеме *DA1*, резисторе *R1*, конденсаторе *C1* и транзисторах *VT1* и *VT2*. Микросхема *DA1* типа КЖ101 представляет собой стабилизатор тока, работающий при напряжениях 1,8—120 В. Падение напряжения при протекании стабильного тока через нагрузку во время заряда конденсатора *C1* ограничено аналогом низковольтного стабилитрона, собранного на транзисторах *VT1* и *VT2*. При положенной трубке

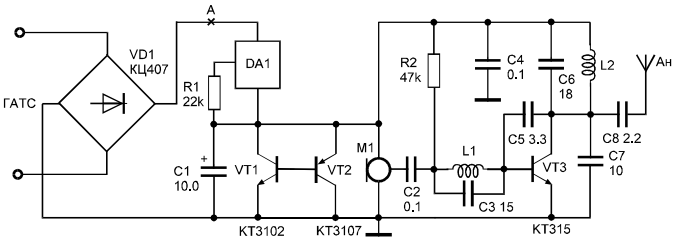


Рис. 3.30. Принципиальная схема радиомикрофона-радиоретранслятора с питанием от телефонной линии

устройство работает как обычный радиомикрофон. Описание схемы радиомикрофона и его настройка подробно приведены в разделе, посвященном радиомикрофонам. При снятой трубке незначительное изменение тока, протекающего через нагрузку — радиомикрофон, вызывает изменение рабочей точки транзистора *VT3* и тем самым осуществляет частотную модуляцию радиомикрофона.

Транзисторы *VT1* и *VT2* можно заменить на КТ315 и КТ361 соответственно. Конденсатор *C1* — с минимальным током утечки. Настройка источника питания сводится к установке резистором *R1* тока, протекающего через нагрузку. Ток в точке *A* не должен превышать 1,5 мА.

3.2. Контроль мобильных средств связи

Электронные средства коммуникации (телефакс, телеграф и служебные и личные радиостанции, сотовые телефоны, пейджеры) на сегодняшний день имеют повсеместное распространение и дают возможность получить потрясающий объем деловой и интимной информации, относящейся к исследуемому объекту. Так уж устроен мир, что любое техническое изобретение человеческого разума, расширяющее наши возможности и создающее для нас дополнительный комфорт, неизбежно содержит в себе и отрицательные стороны, которые могут представлять потенциальную опасность для пользователя. Не являются исключением в этом плане и современные средства беспроводной персональной связи. Да, они несоизмеримо расширили нашу свободу, освободив нас от телефонного аппарата на рабочем столе и дав нам возможность в любое время и в любом месте связаться с необходимым корреспондентом. Но немногие знают, что эти чудеса техники скрывают в себе весьма опасные ловушки. И для того чтобы однажды ваш помощник — сотовый телефон не превратился в вашего врага, об этих ловушках необходимо все знать.

Бытует мнение, что сотовые радиотелефоны обеспечивают высокую безопасность переговоров, поскольку каждый вход в связь абонентского аппарата происходит на другом канале (частоте) и, кроме того, каналы приема и передачи разнесены между собой. Это в еще большей степени касается сотовых систем, использующих цифровые стандарты обработки сигналов. Однако существуют системы, состоящие из специализированного интеллектуального контроллера-демодулятора и приемника-сканера, управляемых портативным ком-

пьютером. Оператору достаточно лишь ввести номер интересующего его абонента — и комплекс будет автоматически записывать все входящие и исходящие звонки (переговоры), а также определять телефонные номера и сопровождать мобильный объект при переходе из соты в соту. Так ли это на самом деле?

Чтобы лучше понять проблемы, связанные с использованием беспроводных средств связи, давайте вспомним, что эти средства из себя представляют и как работают.

Современные беспроводные средства персональной связи включают в себя мобильные телефоны сотовой связи, пейджеры и беспроводные стационарные радиотелефоны.

Мобильные телефоны сотовой связи фактически являются сложной миниатюрной приемо-передающей радиостанцией. Каждому сотовому телефонному аппарату присваивается свой электронный серийный номер, который кодируется в микрочипе телефона при его изготовлении и сообщается изготовителями аппаратуры специалистам, осуществляющим его обслуживание. Кроме того, некоторые изготовители указывают этот номер в руководстве для пользователя. При подключении аппарата к сотовой системе связи техники компании, предоставляющей услуги этой связи, дополнительно заносят в микрочип телефона еще и мобильный идентификационный номер.

Мобильный сотовый телефон имеет большую, а иногда и неограниченную дальность действия, которую обеспечивает сотовая структура зон связи. Вся территория, обслуживаемая сотовой системой связи, разделена на отдельные прилегающие друг к другу зоны связи, или соты. Телефонный обмен в каждой такой соте управляется базовой станцией, способной принимать и передавать сигналы на большом количестве радиочастот. Кроме того, эта станция подключена к обычной проводной телефонной сети и оснащена аппаратурой преобразования ВЧ-сигнала сотового телефона в НЧ-сигнал проводного телефона, и наоборот, чем обеспечивается сопряжение обеих систем. Периодически базовая станция излучает в эфир служебный сигнал. Приняв его, мобильный телефон автоматически добавляет к нему свои серийный и идентификационный номера и передает получившуюся кодовую комбинацию на базовую станцию. В результате этого осуществляется идентификация конкретного сотового телефона, номера счета его владельца и привязка аппарата к определенной зоне, в которой он находится в данный момент времени. Когда пользователь звонит по своему телефону, базовая станция выделяет ему одну из свободных частот той зоны, в которой он находится, вносит соответствующие изменения в его счет и передает его вызов по назначению. Если мобильный пользователь во время разговора перемещается из одной зоны связи в другую, базовая станция покидаемой зоны автоматически переводит сигнал на свободную частоту новой зоны.

Пейджеры представляют собой мобильные радиоприемники с устройством регистрации сообщений в буквенном, цифровом или смешанном представлении, работающие в основном в диапазоне 140—400 МГц. Система пейджинговой связи принимает сообщение от телефонного абонента, кодирует его в нужный формат и передает на пейджер вызываемого абонента.

Стационарный беспроводный радиотелефон объединяет в себе обычный проводный телефон, представленный самим аппаратом, подключенным к телефонной сети, и приемо-передающее устройство в виде телефонной трубки, обеспечивающей двусторонний обмен сигналами с базовым аппаратом. В зависимости от типа радиотелефона, используемого диапазона частот, мощности передатчика и чувствительности приемника, с учетом наличия помех и переотражающих поверхностей дальность связи между трубкой и базовым аппаратом в помещении составляет в среднем до 50 м, а в зоне прямой видимости — до 3 км.

Проблема безопасности при пользовании сотовым телефоном и другими мобильными средствами персональной беспроводной связи имеет два аспекта:

- физическую безопасность пользователя;
- безопасность информации, передаваемой с помощью этих устройств.

Здесь мы рассмотрим только вопросы, касающиеся информационной безопасности. В настоящее время электронный перехват информации, циркулирующей в сотовых, беспроводных радиотелефонах или пейджерах, стал широко распространенным явлением.

Электронный перехват сотовой связи не только легко осуществить, он к тому же не требует больших затрат на аппаратуру, и его почти невозможно обнаружить. На Западе прослушивание и/или запись разговоров, ведущихся с помощью беспроводных средств связи, практикуют правоохранительные органы, частные детективы, промышленные шпионы, представители прессы, телефонные компании, компьютерные хакеры и т. п. Так, например, в Канаде, по статистическим данным, от 20 до 80 % радиообмена, ведущегося с помощью сотовых телефонов, случайно или преднамеренно прослушивается посторонними лицами.

В западных странах уже давно известно, что мобильные сотовые телефоны, особенно аналоговые, являются самыми уязвимыми с точки зрения защиты передаваемой информации.

Принцип передачи информации такими устройствами основан на излучении в эфир радиосигнала, поэтому любой человек, настроив соответствующее радиоприемное устройство на ту же частоту, может услышать каждое ваше слово. Для этого даже не нужно иметь особо сложной аппаратуры. Разговор, ведущийся с сотового телефона, может быть прослушан с помощью программируемых приемников-сканеров с полосой приема 30 кГц, способных осуществлять поиск в диапазоне 450—1900 МГц.

Легче всего перехватываются аналоговые неподвижные или стационарные сотовые телефоны, труднее — мобильные, так как перемещение абонента в процессе разговора сопровождается снижением мощности сигнала и переходом на другие частоты в случае передачи сигнала с одной базовой станции на другую.

Более совершенны с точки зрения защиты информации цифровые сотовые телефоны, передающие информацию в виде цифрового кода. Однако используемый в них алгоритм шифрования может быть вскрыт опытным специалистом в течение нескольких минут с помощью персонального компьютера. Что касается цифровых кодов, набираемых на клавиатуре цифрового сотового те-

лефона (телефонные номера, номера кредитных карточек или персональные идентификационные номера), то они могут быть легко перехвачены с помощью того же цифрового сканера.

Не менее уязвимыми с точки зрения безопасности информации являются беспроводные радиотелефоны. Они при работе используют две радиочастоты: одну — для передачи сигнала от аппарата к трубке, другую — от трубки к аппарату. Наличие двух частот еще больше расширяет возможности для перехвата. Дальность перехвата, в зависимости от конкретных условий, составляет в среднем до 400 м, а при использовании дополнительной дипольной антенны диапазона — до 1,5 км.

Следует отметить, что часто рекламируемые возможности беспроводного телефона — цифровой код безопасности (*digital security code*) и снижение уровня помех (*interference reduction*) — нисколько не предотвращают возможность перехвата разговоров. Они только препятствуют несанкционированному использованию этого телефона и не дают соседним радиотелефонам звонить одновременно. Сложнее перехватить цифровые радиотелефоны, которые могут использовать при работе от 10 до 30 частот с автоматической их сменой по определенному закону. Однако и их перехват не представляет особой трудности для специалиста.

Такими же уязвимыми в отношении безопасности передаваемой информации являются и пейджеры. В большинстве своем они используют протокол POCSAG, который практически не обеспечивает защиты от перехвата. Сообщения в пейджинговой системе связи могут перехватываться радиоприемниками или сканерами. Существует также целый ряд программных средств, которые позволяют компьютеру в сочетании со сканером автоматически захватывать рабочую частоту нужного пейджера или контролировать весь обмен в конкретном канале пейджинговой связи. Эти программы предусматривают возможность перехвата до 5000 пейджеров одновременно и хранение всей переданной на них информации в своей памяти.

На практике различают узкополосные (аналоговые) и широкополосные (цифровые) каналы передачи сообщений. Под узкополосным каналом понимают стандартный канал, не обладающий частотной избыточностью. Любое преобразование речевых сигналов и данных не должно приводить к существенному расширению спектра передаваемого сообщения.

Для широкополосных каналов полоса спектра сигнала существенно больше полосы спектра сообщения, поэтому возможности таких каналов существенно больше, чем узкополосных.

Любые преобразования в канале связи сопровождаются погрешностями, обусловленными влиянием различного рода дестабилизирующих факторов и помех. В связи с этим важной проблемой наряду с качеством защиты информации является проблема качества восстановленного сообщения.

Радиочастотное общение (переговоры) производится, как правило, с помощью специальных радиостанций и радиотелефонов (рис. 3.31), в том числе и сотовых, действующих преимущественно в диапазоне УКВ-волн.

Под радиотелефоном подразумевается радиостанция, функционирующая в паре с телефонной линией, причем вся эта система может быть либо сугубо индивидуальной (радиоудлинители), либо групповой (сотовой и транковой).

Практика радиообщения зависит от конструкции аппаратуры и осуществляется как на единой общей частоте, так и на разных; как одновременно, т. е. дуплексно, без переключения «прием — передача», так и поочередно, т. е. симплексно с таковым переключением.

Для перехвата радиопереговоров надо знать несущую частоту радиопередачи, на которую в ходе прослушивания и настраивают свою аппаратуру. Если же рабочая частота передатчика совершенно неизвестна (некоторую ориентацию здесь способны дать габариты и конструкция применяемых антенн), то пытаются выявить момент радиосвязи и внимательно просканировать весь диапазон широковолновым радиоприемником (сканером), засекая нужную волну по нюансам разговора или голосу общающегося. Иногда подобный перехват удается провести посредством телевизионного или вещательного ЧМ-приемника либо западного «сэконд-хэндового» радиотелефона.

Зная, что прием и передача зачастую происходят на различных частотах, целесообразно иметь под рукой два радиоприемника, каждый из которых наблюдает за отдельной полосой контролируемого диапазона.

Так как факт радиоперехвата незасекаем, для нейтрализации подобной неприятности разработаны активные уловки, вроде кодирования радиосигналов или резко «прыгающей» частоты. Встретившись с такими изощрениями, проще будет не преодолевать их, а переходить на иные пути добычи потребной информации.

Никто не спорит, сотовые телефоны, пейджеры и просто радиостанции очень практичны. Особенно если человек постоянно в пути. Поэтому все современные виды связи так быстро внедряются в повседневную жизнь любого делового человека, а не только «нового русского». Однако, все шире осваивая образцы западной техники, мы крайне редко задумываемся о том, какую угрозу несет подобное техническое новаторство.

Сотовый телефон — это замечательно, удобно и практично. Но важно знать, что в любой аппаратуре сотовой связи на этапе разработки закладываются следующие возможности:

- представление информации о точном местоположении абонента;
- запись и прослушивание разговоров;
- фиксация номеров (даты, времени, категории и т. д.) вызывающей и принимающей вызов стороны;
- дистанционное включение микрофона для прослушивания.

Немногие знают, что наличие мобильного сотового телефона позволяет определить как текущее местоположение его владельца, так и проследить его перемещения в прошлом.

Текущее положение может выявляться двумя способами. Первым из них является обычный метод триангуляции (пеленгования), определяющий направ-

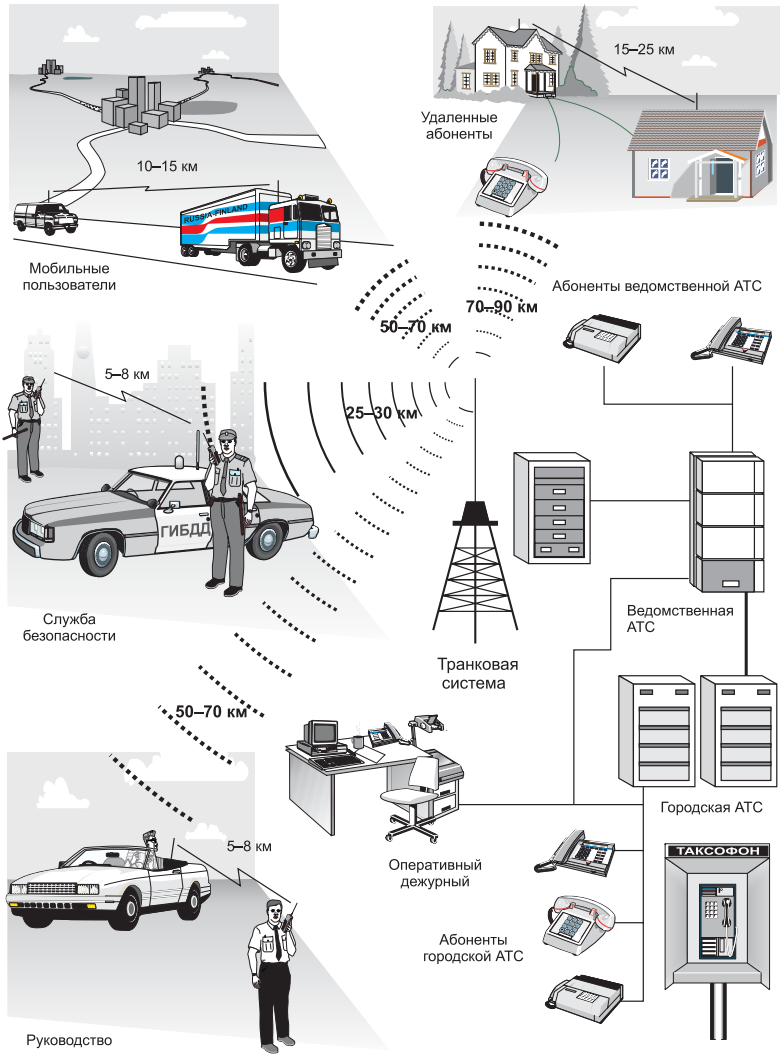


Рис. 3.31. Пример построения радиотелефонной системы

ление на работающий передатчик из нескольких (обычно трех) точек и дающий засечку местоположения источника радиосигналов. Необходимая для этого аппаратура хорошо разработана, обладает высокой точностью и вполне доступна.

Второй метод — через компьютер предоставляющей связь компании, который постоянно регистрирует, где находится тот или иной абонент в данный момент времени даже в том случае, когда он не ведет никаких разговоров (по идентифицирующим служебным сигналам, автоматически передаваемым телефоном на базовую станцию, о которых мы говорили выше). Точность опре-

деления местонахождения абонента в этом случае зависит от целого ряда факторов:

- топографии местности;
- наличия помех и переотражений от зданий;
- положения базовых станций;
- количества работающих в настоящий момент телефонов в данной соте;
- размера соты.

Анализ данных о сеансах связи абонента с различными базовыми станциями (через какую и на какую базовую станцию передавался вызов, дата вызова и т. п.) позволяет восстановить все перемещения абонента в прошлом. Такие данные автоматически регистрируются в компьютерах компаний, предоставляющих услуги сотовой связи, поскольку оплата этих услуг основана на длительности использования системы связи. В зависимости от фирмы, услугами которой пользуется абонент, эти данные могут храниться от 60 дней до 7 лет.

Такой метод восстановления картины перемещений абонента очень широко применяется полицией многих западных стран при расследованиях, поскольку дает возможность восстановить с точностью до минут, где был подозреваемый, с кем встречался (если у второго тоже был сотовый телефон), где и как долго происходила встреча или был ли подозреваемый поблизости от места преступления в момент его совершения.Более того, в связи с тем, что алгоритмы кодирования и защиты в сотовых системах связи намеренно ослаблены (имеют дыры), они становятся легкой добычей для разного рода хакеров и проходимцев.

Тут надо сказать и о СОРМ. Система технических средств по обеспечению оперативно-розыскных мероприятий на отечественных и импортных электронных телефонных станциях предназначена для оперативного контроля соединений определенных абонентов из удаленного пункта управления правоохранительных органов путем взаимодействия этого пункта с оборудованием станций. Она состоит из аппаратно-программных средств и включается в состав штатного оборудования электронных телефонных станций.

Пейджер сегодня стал для многих незаменимым средством оперативного общения. Но мало кто знает, что технология пейджинга позволяет организовать прослушивание (мониторинг) пейджинговых сообщений с помощь несложной аппаратуры (сканер+компьютер+программное обеспечение). Поэтому пейджинговые компании контролируются не только ФСБ, ФАПСИ, но и всеми кому не лень, в том числе криминальными структурами и новоявленными джеймс бондами в лице отечественных фирм, занимающихся частным сыском.

Высшее российское руководство пользуется аппаратами специальной связи, которые контролируются ФАПСИ — Федеральным агентством правительственной связи и информации при президенте. Однако многочисленные «табуны» чиновников, которые привычно обслуживают верховную власть, уже давным-давно обзавелись сотовыми телефонами, пейджерами и радиостанциями.

Новая поросль номенклатурщиков, кажется, напрочь забыла один из главных принципов своих предшественников — «Не болтай! Враг подслушивает!» — и порой несет по служебным радиотелефонам такое, что их недруги просто лопаются от восторга (разумеется, когда ценные данные из радиоперехватов ложатся на их столы).

Владимир С. — бывший кадровый сотрудник КГБ. Ныне, как и положено уважающему себя чекисту в отставке, он возглавляет службу безопасности одного из крупнейших российских банков. Его шеф не только складывает деньги в кубышку, но и старается влезть в большую политику, а значит, интересуется закулисными сторонами жизни сильных мира сего. Поэтому первый четко докладывает своему шефу расстановку сил, а также интересные пикантные подробности, касающиеся его конкурентов. «Для того чтобы все это накопать, мне не надо кому-либо платить деньги, — откровенно признается Владимир. — Чаще всего мы обходимся обыкновенными радиоперехватами. Ведь у каждого крупного чиновника есть помощники, охрана, водители, личные фотографы, парикмахеры и так далее. Стоит определить круг этих людей, номера их пейджеров, сотовых телефонов, частоты станций, чтобы узнать все необходимое. Когда рядом с нужным человеком ошиваются десятки, сотни людей и при этом они постоянно с кем-то разговаривают, выдавая хоть косвенную, но достаточную для анализа информацию, очень просто понять все происходящее вокруг него. Именно по этой причине нам ничего не стоит «вычислить» кого угодно».

Человек, далекий от мира техники, неминуемо придет в ужас, узнав, что в любой момент он может оказаться «под колпаком» у каких-то неизвестных людей. Но технари давно в курсе и относятся к подобным вариантам спокойно. Они говорят: «Если человеку бояться нечего, то он может спокойно пользоваться всеми видами телекоммуникации. Если он хочет обезопасить себя, то пусть предохраняется — покупает что-нибудь подороже или переходит на эзопов язык. Другого пути нет».

Для перехвата радиопереговоров необходимо знать несущую частоту радиопередачи, на которую в ходе прослушивания и настраивают аппаратуру перехвата. Если же рабочая частота передатчика совершенно неизвестна (некоторую ориентацию здесь способны дать габариты и конструкция применяемых антенн), сканируется весь диапазон широковолновым радиоприемником (сканером), засекая нужную волну по нюансам разговора или голосу общающегося. Уникальными возможностями для подслушивания обладает радиотелефон «Алтай» и ему подобные.

Зная, что прием и передача зачастую происходят на различных частотах, целесообразно иметь под рукой два радиоприемника, каждый из которых наблюдает за отдельной частотной полосой контролируемого диапазона.

Так как факт радиоперехвата незасекаем, для нейтрализации подобной неприятности разработаны различные уловки, вроде кодирования радиосигналов, скремблирования или шифрования передаваемой информации. Встретившись с такими изощрениями, проще будет не преодолевать их, а переходить на иные пути добычи необходимой информации.

Рис. 3.32. Мобильный автоматизированный комплекс

Все чаще для подобных целей используются специальные аппаратно-программные комплексы, способные выполнять двойную задачу:

- контроль за несанкционированным снятием информации и обнаружение каналов утечки;
- получение информации, передаваемой по средствам связи.

Примером может служить мобильный автоматизированный комплекс «Крона-5». Этот комплекс предназначен для автоматического обнаружения радиоизлучающих устройств различных типов, в том числе с закрытием канала передачи информации путем инверсии спектра и частотной мозаики, средств съема акустической информации с передачей ее по электросети, ИК-каналу, телефонным и любым другим проводным линиям. Комплекс имеет небольшие габариты (рис. 3.32) и удобен в эксплуатации. В самом простом и дешевом варианте комплектации комплекс состоит из сканирующего радиоприемника с антенной, аппаратуры электропитания, панели коммутации и управления, смонтированных в кейсовой укладке, и специального программного обеспечения. Наращивание возможностей такого варианта комплекса осуществляется за счет установки в заранее предусмотренных отсеках корпуса дополнительных элементов.

Защита информации в средствах связи

Безопасность связи при передаче речевых сообщений основывается на использовании большого количества различных методов закрытия сообщений, меняющих характеристики речи таким образом, что она становится неразборчивой и неузнаваемой для подслушивающего лица, перехватившего закрытое сообщение. При этом оно занимает ту же полосу частот, что и открытый сигнал. Выбор методов закрытия зависит от вида конкретного применения и технических характеристик канала передачи.

В зависимости от спектра передачи речевых сигналов методы защиты речевых сигналов в узкополосных каналах разделяют на следующие виды:

- аналоговое скремблирование;
- маскирование сигнала специальной заградительной помехой;
- дискретизация речи с последующим шифрованием.

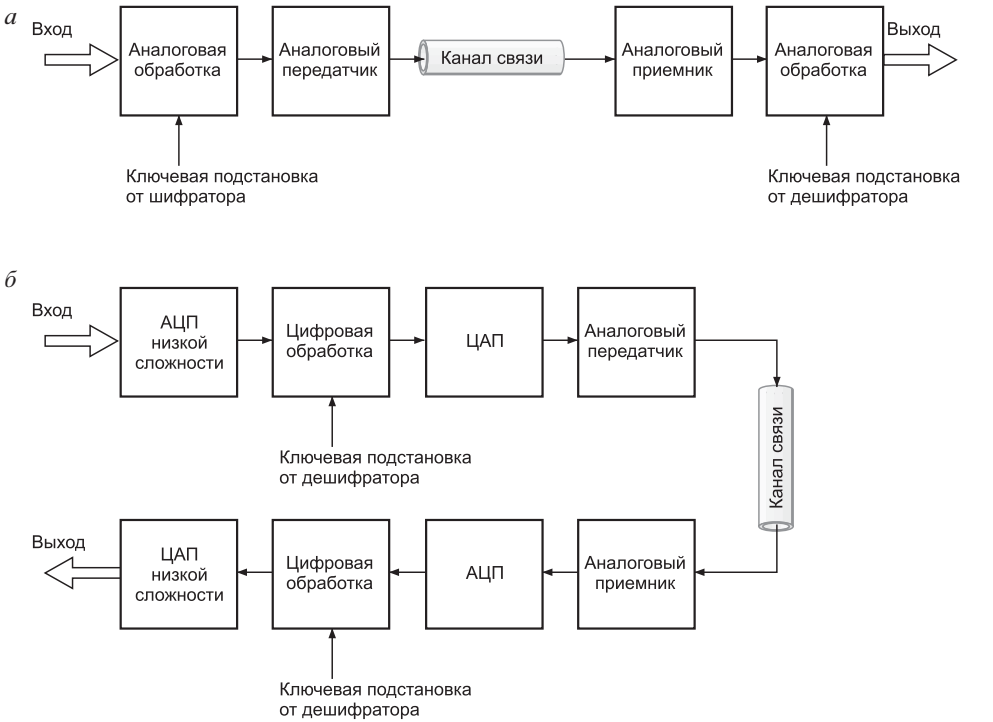


Рис. 3.33. Структурная схема аналогового скремблера: *а* — с частотными или временными перестановками; *б* — с применением цифровой обработки

При аналоговом скремблировании изменяется характеристика речевого сигнала, в результате чего образуется модулированный сигнал, обладающий свойствами неразборчивости и неузнаваемости. Полоса частот спектра преобразованного сигнала остается такой же, как и исходного. Аналоговое скремблирование осуществляется на базе временной и/или частотной перестановок отрезков речи.

За счет временных перестановок преобразованное сообщение кодируется, при этом расширяется спектр. Искажения спектра в узкополосном канале определяют потери в восстановленном сообщении. Аналогично перестановки отрезков спектра при частотном скремблировании приводят к интермодуляционным искажениям восстанавливаемого сообщения.

Маскирование речевого сигнала основано на формировании аддитивной заградительной помехи с последующим ее выделением и компенсацией на приемной стороне. Как правило, этот метод используется в сочетании с простейшим скремблированием (наложением мультипликативной помехи на сигнал).

При указанном преобразовании полоса спектра преобразованного сообщения не должна существенно расширяться. В противном случае возникают искажения восстановленного сообщения. Необходимо, чтобы время корреля-

ции скремблирующих последовательностей было значительно больше времени корреляции сообщения.

Метод дискретизации речи с последующим шифрованием предполагает передачу основных компонентов речевого сигнала путем преобразования их в цифровой поток данных, который смешивается с псевдослучайной последовательностью. Полученное таким образом закрытое сообщение с помощью модема передается в канал связи.

В цифровых системах компоненты речи преобразуются в цифровой поток. Дальнейшие операции преобразования включают перестановку, скремблирование псевдослучайной последовательностью, временное запаздывание.

Для согласования результирующего потока закрытых данных с полосой канала используется модем. Предварительно сжимается спектр сообщения, например, с помощью вокодера (*voice coder* — кодирование голоса), выделяющего наиболее важные компоненты речи. Если не используется сжатие, то применяют высокоскоростные модемы. В любом случае это приводит к потере качества воспроизведения сообщения.

Рассмотрим структурные схемы, реализующие указанные методы защиты (рис. 3.33).

В этих схемах в канале связи при передаче присутствуют отрезки исходного, открытого сообщения, преобразованные в частотной и/или временной области. Обычно считалось, что наряду с высоким качеством и разборчивостью восста-

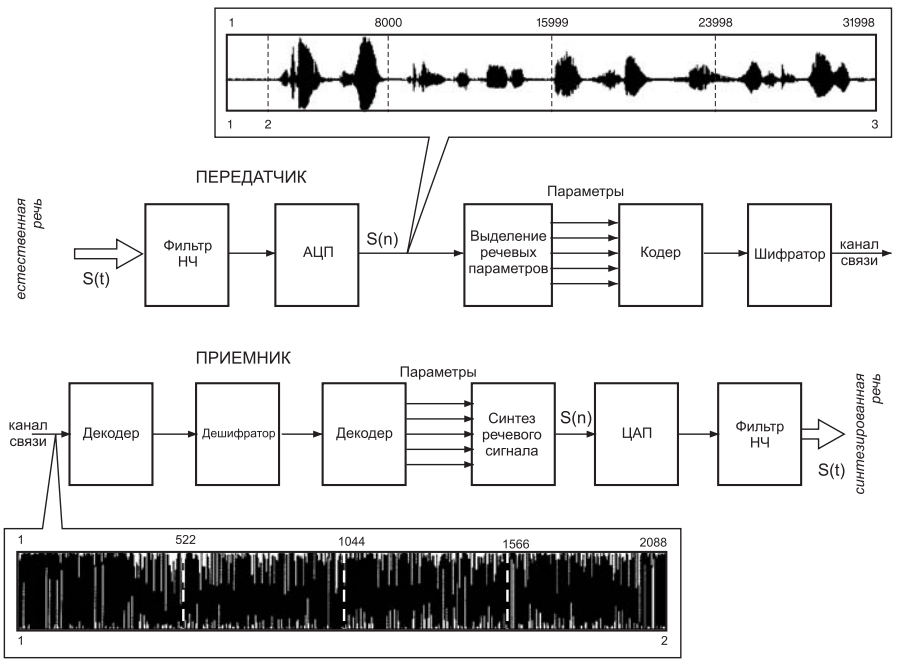


Рис. 3.34. Система скремблирования, обеспечивающая высокий уровень защиты

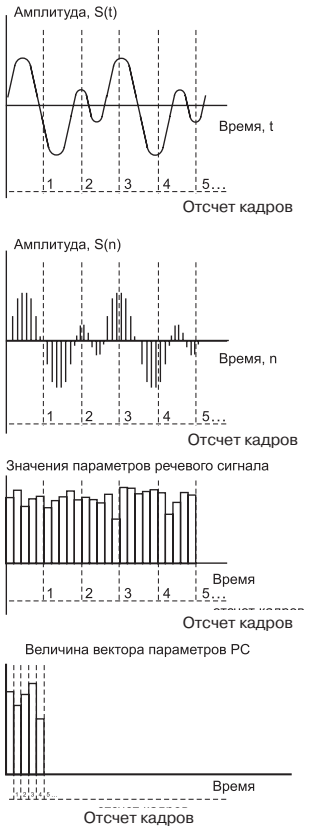


Рис. 3.35. Анализ речевого сигнала

новленной речи аналоговые скремблеры могут обеспечивать лишь низкую или среднюю, по сравнению с системами цифрового кодирования и шифрования, степень секретности. Однако новейшие алгоритмы обработки сигналов способны обеспечить не только средний, но иногда и очень высокий уровень защиты в системе, представленной на рис. 3.34.

В этой системе скремблирования используется вокодер. На этапе анализа речи речевой сигнал *S(t)* пропускается через фильтр нижних частот с частотой среза, не превышающей половины частоты дискретизации, а затем подвергается аналого-цифровому преобразованию. Затем производится членение оцифрованного сигнала *S(t)* на кадры (рис. 3.35). В дальнейшем обработка речевого сигнала производится кадр за кадром, причем длина анализируемого кадра может быть переменной, но частота следования кадров обычно остается постоянной. На каждом кадре речи выполняется процедура выделения ряда речевых параметров. Далее следуют необходимые для заданной скорости передачи и степени защиты речевой информации процедура кодирования (побитной упаковки) и процедура шифрования (перемещение битов) полученных при анализе параметров в вектор передаваемых кодовых сигналов.

На этапе синтеза речи (в приемнике) кодовые символы дешифрируются и декодируются с целью выделения переданных параметров, и на их основе осуществляется синтез речевого сигнала.

Система, схема которой приводится на рис. 3.36, кроме задачи закрытия речевой информации обеспечивает и сокрытие факта передачи полезного сигнала по каналу связи, поскольку результирующий маскированный сигнал воспринимается сторонними наблюдателями как случайная помеха. Системы увеличивают степень закрытия передачи дискретной речи, так как в канал связи передается непрерывный кодированный сигнал, а не отдельными отрезками, как в предыдущих методах.

При передаче больших объемов закрытой информации по существующим сетям общего пользования возникает задача защиты этих каналов. В этом случае наиболее эффективными являются средства канального шифрования. Потенциальными потребителями таких средств защиты являются организации, имеющие выделенные каналы связи между своими подразделениями. Это государственные, дипломатические, банковские и другие организации.

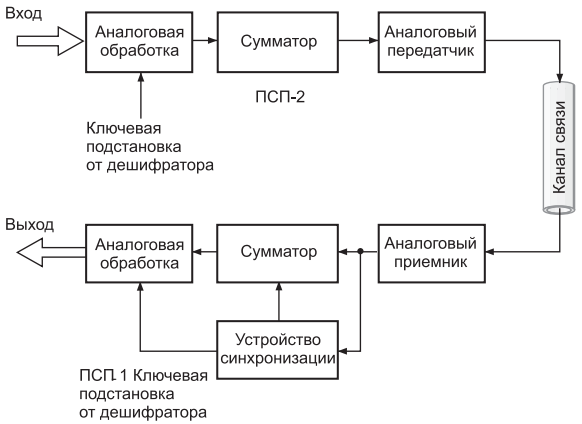


Рис. 3.36. Структурная схема маскиратора речевого сигнала заградительной помехой

Известные поточные методы защиты построены на скремблировании (суммировании по модулю два) потока данных, передаваемых от открытого источника информации, и последовательности, формируемой на основе известных законов образования псевдослучайных последовательностей (ПСП). Перед началом каждого закрытого сеанса связи в канал связи передается синхропосылка, длительность и закон образования которой остаются неизменными от сеанса к сеансу. Это упрощает взаимодействие между абонентами обмена, но уменьшает степень защиты, так как обозначает начало анализа дешифрования закрытых данных.

Известны средства защиты, в которых для каждого сеанса связи передается дополнительно с синхропосылкой ключ сеанса со случайным законом образования. Это увеличивает количество переборов различных комбинаций при анализе, однако при знании длительности ключа сеанса все равно обозначает начало дешифрования потока закрытых данных.

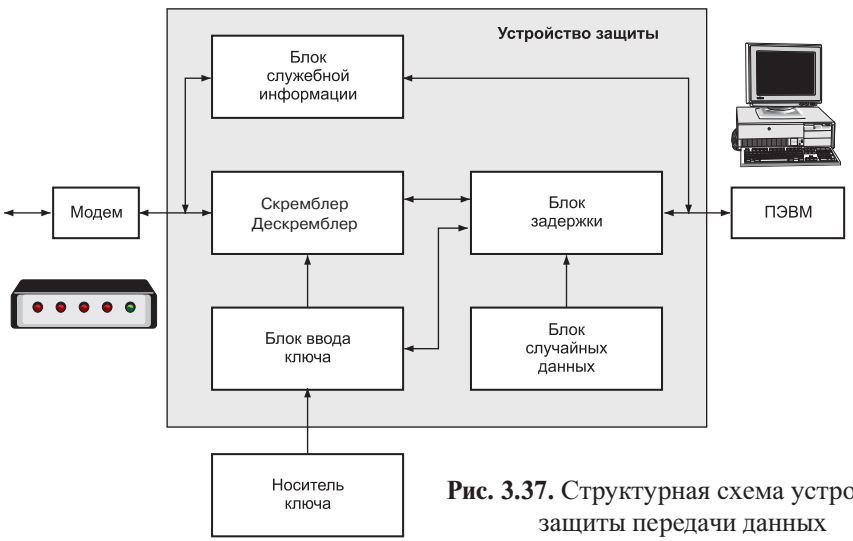


Рис. 3.37. Структурная схема устройства защиты передачи данных

Существует алгоритм (рис. 3.37), который обеспечивает более высокую степень защиты. Это достигается, по сравнению с предыдущим методом, введением случайной задержки начала шифрования потока данных и имитации случайных данных между синхропосылкой и началом шифрования.

Устройство работает следующим образом. Перед сеансом связи производится перевод устройства защиты в режим закрытого канала. Данная операция осуществляется по команде с компьютера. Для этого потребитель должен ввести ключевую информацию с носителя ключа. Носитель ключа может быть магнитным, оптическим и т. д. После того как информация индивидуального носителя сравнилась и совпала с заранее записанной, на мониторе компьютера появляется надпись «Канал закрыт». Далее потребитель производит установление соединения между абонентами по обычному протоколу обмена. Когда абоненты установили соединение, происходит передача: синхропосылки, ключа сеанса связи и случайных данных, сформированных датчиком случайных чисел. После этого происходит шифрование потока данных.

Для того чтобы оценить степень защиты кодирования с помощью такого алгоритма, требуется оценить количество возможных комбинаций при дешифровании. При условии, что анализ дешифрования производится путем поиска стандартных комбинаций (например, «длинные паузы в начале текста», «смысловые фразы» и т. д.), то степень защиты может быть оценена отношением вероятностей, первая из которых зависит от многих факторов, в том числе каким быстродействием и интеллектуальным качеством будет обладать аппаратура анализа, а вторая — от реализации конкретной аппаратуры защиты канала связи. Степень защиты можно увеличивать путем повышения количества возможных значений задержек и увеличения алфавита стандартных фраз в датчике случайных данных.

Для широкополосных каналов полоса спектра сигнала существенно больше полосы спектра сообщения. Дополнительная защита информации осуществляется путем скремблирования цифрового потока либо модуляцией узкополосного сигнала псевдослучайной последовательностью. На приемной стороне происходит обратное преобразование (сжатие сигнала с последующим выделением информации).

Особенностью таких систем является энергетическая скрытность, а также возможность качественной работы многих абонентов в общей полосе частот за счет кодового разделения каналов. В случае передачи речевых сообщений по широкополосным каналам возможны, по крайней мере, два варианта построения:

модуляция речевым сообщением одного из параметров скремблирующей последовательности (задержка, тактовая частота и т. д.) и последующий перенос спектра полученного сигнала в заданный диапазон;

формирование радиосигнала путем модуляции речевым сообщением одного из параметров несущего колебания и последующая манипуляция одного из параметров радиосигнала скремблирующей последовательности.

Спектры сигналов для этого случая приведены на рис. 3.38 *(а—г)*. При относительно высоком качестве воспроизведения речевых сообщений указан-

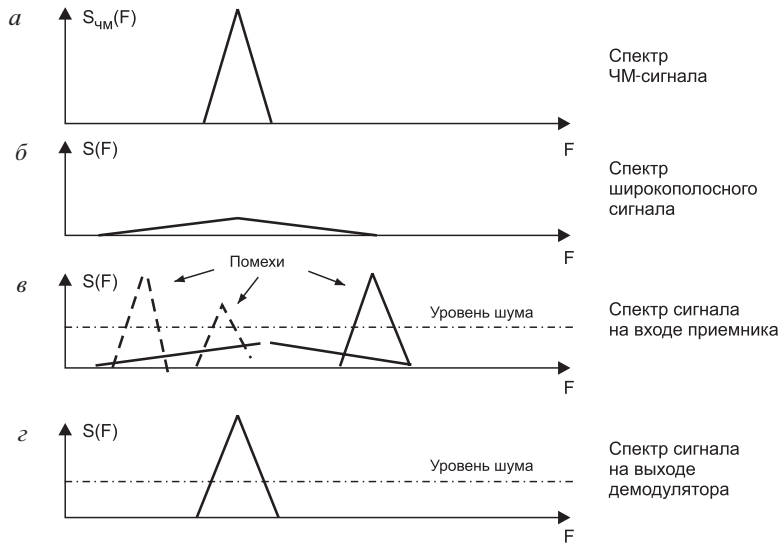


Рис. 3.38. Спектры сигналов в широкополосной системе

ные методы обеспечивают высокую степень защиты. Кроме того, за счет расширения спектра передаваемого сигнала обеспечивается энергетическая скрытность радиолиний. Обобщенные характеристики систем защиты речевых сообщений и данных, передаваемых по каналам связи, приведены в табл. 3.1.

Проблема безопасности при использовании современных беспроводных средств связи достаточно серьезна, но, используя здравый смысл и известные приемы противодействия, ее можно в той или иной степени решить. Не будем затрагивать тех мер, которые могут предпринять только провайдеры связи (например, введение цифровых систем). Поговорим о том, что может сделать каждый самостоятельно.

Для предотвращения перехвата информации с сотовых телефонов:

- используйте общепринятые меры по предупреждению раскрытия информации: избегайте или сведите к минимуму передачу конфиденциальной информации, такой, как номера кредитных карточек, финансовые вопросы, пароли. Прибегайте в этих целях к более надежным проводным телефонам, убедившись, однако, что ваш собеседник не использует в этот момент радиотелефон. Не используйте сотовые или беспроводные телефоны для ведения деловых разговоров;

Таблица 3.1. **Характеристики систем защиты речевых сообщений и данных**

Среднегеометрические частоты октавных полос, Гц	63	125	250	500	1000	2000	4000	8000
b_a, дБ/км	0	0,7	1,5	3	6	12	24	48

- помните, что труднее перехватить разговор, который ведется с движущегося автомобиля, так как расстояние между ним и перехватывающей аппаратурой (если та находится не в автомобиле) увеличивается и сигнал ослабевает. Кроме того, при этом ваш сигнал переводится с одной базовой станции на другую с одновременной сменой рабочей частоты, что не позволяет перехватить весь разговор целиком, поскольку для нахождения этой новой частоты требуется время;
- используйте системы связи, в которых данные передаются с большой скоростью при частой автоматической смене частот в течение разговора;
- используйте при возможности цифровые сотовые телефоны;
- отключите полностью свой сотовый телефон, если не хотите, чтобы ваше местоположение стало кому-то известно.

В случае использования беспроводного радиотелефона:

- при покупке выясните, какую защиту он предусматривает;
- используйте радиотелефоны с автоматической сменой рабочих частот типа *spread spectrume* или цифровые, работающие на частотах порядка 900 МГц и более;
- при возможности используйте радиотелефоны со встроенным чипом для шифрования сигнала.

Для предотвращения мошенничества:

- узнайте у фирмы-производителя, какие средства против мошенничества интегрированы в ваш аппарат;
- держите документы с идентификационным номером вашего телефона в надежном месте;
- ежемесячно и тщательно проверяйте счета на пользование сотовой связью;
- в случае кражи или пропажи вашего сотового телефона сразу предупредите фирму, предоставляющую вам услуги сотовой связи;
- держите телефон отключенным до того момента, пока вы не решили им воспользоваться. Этот способ самый легкий и дешевый, но следует помнить, что для опытного специалиста достаточно одного вашего выхода на связь, чтобы выявить все параметры номера вашего аппарата;
- регулярно меняйте через компанию, предоставляющую вам услуги сотовой связи, идентификационный номер вашего аппарата. Этот способ несколько сложнее предыдущего и требует времени;
- попросите компанию, предоставляющую вам услуги сотовой связи, установить для вашего телефона дополнительный 4-значный PIN-код, набираемый перед разговором. Этот код затрудняет деятельность мошенников, но, к сожалению, небольшая модификация аппаратуры перехвата позволяет выявить и его;
- наиболее эффективным методом противодействия является шифрование идентификационного номера (вместе с голосовым сигналом) по случайному закону.

ГЛАВА ЧЕТВЕРТАЯ
ИНФОРМАЦИЯ В КОМПЬЮТЕРНЫХ СЕТЯХ

4.1. Получение информации с компьютера

Концентрация информации в компьютерах — аналогично концентрации наличных денег в банках — заставляет все более усиливать контроль в целях защиты информации. Юридические вопросы, частная тайна, национальная безопасность — все эти соображения требуют усиления внутреннего контроля в коммерческих и правительственных организациях. Работы в этом направлении привели к появлению новой дисциплины: безопасность информации. Специалист в области безопасности информации отвечает за разработку, реализацию и эксплуатацию системы обеспечения информационной безопасности, направленной на поддержание целостности, пригодности и конфиденциальности накопленной в организации информации. В его функции входит обеспечение физической (технические средства, линии связи и удаленные компьютеры) и логической (данные, прикладные программы, операционная система) защиты информационных ресурсов.

Сложность создания системы защиты информации определяется тем, что данные могут быть похищены из компьютера и одновременно оставаться на месте; ценность некоторых данных заключается в обладании ими, а не в уничтожении или изменении.

Обеспечение безопасности информации — дело дорогостоящее, и не столько из-за затрат на закупку или установку различных технических или программных средств, сколько из-за того, что трудно квалифицированно определить границы разумной безопасности и соответствующего поддержания системы в работоспособном состоянии.

Объектами посягательств могут быть как сами технические средства (компьютеры и периферия), как материальные объекты, так и программное обеспечение и базы данных, для которых технические средства являются окружением.

В этом смысле компьютер может выступать и как предмет посягательств, и как инструмент, с помощью которого оно возможно. Если разделять два последних понятия, то термин «компьютерное преступление» как юридическая категория не имеет особого смысла. Если компьютер — только объект посягательства, то квалификация правонарушения может быть произведена

по существующим нормам права. Если же только инструмент, то достаточен такой признак, как «применение технических средств». Возможно объединение указанных понятий, когда компьютер одновременно и инструмент, и предмет. В частности, к этой ситуации относится факт хищения машинной информации. Если хищение информации связано с потерей материальных и финансовых ценностей, то этот факт можно квалифицировать как преступление. Также если с данным фактом связываются нарушения интересов национальной безопасности, авторства, то уголовная ответственность прямо предусмотрена в соответствии с законами РФ.

Каждый сбой работы компьютерной сети — это не только моральный ущерб для работников предприятия и сетевых администраторов. По мере развития технологий платежей электронных, «безбумажного» документооборота и других серьезный сбой локальных сетей может просто парализовать работу целых корпораций и банков, что приведет к ощутимым материальным потерям. Не случайно защита данных в компьютерных сетях становится одной из самых острых проблем в современной информатике.

Обеспечение безопасности информации в компьютерных сетях предполагает создание препятствий для любых несанкционированных попыток хищения или модификации передаваемых в сети данных. При этом весьма важным является сохранение таких свойств информации, как

- доступность,
- целостность,
- конфиденциальность.

Доступность — это свойство информации, характеризующее ее способность обеспечивать своевременный и беспрепятственный доступ пользователей к интересующей их информации.

Целостность информации заключается в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

Конфиденциальность — это свойство информации, указывающее на необходимость введения ограничений на доступ к данной информации определенного круга пользователей.

Следует также отметить, что отдельные сферы деятельности (банковские и финансовые институты, информационные сети, системы государственного управления, оборонные и специальные структуры) требуют специальных мер безопасности данных и предъявляют повышенные требования к надежности функционирования информационных систем в соответствии с характером и важностью решаемых ими задач.

Для того чтобы правильно оценить возможный реальный ущерб от потери информации, хранящейся на вашем компьютере или циркулирующей в вашей вычислительной сети, рассмотрим сначала, какие же угрозы при этом могут возникнуть и какие необходимо принимать адекватные меры по их защите.

Перехват компьютерной информации

Стандартность архитектурных принципов построения оборудования и программного обеспечения определяет сравнительно легкий доступ профессионала к информации, находящейся в персональном компьютере (ПК). Ограничение доступа к ПК путем введения кодов не обеспечивает полной защиты информации. Включить компьютер и снять код доступа к системе не вызывает особых затруднений — достаточно отключить аккумулятор на материнской плате. На некоторых моделях материнских плат для этого предусмотрен специальный переключатель. Также у каждого изготовителя программы BIOS (AMI, AWARD и др.) есть коды, имеющие приоритет перед любыми пользовательскими, набрав которые можно получить доступ к системе. В крайнем случае можно украсть системный блок компьютера или извлечь из него жесткий диск и уже в спокойной обстановке получить доступ к необходимой информации. Среди большого количества возможных угроз безопасности информации рассмотрим те, которые связаны с целенаправленным непосредственным доступом злоумышленников к техническим средствам информационно-вычислительных компьютерных сетей и обусловлены недостатками технических и программных средств зашиты данных, операционных систем, математического и программного обеспечения.

К умышленным угрозам относятся:

- несанкционированный доступ к информации и сетевым ресурсам;
- раскрытие и модификация данных и программ, их копирование;
- раскрытие, модификация или подмена трафика вычислительной сети;
- разработка и распространение компьютерных вирусов, ввод в программное обеспечение «логических бомб»;
- кража магнитных носителей и расчетных документов, разрушение архивной информации или умышленное ее уничтожение;
- фальсификация сообщений, отказ от факта получения информации или изменение времени ее приема;
- перехват и ознакомление с информацией, передаваемой по каналам связи, и т. п.

Проблема информационной безопасности постоянно усугубляется процессами проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных, и прежде всего информационно-вычислительных систем. Десятилетие назад, когда компьютеры еще не были объединены в сети, единственной возможностью несанкционированного доступа к информации было знание пароля, который можно было получить от небрежного пользователя или подобрать.

Хакеры, «электронные корсары», «компьютерные пираты» — так называют людей, осуществляющих несанкционированный доступ в чужие информационные сети, как правило, для забавы. Набирая наудачу один номер за другим, они терпеливо дожидаются, пока на другом конце провода не отзовется

чужой компьютер. После этого телефон подключается к приемнику сигналов в собственном ПК — и связь установлена. Если теперь угадать код (а слова, которые служат паролем, часто банальны), то можно внедриться в чужую компьютерную систему.

Несанкционированный доступ к файлам законного пользователя осуществляется также нахождением слабых мест в защите системы. Однажды обнаружив их, нарушитель может не спеша исследовать содержащуюся в системе информацию, копировать ее, возвращаться к ней много раз, как покупатель рассматривает товары на витрине.

В наши дни хакер может написать простенькую программу, которая выдает себя за клиента сетевой файловой системы NFS (Network File System), и, обходя обычные средства контроля доступа, получить прямой доступ к файлам пользователя. NFS — не единственное сетевое средство, уязвимое для подобного рода вмешательств, практически все сетевые модули имеют этот недостаток.

Программисты иногда допускают ошибки в программах, которые не удается обнаружить в процессе отладки. Авторы больших сложных программ могут не заметить некоторых слабостей логики их работы. Обычно они все-таки выявляются при проверке, редактировании, отладке программы, но абсолютно избавиться от них невозможно. Кроме того, уязвимые места иногда обнаруживаются и в электронных цепях, особенно в системах связи и передачи данных. Все эти небрежности и ошибки приводят к появлению существенных «брешей» в системах защиты информации.

Бывает, что некто проникает в компьютерную систему, выдавая себя за законного пользователя. Системы, которые не обладают средствами аутентичной идентификации (например, по физиологическим характеристикам: по отпечаткам пальцев, рисунку сетчатки глаза, голосу и т. п.), оказываются без защиты против этого приема. Самый простейший путь его осуществления — это получить коды и другие идентифицирующие шифры законных пользователей. Это может производиться следующими способами:

- приобретением (обычно подкупом персонала) списка пользователей со всей необходимой информацией;
- обнаружением такого документа в организациях, где не налажен достаточный контроль за их хранением;
- подслушиванием через телефонные линии.

Иногда случается, как, например, с ошибочными телефонными звонками, что пользователь с удаленного терминала подключается к чьей-то системе, будучи абсолютно уверенным, что он работает с той системой, с какой и намеревался. Владелец системы, к которой произошло фактическое подключение, формируя правдоподобные отклики, может поддерживать это заблуждение в течение определенного времени и таким образом получить некоторую информацию, в частности коды.

Проблема защиты информации от несанкционированного доступа особо обострилась с широким распространением локальных и особенно глобальных компьютерных сетей. Основной целью хакеров, по мнению специалистов, является сбор большого количества имен и паролей входа. Как правило, их не интересуют коммерческие тайны, хотя некоторым удавалось прорываться в сети крупных компаний по разработке программных продуктов, внедряться в телекоммуникационные сети банков, учреждения министерства обороны и т. п.

К уязвимым местам в вычислительных сетях можно отнести следующие:

- применение компьютеров, не имеющих парольной защиты во время загрузки;
- использование совместных или легко вскрываемых паролей;
- хранение паролей в пакетных файлах и на дисках компьютеров;
- отсутствие установления подлинности пользователя в реальном масштабе времени;
- отсутствие или низкая эффективность применения систем идентификации и аутентификации пользователей;
- недостаточность физического контроля за сетевыми устройствами;
- отсутствие отключения терминала при многочисленных неудачных попытках установления сеанса связи и регистрации таких попыток;
- незащищенность модемов.

Для защиты компьютерных сетей или отдельных компьютеров от несанкционированного использования применяются три основных вида контроля доступа.

В случае контроля доступа, основанного на обладании, речь идет о предметах, принадлежащих пользователю, — физическом ключе, магнитной карте, металлической пластинке причудливой формы, которую вставляют перед началом работы в щель распознавателя, и т. п.

В случае контроля доступа, основанного на личностных характеристиках пользователя, используются биометрические приборы, которые анализируют специфические физические особенности пользователя (подпись, тембр голоса, отпечатки пальцев, рисунок линий на ладони или на сетчатке глаза и т. п.) и сравнивают их с теми, что находятся у них в памяти.

Эти два вида компьютерной защиты могут использоваться и для дистанционного управления доступом, хотя обычно к ним прибегают для ограничения доступа к тому месту, где находятся компьютеры, — компьютерному залу или отдельному кабинету.

Вид контроля доступа, основанный на обладании специфической информацией, является наиболее распространенным. Он характеризуется тем, что правом доступа обладают лишь те лица, которые способны продемонстрировать свое знание определенного секрета, обычно пароля. Это самый простой и дешевый путь защиты любой компьютерной системы. Поскольку его использование не требует больших затрат времени, сил и места в памяти компьютера, то им оснащаются даже те компьютеры, которые вовсе не нуждаются в сред-

ствах защиты. Кроме того, использование пароля дает пользователю ощущение психологического комфорта. Более того, этот вид широко используется в системах, уже защищенных другими средствами — магнитными картами или иными программными методами, типа шифрования, что в еще большей степени увеличивает защиту от несанкционированного доступа.

Пароли, как правило, рассматриваются в качестве ключей для входа в систему, но они используются и для других целей: блокирования записи на дисковод, в командах на шифрование данных, т. е. во всех тех случаях, когда требуется твердая уверенность в том, что соответствующие действия будут производиться только законными владельцами или пользователями программного обеспечения.

Используемые пароли можно подразделить на семь основных групп:

- пароли, устанавливаемые пользователем;
- пароли, генерируемые системой;
- случайные коды доступа, генерируемые системой;
- полуслова;
- ключевые фразы;
- интерактивные последовательности типа «вопрос — ответ»;
- «строгие» пароли.

Первая группа является наиболее распространенной. Большинство таких паролей относится к типу «выбери сам». Для лучшей защиты от несанкционированного доступа необходимо использовать достаточно длинный пароль, поэтому обычно система запрашивает пароль, содержащий не менее четырехпяти букв. Существуют также и другие меры, не позволяющие пользователю создать неудачный пароль. Например, система может настаивать на том, чтобы пароль включал в себя строчные и заглавные буквы вперемешку с цифрами; заведомо очевидные пароли, например «internet», ею отвергаются. В разных операционных системах существует немало программ, которые просматривают файлы, содержащие пароли, анализируют пароли пользователей и определяют, насколько они секретны. Неподходящие пароли заменяются.

Когда человек впервые загружает компьютер и тот запрашивает у него пароль, этот пароль наверняка окажется вариантом одной из общих и актуальных для всех тем — особенно если у пользователя не хватает времени. Представьте себе состояние человека, когда его просят придумать собственный секретный пароль. Как бы то ни было, стоит запросу появиться на экране монитора — и человека посещает мысль о том, что надо немедленно что-то предпринимать. Не считая гениев и безнадежных тупиц, все люди, когда надо принимать быстрые решения, мыслят и действуют примерно одинаково. Им требуется время, чтобы начать мыслить творчески, поэтому начальные предположения и первые умозаключения в определенных группах людей оказываются одинаковыми. И пользователи выдают первое, что приходит им в голову. А в голову приходит то, что они видят или слышат в данный момент, либо то, что собираются сделать сразу же после загрузки. В такой ситуации пароль

создается в спешке, а последующая его замена на более надежный происходит достаточно редко. Таким образом, многие пароли, созданные пользователями, могут быть раскрыты достаточно быстро.

Случайные пароли и коды, устанавливаемые системой, могут быть нескольких разновидностей. Системное программное обеспечение может использовать полностью случайную последовательность символов — вплоть до случайного выбора регистров, цифр, пунктуации длины, или же использовать в генерирующих процедурах ограничения. Создаваемые компьютером пароли могут также случайным образом извлекаться из списка обычных или ничего не значащих слов, созданных авторами программы, которые образуют пароли вроде onah.foopn или ocar- back-treen.

Полуслова частично создаются пользователем, а частично — каким-либо случайным процессом. Это значит, что если даже пользователь придумает легко угадываемый пароль, например «абзац», компьютер дополнит его какой-нибудь неразберихой, образовав более сложный пароль типа «абзац,3ю37».

Ключевые фразы хороши тем, что они длинные и их трудно угадать, зато легко запомнить. Фразы могут быть осмысленными — типа «мы были обеспокоены этим», или не иметь смысла — «ловящий рыбу нос». Следует заметить, что в программировании постепенно намечается тенденция к переходу на более широкое применение ключевых фраз. К концепции ключевых фраз близка концепция кодового акронима, который эксперты по защите оценивают как короткую, но идеально безопасную форму пароля. В акрониме пользователь берет легко запоминающееся предложение, фразу, строчку из стихотворения и т. п. и использует первые буквы каждого слова в качестве пароля. Например, акронимами двух приведенных выше фраз являются «мбоэ» и «лрн». Подобные нововведения в теории паролей значительно затрудняют занятия электронным шпионажем.

Интерактивные последовательности «вопрос — ответ» предлагают пользователю ответить на несколько вопросов, как правило, личного плана: «Девичья фамилия вашей матери?», «Ваш любимый цвет?» и т. д. В компьютере хранятся ответы на множество таких вопросов. При входе пользователя в систему компьютер сравнивает полученные ответы с «правильными». Системы с использованием «вопросов — ответов» склонны прерывать работу пользователя каждые 10 мин, предлагая отвечать на вопросы, чтобы подтвердить его право пользоваться системой. В настоящее время такие пароли почти не используются. Когда их придумали, идея казалась неплохой, но раздражающий фактор прерывания привел к тому, что данный метод практически исчез из обихода.

«Строгие» пароли обычно используются совместно с каким-нибудь внешним электронным или механическим устройством. В этом случае компьютер обычно с простодушным коварством предлагает несколько вариантов приглашений, а пользователь должен дать на них подходящие ответы. Этот вид паролей часто встречается в системах с одноразовыми кодами. Одноразовые коды — это пароли, которые срабатывают только один раз. К ним иногда при-

бегают, создавая временную копию для гостей, чтобы продемонстрировать потенциальным клиентам возможности системы. Они также порой применяются при первом вхождении пользователя в систему. Во время первого сеанса пользователь вводит свой пароль и в дальнейшем входит в систему лишь через него. Одноразовые коды могут также применяться в системе, когда действительный пользователь входит в нее в первый раз; затем пользователю следует поменять свой пароль на более секретный персональный код. В случаях, когда системой пользуется группа людей, но при этом нельзя нарушать секретность, прибегают к списку одноразовых кодов. Тот или иной пользователь вводит код, соответствующий времени, дате или дню недели.

Итак, для того чтобы пароль был действительно надежен, он должен отвечать следующим требованиям:

- быть определенной длины;
- включать в себя как прописные, так и строчные буквы;
- включать в себя одну и более цифр;
- включать в себя один нецифровой и неалфавитный символ.

Одно или несколько из этих правил должны обязательно соблюдаться.

Другое дело, когда попасть в помещение, где установлен компьютер, не удается. В этом случае используют дистанционные способы съема информации. Естественно, они эффективны только тогда, когда компьютер включен. Существуют два способа дистанционного считывания информации: первый способ основан на приеме ВЧ-наводок в силовую сеть, а второй — на приеме побочных электромагнитных излучений соединительных цепей ПК.

Побочные электромагнитные излучения и наводки (ПЭМИН)

Необходимо отметить, что практически все технические средства не только сами излучают в пространство сигналы, содержащие обрабатываемую ими информацию, но и улавливают за счет микрофонов либо антенных свойств другие излучения (акустические, электромагнитные), существующие в непосредственной близости от них. Уловив, они преобразовывают принятые излучения в электрические сигналы и бесконтрольно передают их по своим линиям связи на значительные расстояния. Это еще больше повышает опасность утечки информации. К числу технических устройств, способных образовывать электрические каналы утечки, относятся телефоны (особенно кнопочные), компьютеры, средства громкоговорящей связи, радиотрансляционные приемники, датчики охранной и пожарной сигнализации, их линии, а также сеть электропроводки.

Распространение побочных электромагнитных излучений за пределы контролируемой территории создает предпосылки для утечки информации, так как возможен ее перехват с помощью специальных технических средств конт-

роля. В ПК основными источниками электромагнитных излучений являются монитор и соединительные цепи (устройства ввода и вывода информации). Утечке информации в ПК способствует применение коротких видеоимпульсов прямоугольной формы и высокочастотных коммутирующих сигналов. Для уменьшения уровня побочных электромагнитных излучений применяют специальные средства защиты информации: экранирование помещений, фильтрацию источников питания, дополнительное заземление, электромагнитное заземление, а также средства ослабления уровней нежелательных электромагнитных излучений и наводок при помощи различных резистивных и поглощающих согласованных нагрузок.

Если, работая на компьютере, вы одновременно включали телевизор, то, наверное, заметили, что при включенном компьютере на некоторых телевизионных каналах начинаются помехи. Этому есть простое объяснение. Все составляющие части компьютера — провода, усилители, даже печатные платы — работают как антенны, проводящие электромагнитное излучение. Компьютер не только принимает излучение, но и передает, иногда перенося его на некоторое расстояние от источника, а близлежащая электропроводка и металлические трубки могут впоследствии работать как антенны.

Исследования показывают, что излучение видеосигнала монитора является достаточно мощным, широкополосным и охватывает диапазон метровых и дециметровых волн. Причиной мощного излучения является наложение радиосигнала на импульсы развертки изображения, вырабатываемые строчным трансформатором. При кажущейся сложности проблемы аппаратура для этого вида коммерческой разведки достаточно проста (рис. 4.1) и изготавливается на базе обычного малогабаритного телевизора. Такие устройства позволяют на удалении 50 м получать устойчивую картинку — копию изображения, отображаемого в настоящий момент на экране монитора вашего ПК.

Все компьютеры работают на излучение в широком радиочастотном диапазоне и представляют собой радиопередатчики. Когда телевидение принимает сигналы от компьютера, это происходит случайно; а теперь представьте себе, что кто-то решил целенаправленно принимать такую излучаемую информацию. Конечно же это возможно, и такие случаи бывали. Недаром компьютеры с наиболее засекреченной информацией устанавливают в комнатах с непроницаемыми для излучения стенами.

Рассмотрим это явление более подробно. Работа любой вычислительной техники сопровождается электромагнитными излучениями и наводками на соединительные проводные линии, цепи «питание» и «земля», возникающие вследствие электромагнитных воздействий в ближней зоне излучения. Считалось, что достаточно трудно расшифровать информацию, содержащуюся в излучении, и что поэтому восстановление информации под силу только профессионалам, располагающим очень сложной и дорогой аппаратурой обнаружения и декодирования. Однако это оказалось не так. В 1985 году группа шведских ученых под руководством Вильяма Ван Эйка опубликовала статью «Электромагнитное излучение видеодисплеев: утечка информации?». В статье

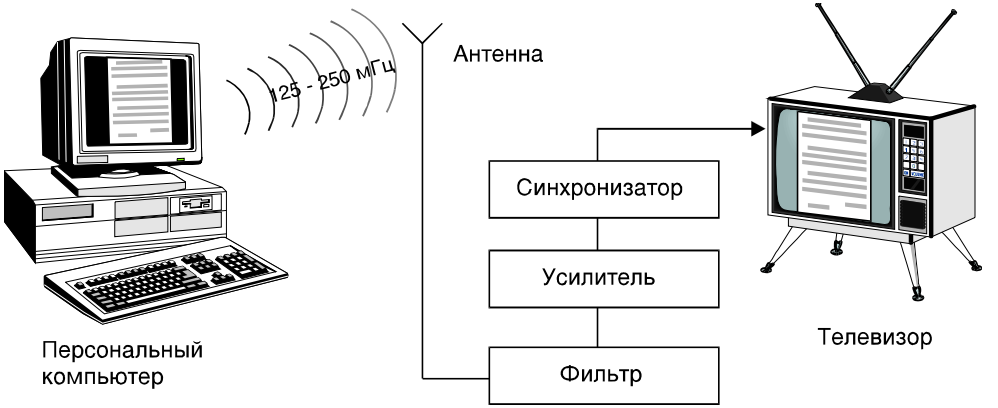


Рис. 4.1. Устройство для снятия информации с компьютера

описывалось, как можно легко и недорого переделать обычный телевизор в прибор для приема и преобразования информации, идущей с любого цифрового устройства, особенно компьютера.

Применение в компьютерах импульсных сигналов прямоугольной формы и ВЧ-коммутации приводит к тому, что в спектре излучений будут компоненты с частотами вплоть до СВЧ. Импульсы — вот ключевое слово. Всем известно, что компьютеры способны преобразовывать длинные строки нулей и единиц во что угодно (например, в наши любимые компьютерные игры). На самом деле, разумеется, по проводам не бегают крошечные нули и единички. По ним просто течет электрический ток различного напряжения, который наше воображение представляет как нули и единички. Любой электрический прибор является источником излучения. Но только цифровой прибор, такой, как компьютер, испускает импульсы высокого и низкого уровня напряжения. Энергетический спектр таких сигналов убывает с ростом частоты, но эффективность их излучения при этом увеличивается и уровень излучений может оставаться постоянным до частот в несколько гигагерц (рис. 4.2). Усиление излучения на некоторых частотах спектра (резонансы) могут вызвать различные паразитные связи. Цепи, не предназначенные для передачи цифровых сигналов, могут излучать их вследствие наводок, например, провода источников питания.

Изображение на экране монитора компьютера формируется в основном так же, как и в телевизионном приемнике. Оно состоит из множества крошечных точек, называемых пикселями. Каждый пиксель представляет собой капельку определенного вещества, которая зажигается (флуоресцирует) под воздействием энергии и покрыта защитным слоем. Контролирующая схема управляет позицией электронной пушки, которая периодически простреливает электронами весь экран, на короткое время зажигая те пиксели, которые должны засветиться. Каждый раз, когда это происходит, мы получаем импульс электро-

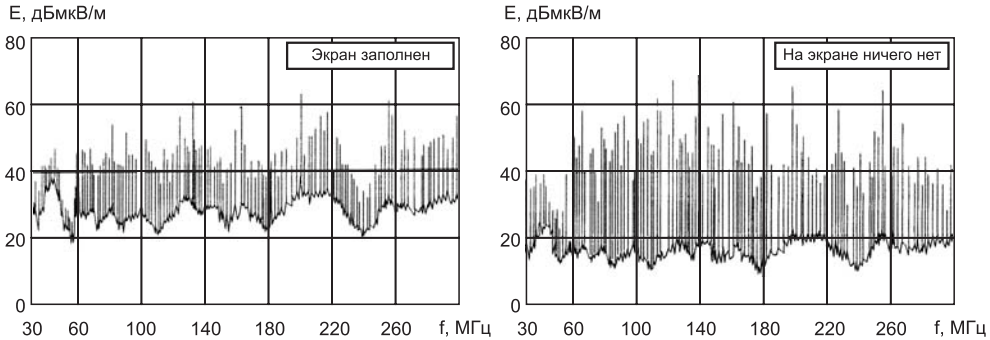


Рис. 4.2. Напряженность электрического поля *E* на расстоянии 1 м от дисплея

магнитного излучения с высоким напряжением. Поскольку видеосигнал является цифровым, то логическая единица создает светящуюся точку, а логический нуль препятствует ее появлению. Однако видеосигнал содержит еще и тактовые синхроимпульсы. Так как последние повторяются, то энергетический спектр видеосигнала содержит гармоники, интенсивность которых убывает с ростом частоты. Источниками излучения видеосигнала дисплея могут быть элементы обработки сигнала изображения и электронный луч кинескопа. Эти сигналы усиливаются до нескольких десятков вольт для подачи на электронно-лучевую трубку.

Уровень широкополосного излучения дисплея зависит от количества букв на экране. Уровень узкополосных составляющих не зависит от заполнения экрана, а определяется системой синхронизации и частотой повторения светящихся точек. Поэтому бывает очень трудно, а подчас и невозможно отделить различные сигналы друг от друга и расшифровать их. Вам вряд ли удастся

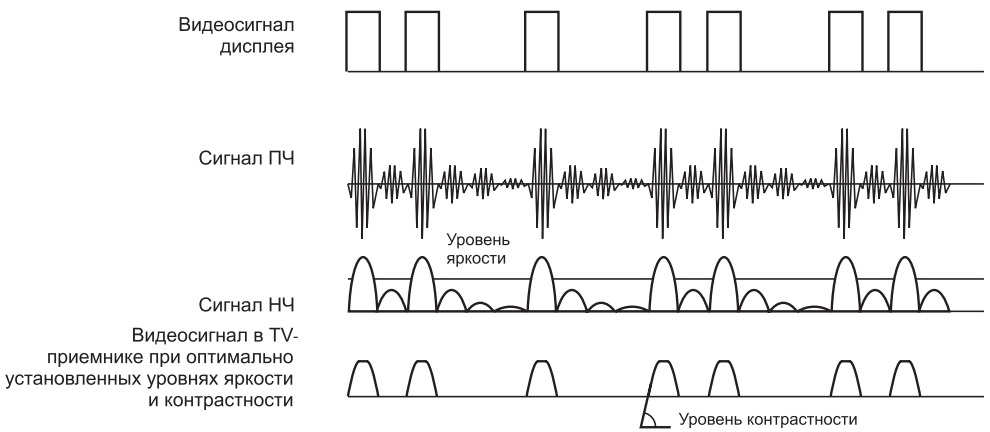


Рис. 4.3. Временные диаграммы сигналов, обрабатываемых в ТВ-приемнике

Рис. 4.4. Видеосигналы в дисплее и ТВ-приемнике

определить, о чем же «думал» компьютер, пока систему сотрясали электромагнитные импульсы. Как же расшифровать всю эту принимаемую мешанину сигналов, исходящих от проводов, печатных плат и т. д.?

Информация, отображаемая на экране дисплея, может быть восстановлена с помощью телевизионного приемника, который обрабатывает лишь небольшую часть спектра сигнала шириной около 8 МГц (обычно ТВ-приемник имеет полосу пропускания 4,5 МГц и демодулятор сигнала с частично подавленной боковой полосой, эквивалентной АМ-детектору с полосой пропускания 8 МГц) на частотах в диапазонах метровых и дециметровых волн. Временные диаграммы сигналов, обрабатываемых ТВ-приемником, представлены на рис. 4.3.

Пусть ТВ-приемник обрабатывает один «лепесток» энергетического спектра излучения, т. е. частота его настройки совпадает с серединой одного из «лепестков», а полоса пропускания равна его ширине. Усиление НЧ-сигнала над порогом, определяющим уровень яркости, задается уровнем контрастности. В первом приближении уровень контрастности определяет крутизну фронтов видеосигнала в приемнике. В отличие от дисплея максимум видеосигнала в ТВ-приемнике определяет уровень черного, а минимум определяет уровень белого. Таким образом, изображение на экране ТВ-приемника будет представлять собой копию изображения на экране дисплея и состоять из черных букв на белом (или сером) фоне.

Если видеосигнал представляет собой длинный импульс, то лучше всего будут излучены в пространство его фронты, которые и дадут при приеме точки (рис. 4.4). Излучение дисплея, принимаемое ТВ-приемником, не содержит информации о синхросигнале, поэтому изображение на экране телевизора будет перемещаться в горизонтальном и вертикальном направлениях. Качество приема может быть улучшено при использовании внешнего генератора синхросигналов. С такой приставкой к обычному телевизору можно восстановить информацию с дисплея почти любого типа при условии достаточно высокого уровня его излучения.

Надо знать, что многочисленные телефоны с кнопочным набором номера сами являются источниками паразитных радиоизлучений, так что разговоры, проводимые с применением некоторых из них, можно пробовать засечь на частоте ДВ-диапазона (около 150 кГц) и дистанции в сотню-другую метров.

Методы защиты информации от ПЭМИН

Методы защиты основываются на особенностях выделения опасного сигнала на фоне внешних помех и внутренних шумов приемника. Они направлены на достижение такого отношения мощности сигнала к мощности помех и шумов, при котором невозможно качественное обнаружение опасного (информационного) сигнала и его регистрация. В связи с этим технические методы защиты информации от утечки через побочные и наведенные электромагнитные поля можно разделить на три группы:

- пассивные методы, связанные с уменьшением интенсивности нежелательных электромагнитных излучений и полей;
- активные методы, связанные с созданием шумовых полей (зашумления) в возможной зоне перехвата информации;
- методы, основанные на применении высокозащищенных (физически) элементов и технологий, в частности волоконно-оптических линий связи.

Основными техническими методами защиты каналов утечки информации являются методы пассивной и активной защиты.

К методам пассивной защиты, локализующим опасные сигналы, относятся:

- экранирование;
- фильтрация;
- заземление;
- применение специальных средств ослабления уровней побочных и наведенных электромагнитных полей.

Одним из основных методов снижения интенсивности нежелательных электромагнитных полей до требуемого уровня является экранирование информационных средств, их элементов и соединительных линий, а также помещений, в которых эти средства размещаются. При его реализации используются средства полного экранирования (экранированные помещения, контейнеры и т. п.) и частичного экранирования (экранирующие щиты, проволочные сетки, металлизированные стекла и ткани, токопроводящие эмали, смолы, смазки и т. д.)

В последние годы наблюдается тенденция все более широкого применения частичного и локального (схемотехнического) экранирования с использованием экранов из специальных проводящих пластмасс и диэлектрических экранов, армированных металлической сеткой или с металлическим напылением. Экранирование теоретически позволяет понизить уровень нежелательного электромагнитного поля.

Фильтрация сигналов, как один из основных методов, используется в различных сечениях (ВЧ- и НЧ-трактах, сигнальных цепях и т. п.) информационных систем, в цепях электропитания, электрочасофикации, пожарной и ох-

ранной сигнализации для ослабления нежелательных излучений, исключения воздействия навязываемых ВЧ-сигналов и прохождения опасных сигналов за пределы контролируемой территории. Основное назначение защитных фильтров — пропускать без значительного ослабления сигналы с частотами, лежащими в их рабочей полосе частот, и подавлять сигналы с частотами, лежащими за пределами этой полосы. Реальные фильтры обеспечивают затухание опасных сигналов на несколько порядков.

Применяются и другие пассивные методы и средства защиты информации, например заземление, поглощающие и неотражающие покрытия и согласованные нагрузки, поглощающие высокочастотные ферритовые кольца, устанавливаемые на кабели, и др.

В ряде случаев эти методы все-таки не обеспечивают необходимого ослабления опасного сигнала за пределами контролируемой зоны. Кроме того, применение средств пассивной защиты может значительно увеличить массу и габариты защищаемого информационного объекта и существенно усложнить процесс его эксплуатации. В таких ситуациях используют системы и средства активной защиты.

Методы активной защиты основаны на создании маскирующих и имитирующих помех для энергетического подавления информационного (опасного) сигнала в канале утечки — электромагнитное зашумление, а также на дополнительном структурном преобразовании информации (кодировании) — кодовое зашумление.

Различают следующие виды электромагнитного зашумления — линейное (зашумление опасных сигналов в кабелях, проводах и токоведущих конструкциях) и пространственное (создание маскирующих помех в пространстве). Специфическим видом электромагнитного зашумления является «самозашумление», возможное при параллельной независимой работе нескольких компьютеров или при использовании мультипрограммного режима работы отдельного компьютера.

Система линейного зашумления представляет собой генератор шумового сигнала, формирующий шумовое напряжение с заданными энергетическими и спектральными характеристиками, который подключается в зашумляемую токоведущую цепь. В системах пространственного зашумления с помощью специальных антенн осуществляется излучение маскирующих помех в окружающее пространство.

При применении систем активного электромагнитного зашумления необходимо учитывать их возможное влияние на качество работы защищаемых и других информационных объектов, расположенных в зоне действия преднамеренных помех. В этом случае более целесообразным может оказаться использование кодового зашумления.

Для достижения наилучших результатов необходимо комплексно использовать средства активной и пассивной защиты, и среди них средства с высокой скрытностью опасных сигналов, в частности волоконно-оптические линии связи.

Рис.4.5. Программно-аппаратный комплекс «Навигатор»

Для обнаружения и автоматизированного измерения побочных электромагнитных излучений от различных технических средств, регистрации, хранения, обработки и документирования полученной информации может использоваться, например, программно-аппаратный комплекс «Навигатор», представленный на рис. 4.5.

Комплекс создан на базе современного анализатора спектра фирмы Hewlett Packard, управляемого компьютером, использующим специальное программное обеспечение. Характерной особенностью комплекса является модульный принцип его построения, позволяющий использовать различные типы анализаторов спектра, измерительных антенн и других компонентов.

Генератор шума «Гном-3»

Генератор шума «Гном-3» (рис. 4.6) предназначен для работы в системах активной защиты. Он устанавливается на объектах ЭВТ для защиты от утечки конфиденциальной информации за счет побочных электромагнитных излучений. Технические характеристики прибора представлены в табл. 4.1.

При установке в помещениях требуется производить монтаж рамочных антенн в соответствии с требованиями руководства по эксплуатации. В комплект поставки антенны не входят и изготавливаются при монтаже.

Рис. 4.6. Генератор шума «Гном-3»

Однако основным способом сохранения секретности данных и сообщений является применение шифрования информации на основе разнообразных криптографических методов.

Конфиденциальная информация, как правило, должна храниться в зашифрован-

Таблица 4.1. **Технические характеристики генератора шума «Гном-3»**

Уровень сигнала на выходных разъемах генератора в различных диапазонах частот		
Диапазон частот	Полоса пропускания, кГц	Уровень сигнала, дБ, не менее
10—150 кГц	200 Гц	70
400 МГц	120	75
150 кГц—30 МГц	9	70
0,4—1 ГГц	120	70
Ослабление уровня выходного сигнала, дБ, в диапазонах частот		
10—150 кГц; 150 кГц—30 МГц		не менее 30
30—400 МГц		не менее 20
Энтропийный коэффициент качества шума на выходе генератора, дБ		не менее 0,8
Система контроля функционирования генератора обеспечивает: индикацию наличия генерации (свечение светодиода РАБОТА); выдачу сигнала АВАРИЯ в виде уровня напряжения $И_{вых.3}$=<0,45 В при срыве генерации на выход, обозначенный ВЫХ.3. При этом светодиод РАБОТА гаснет		
Генератор сохраняет работоспособность при круглосуточной работе		
Питание генератора осуществляется от однофазной сети переменного тока напряжением 220 В +10—15 %, частотой 50±0,5 Гц		
Максимальная электрическая мощность потребления, ВА		не более 20

Окончание табл. 4.1.

Условия работы	
Температура окружающего воздуха, °С	5—40
Относительная влажность воздуха при 30 °С, %	не более 95
Атмосферное давление, мм рт. ст. (кПа)	630—800 (84—106,7)
Габариты, мм	310 97 48,5
Вес, кг	не более 1,8
Средняя наработка на отказ, ч	10 000
Средний срок службы, лет	10
Гарантийный срок эксплуатации, мес.	18

ном виде. В этом случае угроза раскрытия данных будет существенно снижена даже тогда, когда механизмы идентификации, аутентификации и управления доступом будут преодолены. Использование шифрования сокращает риск перехвата и чтения проходящих транзитом через компьютерные сети сообщений конфиденциального характера. Только пользователь сети, обладающий истинным ключом, может расшифровать сообщение после его получения.

Для обеспечения конфиденциальности данных и сообщений могут быть использованы следующие средства и процедуры защиты информации:

- шифрование данных и сообщений;
- защита от перехвата информации в передающей среде компьютерной сети и ее компонентах;
- маскирование содержания сообщений;
- ограничение широковещательной передачи сообщений с помощью маршрутизаторов сети.

Несанкционированное внедрение в базы данных

В последнее время все чаще говорят о несанкционированном внедрении в базы данных. Этот вид пиратства очень быстро развивается вследствие бурного развития компьютеризации при обработке информации в коммерческих кругах с выходом информационных сетей в телефонную сеть общего пользования. Компьютерные взломщики, «хакеры», не ограничиваются вопросами бесплатного получения коммерческой информации, — достаточно случаев вскрытия и перевода денежных счетов из одного банка в другой через информационную сеть общего пользования.

Механизм защиты информации представляет собой совокупность средств (процедур) защиты, функционирующих совместно для выполнения определенной задачи по защите информации.

Для обеспечения безопасности передачи данных в компьютерных сетях используются следующие виды механизмов защиты информации:

- идентификация и аутентификация;
- управление доступом;
- обеспечение конфиденциальности данных и сообщений;
- обеспечение целостности данных и сообщений;
- контроль субъектов взаимодействия;
- регистрация и наблюдение.

Следует отметить, что назначение указанных выше механизмов может быть разнообразным. Некоторые из них предназначены для уменьшения риска угроз, другие обеспечивают защиту от этих угроз, третьи их обнаруживают. При этом в каждом из указанных механизмов важную роль играет применение методов криптографии, позволяющих создавать более совершенные средства защиты.

Первым шагом в обеспечении безопасности информации в компьютерных сетях является возможность проверки подлинности любого пользователя сети. Гарантированная проверка личности пользователя — задача различных механизмов идентификации и аутентификации.

Идентификация основана на назначении каждому пользователю (группе пользователей) сети определенного отличительного признака — идентификатора, и его сравнении с утвержденным перечнем. Однако только заявленный идентификатор в сети не может обеспечить защиту от несанкционированного подключения без проверки личности пользователя.

Процесс проверки личности пользователя получил название аутентификации. Он происходит с помощью предъявляемого пользователем особого отличительного признака — аутентификатора, присущего именно ему. Эффективность аутентификации определяется прежде всего отличительными особенностями каждого пользователя.

Конкретные механизмы идентификации и аутентификации в сети могут быть реализованы на основе следующих средств и процедур защиты информации:

- паролей;
- средств биометрии;
- интеллектуальных карт;
- прекращения доступа пользователя в сеть после нескольких ошибок при регистрации, блокировке компьютера (клавиатуры) или автоматизированного рабочего места с помощью пароля;
- криптография с уникальными ключами для каждого пользователя.

В качестве таких особенностей пользователей вследствие максимальной простоты реализации чаще всего используются пароли. Однако пользовате-

ли, как правило, стараются создавать для себя легко запоминаемые пароли, а значит, и легкие для их угадывания. С другой стороны, создание сложных паролей приводит к необходимости их записи в открытом виде. В случае использования только парольной защиты принимаются надлежащие меры по обеспечению управления созданием паролей, их хранением, слежением за истечением срока их использования и своевременным удалением. Криптографическое закрытие паролей позволяет в значительной степени решить эту проблему и затруднить злоумышленнику преодоление механизма аутентификации.

До настоящего времени единственным средством защиты компьютерной сети от несанкционированного доступа являлась парольная система. При стандартной процедуре входа в сеть каждый пользователь должен знать свое сетевое имя и сетевой пароль. В связи с этим администратор, назначающий эти атрибуты, как правило, не применяет случайных или плохо запоминаемых последовательностей символов, поскольку это может привести к тому, что сетевое имя и пароль могут быть записаны на какой-либо носитель (бумагу, дискету и т. п.) и может произойти утечка секретного пароля и имени пользователя.

Наиболее действенным способом, делающим вход в сеть более корректным (по соображениям защиты от несанкционированного доступа), является возможность избавления пользователя от обязанности запоминания перечисленных выше атрибутов. Имя и пароль могут быть записаны в память специального носителя информации — ключа-идентификатора, в качестве которого используются, например, интеллектуальные (микропроцессорные) карты. В процессе запуска или работы защищаемое программное приложение проверяет этот особый ключ, сверяя его с эталонным. В случае совпадения ключей программа функционирует в заданном режиме, если нет — прекращается выполнение операций в программе.

Несколько лет тому назад в качестве особого ключа защиты использовались некопируемая ключевая дискета или уникальные характеристики компьютера.

Сегодня для этих целей применяются более современные и удобные устройства — электронные ключи, позволяющие решать задачи обеспечения информационной безопасности на любом программно-аппаратном уровне. При этом электронные ключи могут иметь различные характеристики, содержать перезаписываемую энергонезависимую память (EEPROM) и генерировать защитную функцию F(x). Встроенная в программу система защиты получает через ключ информацию, которая используется для аутентификации пользователя и определения набора доступных функций.

Использование электронных ключей для защиты программ и данных имеет ряд достоинств:

- программа или база данных привязана не к компьютеру, а к ключу, через который пользователь получает доступ к данным;
- при запуске защищенная программа проверяется на наличие вирусов и несанкционированных изменений;

- в процессе работы пользователи имеют возможность получать новые версии программ при перепрограммировании ключей соответствующими администраторами.

Важнейшей частью системы защиты с использованием электронных ключей является ее программная компонента. Как правило, она включает в себя:

- защитный «конверт» *(Envelope)*;
- библиотечные функции обращения к ключу API (*Applications Program Interface*).

Каждый из этих способов обеспечения безопасности имеет свое назначение, но в идеале они должны применяться совместно. Системы автоматической защиты (рис. 4.7) предназначены для защиты уже готовых приложений без вмешательства в исходный код программы. Таким образом обеспечивается сохранность COM, EXE-файлов, библиотеки DLL. Для встраивания дополнительного модуля внутрь используется «вирусная» технология вживления и перехвата на себя управления после загрузки.

При использовании «конверта» тело программы шифруется, в нее встраивается дополнительный модуль, который в момент запуска перехватывает управление на себя. После отработки специальных антиотладочных и антитрассировочных механизмов выполняются следующие действия:

- проверка наличия «своего» электронного ключа и считывание из него требуемых параметров;
- анализ «ключевых» условий и выработка решения.

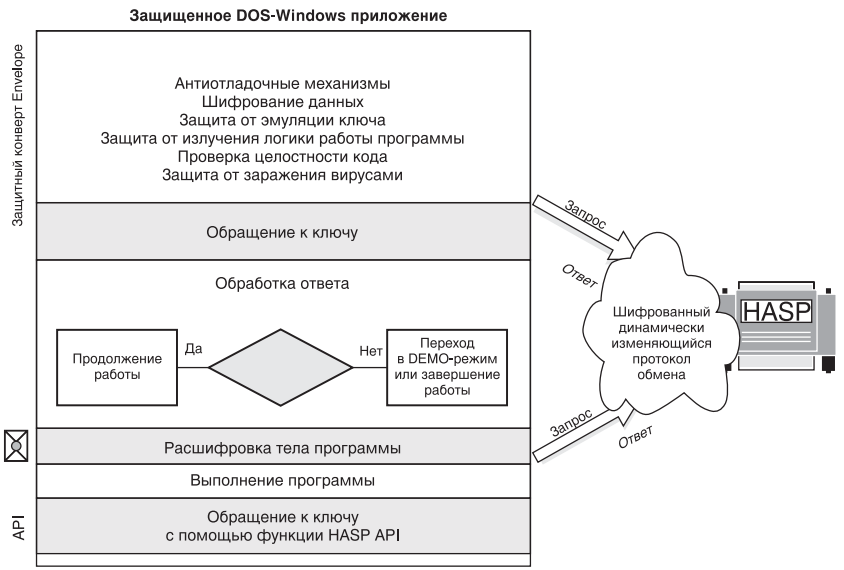


Рис. 4.7. Схема системы автоматической защиты

Для защиты от аппаратной или программной эмуляции обмен между «конвертом» и электронном ключом выполняется с использованием зашумленного изменяющегося во времени («плавающего») протокола.

Некоторые типы «конвертов» обеспечивают фоновые проверки ключа в процессе работы приложения, так что перенести ключ на другой компьютер после того, как защищенная программа запущена, невозможно.

Функции API предназначены для выполнения низкоуровневых операций с ключом, простейшая из которых — проверка наличия ключа. Более сложные функции могут посылать ключу различные входные коды и получать от него ответные, которые затем поверяются на соответствие установленным значениям. Они также могут использоваться в каких-либо вычислительных операциях или при декодировании данных. Программа может осуществлять вызовы обращения к ключу из различных мест, а результаты могут быть разбросаны по телу программы и хорошо замаскированы.

Библиотеки функций API поставляются совместно с электронными ключами HASP (*Hardware Adainst Software Piracy*) для различных языков программирования, компиляторов и т. п.

В последнее время особую важность приобретает не столько защита кода программного продукта, сколько конфиденциальность содержащихся в нем данных (информационного наполнения).

Для защиты от несанкционированного доступа к программам и данным широко используются криптографические системы защиты. Одной из популярных систем защиты программ и данных является Professional ToolKit компании Aladdin Software Security. Эта система позволяет защищать практически любые файлы данных — графические, текстовые, электронные таблицы и т.п. методом прозрачного шифрования, которое осуществляется в среде Windows 95 с помощью электронных ключей HASP — алгоритмы кодирования/декодирования IDEA (*International Data Encryption Algorithm*), длина ключа — 128 бит.

Система не имеет ограничений по количеству открытых файлов и приложений, работающих с защищенной информацией. Внутренние процедуры шифрования драйвера используют данные, содержащиеся в памяти ключа HASP (рис. 4.8), поэтому доступ к зашифрованным файлам без него невозможен. Система поддерживает электронные ключи типа MemoHASP, TimeHASP и NetHASP, причем каждый экземпляр системы работает с одной серией ключей.

«Интеллектуальные» и физические возможности ключа в основном определяются базой, на которой он собран. Сердцем ключа HASP является «заказной» ASIC-чип (*Application Specific Integrated*), логику его функционирования практически невозможно реализовать с помощью стандартных наборов микросхем.

Ключ HASP позволяет использовать функцию Y=F(X), где X — посылаемое в ключ целое число в диапазоне от 0 до 65535, а Y — возвращаемые ключом четыре целых числа из того же диапазона, уникальных для каждой серии.

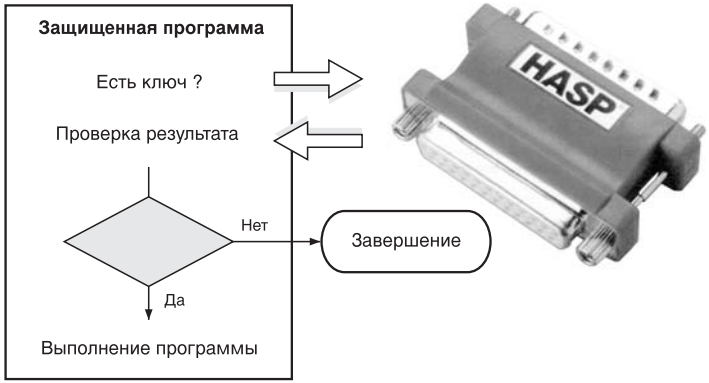


Рис. 4.8. Электронный ключ HASP

Использование механизма генерации чисел качественно усложняет задачу взлома, так как ключевая информация (пароли, шифровальные ключи, часть самого кода и т. п.) не хранится ни в теле программы, ни в памяти ключа ни в открытом, ни в зашифрованном виде.

Существует несколько модификаций ключей HASP:

- MemoHASP — ключ с внутренней энергонезависимой памятью до 4 Кбит, доступной для чтения и записи. Подключается к параллельному порту;
- TimeHASP — содержит встроенные часы с автономным питанием и память до 496 байт. Может использоваться для подготовки учебной или демонстрационной версии программы (ограниченный срок работы), для сдачи программы в аренду или в лизинг для периодического сбора абонентской платы;
- MacHASP — микропроцессорные ключи для защиты приложений под *Macintosh;*
- NetHASP — ключ для защиты сетевых приложений. Предотвращает не только нелегальное тиражирование сетевых программ, но и позволяет контролировать и ограничивать количество пользователей, одновременно работающих с защищенной программой в сети;
- HASP-Card — специальная плата, встраиваемая в стандартный слот компьютера, функционирует как дополнительный свободный параллельный порт. К ней может быть подключено несколько ключей HASP или ключей других типов;
- OpenHASP — микропроцессорные ключи с памятью. Предназначены для защиты платформонезависимых приложений, функционирующих на рабочих станциях;
- PC-CardASP — модификация ключей HASP для компьютеров типа notebook.

Персональные компьютеры и микропроцессорные смарт-карты (*smart-card*) до недавнего времени имели не так уж много точек соприкосновения, так как развивались как бы в разных плоскостях. Что же касается микропроцессорных карт как таковых, то традиционно сфера их применения ограничивалась финансово-банковской и сервисной деятельностью.

Характерной особенностью таких карт является встроенный недорогой, но достаточно производительный микропроцессор. В итоге появляются возможности реализации на уровне пластиковой карты оперативных вычислений, обеспечения надлежащего уровня конфиденциальности и сохранности данных в блоках памяти, а также применения аппаратных методов шифрования. На одной и той же карте может быть реализовано сразу несколько ключей (полномочий пользователя) к различным системным или сетевым ресурсам (рис. 4.9), причем в каждом случае речь будет идти о соответствующих персональных идентификационных номерах.

Надежный контроль доступа и операций, совершаемых с различных рабочих мест, — проблема, весьма остро ощущаемая во многих областях и особенно в открытых компьютерных сетях. В идеале для защиты последних и успешного и безопасного взаимодействия в рамках открытой сети лучше всего подходит реализация алгоритма шифрования данных с открытым ключом. Такие алгоритмы обеспечивают высокий уровень защиты передаваемых сообщений. При этом не представляет сложности процесс первичной генерации секретных ключей, а кроме того, не нужно ломать голову над тем, как безопасным способом сообщить свой секретный ключ другой стороне. Все участники сетевого общения, принявшие данный стандарт передачи сообщений, имеют возможность использовать его где и когда угодно, не боясь раскрытия каких-либо секретов.

В рамках такой технологии смарт-карта может выполнять роль криптопроцессора, генерирующего ключи, и применять самые различные алгоритмы шифрования — DES, «тройной DES», PGP, ГОСТ 28147-89 и т. п.

Кроме смарт-карт в качестве персонального идентификатора в системах ограничения доступа используются электронные карты Touch Memory — специализированные высоконадежные приборы производства фирмы Dallas Semiconductor Inc. (США). Они представляют собой микросхему, размещенную в прочном корпусе из нержавеющей стали, по размерам и форме напоминающем элемент питания от электронных часов (рис. 4.10).

Рис. 4.9. Многоцелевая смарт-карта

Вход на рабочие станции и в локальные вычислительные сети осуществляется при касании считывающего устройства зарегистрированной электронной карточкой Touch Memory и ввода с нее пароля и имени пользователя. В памяти Touch Memory, применяющейся для входа в сеть, записано 64 симво-

Рис. 4.10. Электронная карта Touch Memory

ла сетевого имени и 64 символа сетевого пароля. Эти значения генерируются датчиком псевдослучайных чисел, зашифровываются и записываются в Touch Memory, оставаясь неизвестными даже пользователю. Корректность выполнения процедуры регистрации пользователя в сети обеспечивается передачей управления стандартным сетевым средствам после аутентификации пользователя. Для обеспечения более жесткого контроля входа в сеть пользователь, кроме применения электронной карты, вводит личный секретный пароль.

В последнее время все больше возрастает интерес к биометрическим системам идентификации пользователей компьютерных систем. Технологии идентификации обладают практически неограниченной сферой применения. Правительственные и частные организации заинтересованы в технологиях распознавания лиц, поскольку это позволяет повысить уровень защиты секретной и конфиденциальной информации. Компании, работающие в области информационных технологий, заинтересованы в технологиях распознавания отпечатков пальцев, лиц, голоса, радужной оболочки глаза и т. п., чтобы предотвратить проникновение посторонних в их сети. По мнению президента Microsoft Билла Гейтса: «Биометрия в ближайшем будущем обязательно станет важнейшей частью информационных технологий... Технологии идентификации голоса, лица и отпечатков пальцев будут наиболее важными инновационными технологиями в ближайшие несколько лет».

Но уже и сейчас в компьютерных сетях есть сайты, доступ к которым регламентируется методами дактилоскопии, например разработанные компанией Biometric Trancking. Совсем недавно разработана программа, которая снимает отпечатки пальцев клиента при помощи небольшого устройства. Будучи подключенной к браузеру Netscape Navigator, программа начинает функционировать только в том случае, если сайт, на который пытаются войти, требует дактилоскопии посетителя. Это средство предназначено для повышения мер

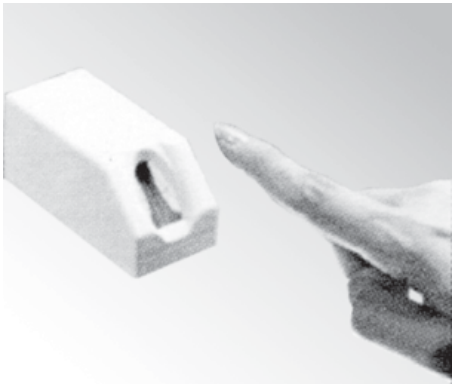


Рис. 4.11. Устройство идентификации по отпечатку пальца

безопасности, совместно с паролями, электронными карточками и т. п. Для непосредственного ввода данных об отпечатках пальцев используется специальный сканер TouchSafe II, изготовленный компанией Identix. Подключается этот сканер к ПК через контроллер, сажаемый на стандартную шину ISA.

Устройство обработки изображения, предназначенное для идентификации отпечатков пальцев FIU (*Fingerprint Identification Unit*) корпорации Sony, например, включает в себя собственный микропроцессор и память, выполняющие полную обработку изображений (рис. 4.11). Это устройство подключается к ПК через последовательный порт и может хранить в памяти до 1000 отпечатков пальцев.

Для идентификации пользователей используется и «интеллектуальное перо» — SmartPen — действительно пишущая шариковая ручка, снабженная сенсорами и крошечным радиопередатчиком, выпускаемая компанией LCI Computer Group (Дания). Ее важным достоинством является то, что она может писать на обычной бумаге, а не на специальной поверхности. Пользователь, к примеру, ставит свою подпись, а ручка снимает детальные динамические биометрические показатели, набор которых уникален для каждого человека, и передает их на компьютер. На головном компьютере может храниться база данных с «профилями рук» множества пользователей. В процессе письма на плоской поверхности ручка совершает движения в трехмерном пространстве. В третьем измерении, в котором ручка давит на бумагу, фиксируются микроперемещения.

В действительности комплект оборудования SmartPen — это весьма сложный технический комплекс. Ручка содержит микромышь, снабженную датчиками для снятия параметров трехмерной траектории, сигнальный процессор для обработки полученных данных, приемопередатчик и даже систему криптографической защиты, для того чтобы предотвратить перехват данных, передаваемых по радиоканалу.

Для идентификации изображений компания Visionics представляет пакет FaceltPC. Программа сравнивает основные черты лица, полученные при обработке трехмерного изображения, причем изменение прически, например, не влияет на результаты идентификации. Такой метод биометрии позволяет достичь более высокого уровня защищенности в отличие от обычных систем типа login/password. Системы, основанные на распознавании образов, практически невозможно обмануть. Например, нельзя подсунуть системе фотографию пользователя, так как для обработки используется трехмерное изображение.

Все чаще для защиты от несанкционированного доступа стали использоваться программно-аппаратные комплексы, которыми могут оснащаться рабочие станции компьютерной сети и автономные компьютеры. В качестве примера рассмотрим комплексы защиты типа DALLAS LOCK.

Комплекс защиты DALLAS LOCK предназначен для исключения несанкционированного доступа к ресурсам компьютера и разграничения полномочий пользователей, а также для повышения надежности защиты входа в локальную сеть. Для идентификации пользователей используются электронные карты Touch Memory и личные пароли.

Программно-аппаратный комплекс DALLAS LOCK for Administrator предназначен для работы в вычислительных сетях совместно с комплексом DALLAS LOCK и представляет собой автоматизированное рабочее место администратора безопасности. Все модификации комплекса DALLAS LOCK возможно применять для защиты бездисковых рабочих станций локальной вычислительной сети. Эти комплексы могут использоваться с различными операционными системами.

Запрос идентификатора при входе на ПК инициируется из ПЗУ на плате защиты до загрузки операционной системы. Загрузка операционной системы с жесткого диска осуществляется только после предъявления зарегистрированного идентификатора (электронной карты) и вводе личного пароля. Поскольку идентификатор и пароль запрашиваются до обращения к дисководам, возможность загрузки с системной дискеты полностью исключается.

При инсталляции комплекса на жесткий диск обеспечивается гибкая настройка аппаратной части путем предварительного выбора адресного пространства ПЗУ платы защиты в свободной области адресов пользовательского BIOS, а также номера порта для работы с картой.

Поддерживается работа до 32 зарегистрированных пользователей на каждом компьютере, причем каждый из них может быть зарегистрирован на нескольких ПК с разными полномочиями. Данные о пользователях хранятся в энергонезависимой памяти на плате защиты.

Энергонезависимая память платы защиты содержит образ системных областей компьютера, что позволяет контролировать их целостность.

Разграничение доступа пользователей возможно как по отношению к внешним устройствам (дисководам, LPT и COM портам), логическим дискам «винчестера» и таймеру, так и по времени работы на компьютере. Для каждого пользователя могут быть назначены свои права и уровни доступа к:

- системному диску C: (полный доступ; только для чтения);
- остальным логическим дискам «винчестера» (полный доступ; нет доступа; только для чтения);
- дисководам A: и B: (полный доступ; нет доступа; только для чтения);
- LPT и COM портам: (полный доступ; нет доступа).

Время начала и окончания работы каждого пользователя на компьютере устанавливается администратором в пределах суток. Интервал времени, в те-

чение которого пользователь может работать на компьютере со своими правами, может быть установлен от 1 мин до 23 ч 59 мин (т. е. круглосуточно). Для предупреждения пользователя об истечении отведенного времени работы предусмотрен режим «будильника». За 5 мин до окончания сеанса работы пользователя выдается прерывистый звуковой сигнал. В пределах оставшихся 5 мин пользователь сможет закончить работу, после чего компьютер будет заблокирован. Предусмотрен режим защиты таймера от изменения системного времени.

При регистрации идентификатора комплекс создает для каждого пользователя индивидуальный файл AUTOEXEC, который будет выполняться после загрузки компьютера пользователем с данной картой.

При выполнении процедуры входа на компьютер комплекс анализирует электронную карту и личный пароль пользователя. При этом в электронном журнале фиксируются номер предъявленной карты, имя пользователя, дата и время попытки «входа» и результат попытки (проход — отказ в доступе), а также причина отказа в загрузке компьютера в случае неудачи. В электронных журналах фиксируются действия пользователей по работе с файлами на дисках. Электронные журналы доступны только администратору. Пользователи могут самостоятельно менять личные пароли для входа на компьютер и для доступа к индивидуальным зашифрованным дискам «винчестера».

Для усиления защиты информации на компьютере администратор может для всех или отдельных пользователей включать режим принудительной смены пароля входа. Пользователь будет вынужден сменить пароль входа после загрузки компьютера установленного числа раз.

Доступ к электронным журналам рабочих станций администратор безопасности получает на своем рабочем месте. Для передачи данных используются протоколы IPX, что позволяет размещать защищенные станции в различных сегментах (рис. 4.12).

Со своего рабочего места администратор получает список активных станций в сети, выбирает любую из них и запрашивает любой из журналов. После установления соединения журнал автоматически переписывается на диск компьютера администратора и обнуляется на рабочей станции. Данные из журналов могут быть выведены в файл или на печать. В случае необходимости оперативного получения информации о событиях, происходящих на рабочей станции, администратор безопасности может негласно просматривать содержание ее экрана. Ему предоставляется возможность установить для любого пользователя режим полного стирания информации из памяти и с носителей при удалении файлов.

Комплекс DALLAS LOCK может быть установлен на любой IBM-совместимый компьютер, работающий автономно или в качестве рабочей станции локальной вычислительной сети. Для размещения файлов и работы комплекса требуется до 3 Мб пространства на системном разделе C: жесткого диска. ПЗУ платы защиты занимает 8 Кб в области памяти пользовательских BIOS.

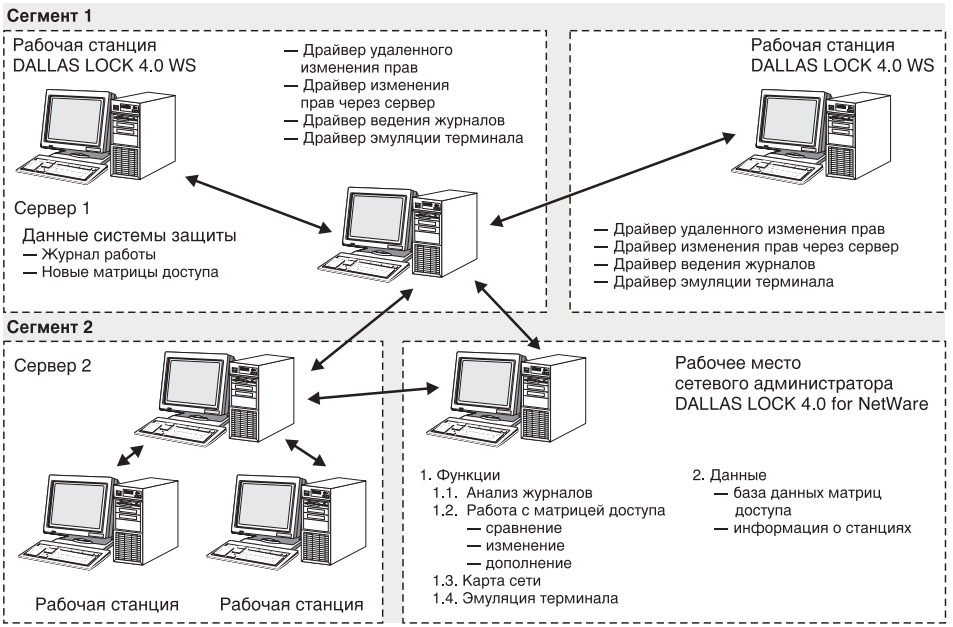


Рис. 4.12. Организация взаимодействия комплексов

Для создания на «винчестере» дополнительных зашифрованных индивидуальных дисков каждому пользователю на системном разделе C: необходимо предусмотреть пространство, равное суммарной емкости этих дисков. Максимальный объем каждого диска — 32 Мб.

4.2. Компьютерные вирусы

Большую угрозу безопасности компьютерных систем доставляют вирусы. Компьютерным вирусом будем называть программу, обладающую способностью к скрытому размножению в среде стандартной операционной системы компьютера путем включения в исполняемые или хранящиеся программы своей, возможно модифицированной копии, которая сохраняет способность к дальнейшему размножению. Условно компьютерные вирусы подразделяются на классы (рис. 4.13). Эта классификация объединяет, естественно, далеко не все возможные вирусы; в каждой категории встречаются варианты, не названные в силу их экзотичности.

Свойство размножения вирусов само по себе в принципе не представляет опасности и может привести в основном к заполнению пространства свободной памяти, увеличению длин хранящихся файлов и замедлению процесса выполнения программ.

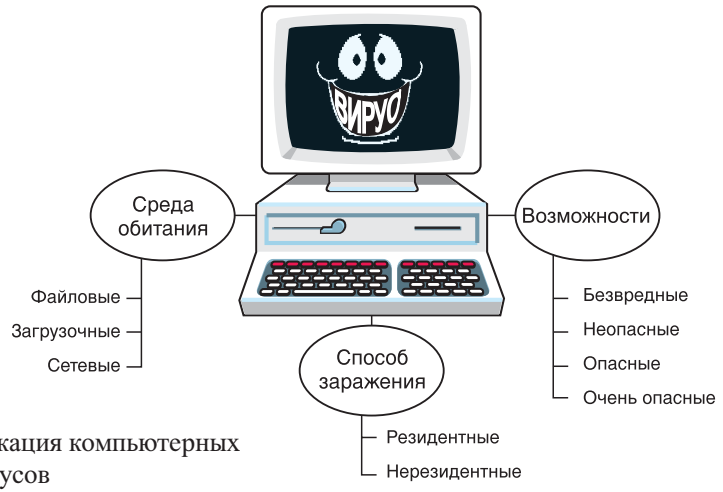


Рис. 4.13. Классификация компьютерных вирусов

Но если подобный вирус начнет размножаться по сети, то в один прекрасный день эта сеть может быть полностью заблокирована. Например, в середине января 1999 г. в сети Internet был обнаружен компьютерный червь, получивший прозвище Happy 99.exe. Он не пытается разрушать файлы на зараженных машинах, зато без ведома жертвы рассылает электронные письма и объявления для телеконференций и способен не только снизить производительность сети, но даже вывести из строя корпоративный сервер электронной почты.

От опасного вируса CIH («Чернобыль»), который активировался 26 апреля 1999 г., в день тринадцатой годовщины катастрофы на Чернобыльской АЭС, пострадало более 100 тысяч компьютеров только в России. По прогнозам Е. Касперского, руководителя антивирусного центра «Лаборатория Касперского», основные причины распространения вируса — нелегальное зараженное программное обеспечение. Жизненный цикл компьютерного вируса может включать следующие этапы:

- внедрение (инфицирование);
- инкубационный период;
- саморазмножение (репродуцирование);
- выполнение специальных функций;
- проявление.

Данные этапы не являются обязательными и могут иметь другую последовательность. Особую опасность представляет этап выполнения специальных функций, которые могут привести к катастрофическим последствиям для пользователей компьютеров.

Компьютерные вирусы могут неограниченное время храниться на дискетах и жестких дисках, а затем случайно или умышленно заразить (инфицировать) компьютер при использовании зараженных файлов.

Вирус заражает компьютер только при выполнении зараженной программы. Но если он сам заражен, то практически любая операция на машине может привести к заражению программы и файлов, находящихся в памяти и на дискетах, вставленных в приемное устройство. При наличии программы с телом вируса в памяти компьютера могут заражаться выполняемые программы, программы, хранящиеся на жестком диске и дискетах, а также файлы на дискетах при просмотре их каталогов, т. е. происходит этап внедрения вируса. Копия вируса вставляется в зараженную программу таким образом, чтобы при запуске на выполнение зараженной программы вирус получил управление первым. Первым и обязательным действием вируса при выполнении инфицированной программы является этап саморазмножения. Этот этап может осуществляться вплоть до уничтожения вирусоносителя. Одновременно с внедрением или после определенного промежутка времени, определенного количества внедренных копий и т. д. вирус приступает к выполнению специальных функций. Последние, именуемые еще «логическими бомбами», вводятся в программное обеспечение и срабатывают только при выполнении определенных условий, например по совокупности даты и времени и т. п., и частично или полностью выводят из строя компьютерную систему.

Не следует думать, что «логические бомбы» — это экзотика, несвойственная нашему обществу. Разновидность «логической бомбы», которая срабатывает по достижении определенного момента времени, получила названия «временной бомбы», она «взрывается» в самый неожиданный момент, разрушая всю библиотеку данных.

Кроме того, часть компьютерных вирусов имеет фазу проявления, которая сопровождается визуальными или звуковыми эффектами. Отдельные вирусы сообщают пользователю о заражении компьютера.

Существует способ внедрения в чужое программное обеспечение, именуемый как «троянский конь», который заключается в тайном введении в атакуемую программу таких команд, что позволяют осуществлять новые, не планируемые владельцем программы функции, но одновременно сохранять и прежнюю работоспособность. С помощью «троянского коня» преступники, например, отчисляют на свой счет определенную сумму с каждой банковской операции. В США, например, получила распространение форма компьютерного вандализма, при которой «троянский конь» разрушает через какой-то промежуток времени все программы, хранящиеся в памяти компьютера.

Компьютерные программные тексты обычно чрезвычайно сложны. Они состоят из сотен, тысяч, а иногда и миллионов команд. Поэтому «троянский конь» из нескольких десятков команд вряд ли может быть обнаружен, если, конечно, нет подозрений относительно этого. Но и в последнем случае экспертам-программистам потребуется много дней и недель, чтобы найти его.

Есть еще одна разновидность «троянского коня». Ее особенность состоит в том, что в безобидно выглядящий кусок программы вставляются не команды, собственно выполняющие «грязную» разрушительную работу, а команды, формирующие и после выполнения уничтожающие их. В этом случае про-

граммисту, пытающемуся найти «троянского коня», необходимо искать не его самого, а команды, его формирующие. Развивая эту идею, можно представить себе команды, которые создают другие команды и т. д. (сколь угодно большое число раз), а в итоге создающие «троянского коня».

Современная техническая литература, посвященная проблемам компьютерных вирусов, изобилует различными терминами, заимствованными из других отраслей науки и научно-фантастических книг, поэтому очень часто одни и те же вирусы имеют разное название.

Все известные вирусы можно разделить на классы по следующим признакам:

- среда обитания вируса;
- способ заражения среды обитания;
- деструктивная возможность;
- особенности алгоритма вируса.

По среде обитания компьютерные вирусы можно разделить на сетевые, файловые и загрузочные. Сетевые вирусы распространяются по компьютерной сети, файловые внедряются в выполняемые файлы, загрузочные — в загрузочный сектор диска (boot-сектор) или в сектор, содержащий системный загрузчик винчестера (*Master Boot Record*). Кроме того, существуют и их сочетания — например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные сектора дисков. Такие вирусы, как правило, имеют довольно сложный алгоритм работы, часто применяют оригинальные методы проникновения в систему.

Вирусы могут размещаться в:

- операционной системе, где они «сцепляются» с программами, расположенными в системной части дискеты или жесткого диска;
- библиотеках компиляторов для внедрения в программы, составляемые компиляторами;
- сетевых драйверах;
- «плохих» или специальных секторах жесткого диска;
- ПЗУ в качестве программно-технической закладки;
- структуре исполняемых программ или файловых программ.

Способ заражения среды обитания подразделяется на резидентный и нерезидентный. Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращение операционной системы к объектам заражения и внедряется в них. Происходит это следующим образом. Резидентный вирус запрашивает у системы участок памяти и копирует себя в него. Он перехватывает прерывания, анализирует их и обеспечивает тем самым управление процессором компьютера. Если следующим этапом жизненного цикла вируса является инкубационный период, то вирус никак не проявляет себя в течение определенного промежутка времени или определенного количества подходящих объектов для заражения. После этого наступает этап размножения. Обнаружив обращение к определенным компонентам системы, которые пригодны для заражения, вирус активизирует процедуру копирования. Обычно эта процедура проверяет, не присутствует ли уже

в объекте заражения копия вируса, если копия уже присутствует, т. е. объект уже заражен, отдельные вирусы проверяют номер версии и заражают объект, если их версия более новая. Если копии вируса нет, то он копируется из памяти в заражаемый объект с модификацией его первой команды. Объектами заражения в этом случае могут быть исполняемые программы, программы на жестком диске и дискетах. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера.

Нерезидентные (транзитные) вирусы не заражают память компьютера и являются активными ограниченное время. Некоторые вирусы оставляют в оперативной памяти небольшие резидентные программы, не распространяющие вирус. Такие вирусы тоже считаются нерезидентными.

Транзитные вирусы не остаются в памяти после выполнения зараженной программы. В этом случае вирус перед передачей управления исходной программе ищет файл, пригодный для внедрения и еще не зараженный. Этап выполнения специальных функций в этом случае не всегда следует за этапом саморазмножения, чтобы успеть создать достаточное количество своих копий, прежде чем факт заражения будет обнаружен пользователем. Поэтому механизм выполнения специальных функций включается достаточно редко и вредные последствия вируса могут быть незаметны. Когда же пользователь заметит изменения в работе компьютера, может оказаться, что вирусом поражены практически все файлы системы.

По деструктивной возможности, т. е. по степени разрушения, вирусы можно разделить на:

- безвредные;
- неопасные;
- опасные;
- очень опасные.

Безвредные вирусы, кроме уменьшения свободной памяти на диске в результате своего распространения, никак больше не влияют на работу компьютера.

Влияние неопасных вирусов ограничивается также уменьшением свободной памяти на диске и дополнительно графическими, звуковыми и другими эффектами.

Опасные вирусы приводят к серьезным сбоям в работе компьютера.

Очень опасные вирусы приводят к потере программ, уничтожению данных, стиранию необходимой для работы компьютера информации, записанной в системных областях памяти. Особо опасными являются вирусы, прикрепляемые к объектной библиотеке какого-либо компилятора. Такой вирус автоматически внедряется в любую программу, работающую с инфицированной библиотекой.

Известные в настоящее время вирусы могут выполнять следующие специальные разрушительные функции:

- изменение данных в файлах;
- изменение данных, передаваемых через параллельные и последовательные порты;

- изменение назначенного диска (запись информации производится не на диск, указанный пользователем, а на указанный вирусом);
- переименование файлов (не сообщая об этом пользователю);
- форматирование отдельных частей жесткого диска (дискеты) или даже всего диска (дискеты);
- уничтожение каталога диска;
- нарушение работоспособности операционной системы, когда она не воспринимает внешних воздействий пользователя и требует перегрузки;
- снижение производительности в результате постоянного выполнения «ложных» программ;
- отказ в выполнении определенной функции (например, блокировка клавиатуры, блокировка загрузки программы с защищенной от записи дискеты и т. д.);
- стирание выводимой на экран дисплея информации и т. п. Очень опасными являются «мелкие» повреждения данных (например, замена первых байтов каждого блока при записи, замена отдельных символов и т. д.), которые долго могут быть не обнаруживаемы пользователем.

Перечень специальных функций, выполняемых вирусами, практически пополняется с каждым новым видом вируса. Исследователи отмечают множество разных видов вирусов, различающихся механизмами размножения и выполняемыми специальными функциями. Среди этих видов существует много вариаций (штампов), которые являются, как правило, результатом усовершенствования одним программистом вируса, созданного другим. Обычно легче модифицировать чужую программу, чем создать оригинальную собственную.

Но даже если в алгоритме вируса не найдено ветвей, наносящих ущерб системе, этот вирус нельзя с полной уверенностью назвать безвредным, так как проникновение его в компьютер может вызвать непредсказуемые, а порой и катастрофические последствия. Ведь вирус, как и всякая программа, имеет ошибки, в результате которых могут быть испорчены как файлы, так и сектора дисков. Возможно также «заклинивание» резидентного вируса и системы при использовании новых версий DOS, при работе в Windows или с другими мощными программными системами.

По особенностям алгоритма функционирования вирусов их можно подразделить на следующие группы:

- компаньон-вирусы (companion);
- вирусы-«черви» (worm);
- паразитические;
- студенческие;
- stealth-вирусы (вирусы-невидимки);
- полиморфик-вирусы (polymorphic).

Компаньон-вирусы (companion) представляют собой программы, не изменяющие файлы. Алгоритм работы этих вирусов состоит в том, что они создают

для EXE-файлов, находящихся в памяти компьютера, файлы-спутники, имеющие то же самое имя, но с расширением .COM: например, для файла XCOPY.EXE создается файл XCOPY.COM. Вирус записывается в COM-файл и никак не изменяет EXE-файл. При запуске такого файла DOS первым обнаружит и выполнит COM-файл, т. е. вирус, который затем запустит и EXE-файл.

Вирусы-«черви» распространяются в компьютерных сетях и так же, как и компаньон-вирусы, не изменяют файлы или сектора на дисках. Они проникают в память компьютера из компьютерной сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Такие вирусы иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

Паразитические вирусы при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов. К этой группе относятся все вирусы, которые не являются вирусами-«червями» или компаньон-вирусами.

Студенческие — это крайне примитивные вирусы, часто нерезидентные и содержащие большое количество ошибок.

Stealth-вирусы, или вирусы-невидимки, представляют собой весьма совершенные программы, которые перехватывают обращения DOS к пораженным файлам или секторам дисков и «подставляют» вместо себя незараженные участки информации. Кроме этого, такие вирусы при обращении к файлам используют достаточно оригинальные алгоритмы, позволяющие обманывать резидентные антивирусные мониторы.

«Полиморфик»-вирусы — это достаточно трудно обнаруживаемые вирусы, не имеющие сигнатур, т. е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфик-вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика. Некоторые вирусы (например, вирусы семейства «Eddie», «Murphy») используют часть функций полноценного вируса-невидимки. Чаще всего они перехватывают функции DOS FindFirst и FindNext и «уменьшают» размер зараженных файлов. Такой вирус невозможно определить по изменению размеров файлов, если, конечно, он резидентно находится в памяти. Программы, которые не используют указанные функции DOS (например, Norton Commander), а напрямую используют содержимое секторов, хранящих каталог, показывают правильную длину зараженных файлов.

При инфицировании файла вирус может производить ряд действий, маскирующих и ускоряющих его распространение. К подобным действиям можно отнести обработку атрибута read-only, снятие его перед заражением с последующим восстановлением. Многие файловые вирусы считывают дату последней модификации файла и восстанавливают ее после заражения. Для маскировки своего распространения некоторые вирусы перехватывают прерывание DOS, возникающее при обращении к защищенному от записи диску, и самостоятельно обрабатывают его. Поэтому к особенностям алгоритма файлового вируса можно отнести и наличие или отсутствие обработки, и

скорость его распространения. Скорость распространения файловых вирусов, заражающих файлы только при их запуске на выполнение, будет ниже, чем у вирусов, заражающих файлы и при их открытии, переименовании, изменении атрибутов файла и т. д. Некоторые вирусы при создании своей копии в оперативной памяти компьютера пытаются занять область памяти с самыми старшими адресами, разрушая временную часть командного интерпретатора COMMAND.COM. По окончании работы зараженной программы временная часть интерпретатора восстанавливается, при этом происходит открытие файла COMMAND.COM и, если вирус заражает файлы при их открытии, его заражение. Таким образом, при запуске подобного вируса первым будет заражен файл COMMAND.COM.

Защита от вирусов

Для защиты от вирусов обычно используются:

- общие средства защиты информации, которые полезны так же, как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователей;
- профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
- специализированные программы для защиты от вирусов.

К сожалению, количество вирусов и их штаммов быстро увеличивается и характер борьбы может зависеть от вида вируса и его характеристик. В настоящее время для защиты компьютеров и сетей от вирусов имеется достаточное количество программных средств защиты, которые обычно называют антивирусными.

Среди многообразия антивирусных программ можно выделить, например, три основных вида:

- предупреждающие (фильтры);
- обнаруживающие (детекторы);
- опознающие (доктора).

Предупреждающие (предотвращающие) программы находятся резидентно в памяти все время. Эти программы фильтруют доступ к файлам (чтение и запись), разрешенный другим программам. Они контролируют загрузку программ в память и проверяют работу всех обслуживающих программ операционной системы (системные таблицы, управляющие структуры и т. д.). При попытке доступа вируса к одной из выполняемых программ предупреждающая заражение программа «замораживает» систему, не давая вирусу инфицировать выполняемую программу, и сообщает об этом пользователю.

Работа программ обнаружения заражения основана на том, что вирусная информация может быть обнаружена по следам, оставленным вирусом. Такие программы-детекторы используют один из двух вариантов: вакцинацию защищаемых программ (включая самовакцинацию) через контрольные суммы и

фиксированное состояние памяти («снимок» состояния памяти). Программы-вакцины, или иммунизаторы, модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, против которого производится вакцинация, считает эти программы или диски уже зараженными. В ходе работы пользователя периодически запускаются программы сверки текущего состояния системы с начальным, которые регистрируют всю критическую к заражению информацию системы.

К недостаткам программ-вакцин можно отнести:

- необнаружение заражения, если оно произошло до «вакцинации»;
- большой объем запоминаемой информации (возрастание длины защищаемой программы);
- увеличение времени загрузки защищаемой программы и времени ее выполнения;
- возможность несрабатывания (некоторые вирусы могут обходить известные им программы-вакцины).

Программы слежения за состоянием файловой системы похожи на вакцины и реагируют на попытки заражения файлов. Эти программы запоминают отдельные характеристики файлов (длину, контрольную сумму, дату создания и др.) в отдельных специально создаваемых файлах. При этом длины защищаемых файлов не увеличиваются, и процесс слежения за их состоянием для вируса остается незамеченным. Программы слежения универсальны, так как реагируют на инфицирование любыми вирусами.

К недостаткам программ слежения можно отнести следующие:

- их эффективность зависит от частоты запуска;
- они не в состоянии обнаружить заражение, если оно произошло до запуска программы слежения;
- увеличение затрат процессорного времени.

Программы определения заражения хорошо работают, когда система уже заражена и уже поздно для предупреждения (наличие вируса очевидно). Эти программы ищут специфические символы, которые могут быть в теле программы вируса, во всех частях системы. Когда они находят такие символы, то тем самым определяют вид вируса и уничтожают его, т. е. восстанавливают программу в то состояние, в котором она находилась до заражения вируса, если это возможно. В качестве специфических символов могут использоваться последовательности команд: метки, флаги прерываний, имена файлов и т. п.

Программы-мониторы предназначены для блокирования процесса размножения вирусов и других опасных попыток доступа к винчестеру и дискетам. Они анализируют все запросы на доступ к дискетам и логическим дискам, имеющие отношение к возможной деятельности вирусов, и обеспечивают защиту дисков на уровне работы с файлами (при их создании, открытии, позиционировании, чтению и записи), а также на уровне доступа к секторам по абсолютным адресам и на уровне физической адресации (цилиндр, дорожка, сектор).

Программы-мониторы:

- поднимают тревогу при попытке создать или изменить файлы типа .EXE;
- отслеживают разные события и обладают возможностью перенастройки в процессе работы;
- проверяют законность доступа к файлам на всех уровнях;
- имеется возможность настроить программу на защиту определенных логических частей диска;
- не позволяют вирусам перехватывать прерывания определенного вида и в большинстве случаев успешно подавляют активность размножения вирусов.

Таким образом, программные средства защиты обеспечивают в большой степени обнаружение уже известных видов вирусов и частично их уничтожение. Уменьшить вероятность заражения компьютера вирусом, а также свести к минимуму возможный ущерб от действий вируса, если заражение все же произошло, позволяют некоторые профилактические меры защиты:

- загружайтесь только с использованием винчестера, если его нет — только с защищенной от записи дискеты;
- разделяйте на винчестере логические диски для системных программ, программ общего математического обеспечения и программ пользователей с различными атрибутами доступа;
- периодически архивируйте изменяемые файлы;
- включайте вызов программ-детекторов в командный файл, выполняемый при начальной загрузке;
- периодически используйте программы демонстрации содержимого оперативной памяти и определения состояния векторов прерываний (и им подобных);
- обращайте внимание и поднимайте тревогу при изменениях работоспособности компьютера, например:
  обращения к дискам кажутся чрезмерными при выполнении данной программы;
  стали часто появляться ошибочные сообщения операционной системы;
  программы или файлы исчезли из каталога;
  произошло уменьшение свободного пространства операционной памяти;
  появились визуальные эффекты, свидетельствующие о наличии вируса.

Профилактические меры не могут обеспечить полную гарантию, что заражение вирусом не произойдет по случайной или злоумышленной причине. Поэтому если заражение все же произошло, то необходимо следовать определенной методике работы. Хотя действия, которые необходимо предпринять для удаления вируса и его последствий, вообще говоря, индивидуальны для каждого вируса (или даже штамма), тем не менее опыт специалистов позволяет сформировать методику действий пользователя при обнаружении заражения:

- определить вид вируса и повреждения, нанесенные им;
- выключить зараженный компьютер;
- включить компьютер и загрузиться с защищенной от записи дискеты, убедиться, что загрузка прошла нормально;
- не запускать никаких программ зараженной машины на исполнение;
- скопировать все невыполняемые файлы на заранее подготовленные чистые дискеты, используя утилиты с загрузочной дискеты;
- просмотреть все файлы зараженного диска и составить список выгрузки. Если копии этих файлов есть в архиве на дискетах, то такие файлы можно не выгружать;
- подвергнуть оставшиеся файлы обработке антивирусными программами с защищенной от записи дискеты;
- если какой-либо файл вызывает сомнение, исключить его из списка выгружаемых файлов;
- выгрузить файлы, копий которых нет в архиве (таковыми должны быть только те, которые изменялись после последней выгрузки до момента обнаружения вируса);
- переформатировать зараженный диск и проверить его «чистоту»;
- восстановить операционную систему;
- восстановить директории;
- заменить все выполняемые файлы с архивных (эталонных) дискет;
- определить все дискеты, которые ставились или могли быть поставлены на зараженный компьютер. Подвергнуть их обработке антивирусными средствами;
- проверить работоспособность программного обеспечения, обращая внимание на возможные проявления данного вируса и используя все имеющиеся в наличии антивирусные программы.

При обнаружении заражения бутовым вирусом:

- выключить питание зараженного компьютера;
- загрузиться с защищенной от записи дискеты;
- заменить бутовый сектор на пораженном диске.

Это позволит устранить вирус, но сохранит его в других секторах, которые вирусы обычно указывают как плохие. Сохранение полной емкости диска достигается переформатированием диска. Аналогичные действия произвести с дискетами, зараженными бутовым вирусом.

4.3. Криптографические методы защиты информации

Универсальным и надежным способом защиты информации является ее криптографическое преобразование в форму, непонятную для посторонних. История применения криптографических методов насчитывает десятки веков.

Упоминание о криптографии (от греч. тайнопись) встречается у античных авторов Геродота и Плутарха, а также в русских рукописях XII—XIII вв.

В настоящее время криптографические методы традиционно используются для обеспечения конфиденциальности информации, представленной в любой материальной форме:

- в виде письменных текстов;
- данных, хранящихся на гибком диске;
- сообщений, передаваемых в телекоммуникационных сетях;
- программного обеспечения, графики или речи, закодированных цифровыми последовательностями, и т. п.

Эти методы могут быть использованы и для многих других приложений, связанных с защитой информации, в частности для обнаружения фактов вторжения в телекоммуникационную или компьютерную сеть и введения в нее имитирующих сообщений (нарушение целостности). С помощью криптографических преобразований может быть осуществлена проверка целостности сообщений (установление их подлинности), например цифровой подписи, а также обеспечена целостность данных и программ, хранящихся в памяти. При кодировании для скрытой передачи сообщений используется система условных обозначений элементов информации (заранее выбранных кодов), представляющих сочетание цифр, букв или других символов. Элементы защищаемых сведений (отдельные буквы и цифры, слова, группы слов) и их условные обозначения представляются в виде кодировочных таблиц или книг, которые должны быть у всех участников информационного обмена. Но немного отвлечемся от современного использования криптографии и сделаем экскурс в историю. Рассмотрим лишь небольшой отрезок времени и посмотрим, что и как шифровали в нашем недалеком прошлом.

Шифр — это язык разведчиков, а они обычно вынуждены вести свои разговоры шепотом. Успех разведчика да и сама его жизнь зависят от умения остаться незамеченным. Он использует коды, имеющие вид обычных открытых текстов, невидимые чернила, послания микроскопически малых размеров, т. е. стеганографические методы, которые скрывают сам факт отправки какого-либо сообщения.

После нападения Японии Соединенные Штаты создали орган цензуры, насчитывающий около 15 тысяч сотрудников, которые проверяли ежедневно до миллиона писем, прослушивали бесчисленное множество телефонных разговоров, просматривали кинофильмы, газеты, журналы.

Чтобы перекрыть максимальное количество стеганографических каналов связи, американская цензура категорически запретила отправление по почте целого ряда сообщений. Были отменены шахматные матчи по переписке. Из писем вымарывались кроссворды, так как у цензоров не хватало времени решать их, чтобы проверить, не содержат ли они тайные послания. Не разрешалось посылать по почте табели успеваемости учащихся. Одно письмо с инструкциями по вязанию было задержано до тех пор, пока цензор не связал по ним свитер, чтобы проверить, не содержат ли они какой-либо скрытой информации.

С появлением компьютеров и использованием для связи компьютерных сетей шифрование данных стало еще более изощренным. Современные системы позволяют шифровать сообщения так, что на их раскрытие могут понадобится десятки или даже сотни лет непрерывной работы.

В настоящее время используются различные компьютерные программы для шифрования данных, в которые заложены такие методы шифрования, как DES, RSA, PGP, ГОСТ 28147-89.

Двумя основными методами криптографической защиты являются кодирование и шифрование. Наряду с ними к криптографическим методам относят методы рассечения—разнесения, сжатия—расширения.

Рассечение—разнесение информации заключается в том, что массив защищенных данных делится на такие элементы (части), каждый из которых в отдельности не позволяет раскрыть содержание защищаемой информации. Эти части информации могут передаваться по нескольким источникам, разноситься при передаче по времени или по месту записи на дискете (любом другом запоминающем устройстве).

Сжатие—расширение информации представляет собой замену часто встречающихся одинаковых последовательностей символов некоторыми заранее выбранными символами или же подмешивание дополнительной информации.

Стеганография

Когда в V в. до н.э. тиран Гистий, находясь под надзором царя Дария в Сузах, должен был послать секретное сообщение своему родственнику в анатолийский город Милет, он побрил наголо своего раба и вытатуировал послание на его голове. Когда волосы снова отросли, раб отправился в путь. Так Геродот описывал один из первых случаев применения в древнем мире стеганографии — искусства скрытого письма.

В основе этого искусства лежит попытка скрыть само существование секретного сообщения, а потому его приемы заслуживают самого широкого употребления. Здесь могут быть использованы «подкладочное письмо», когда запись сокрыта какой-либо защитной оболочкой, «хоббийное кодирование» с использованием кроссвордов, музыкальных нот и шахматных партий, «жаргонные шифры», в которых вроде бы невинные слова имеют совершенно другой смысл.

Искусство развивалось, превратившись в науку, помогавшую людям на протяжении многих веков скрывать от посторонних глаз сам факт передачи информации. Еще древние римляне писали между строк невидимыми чернилами, в качестве которых использовались фруктовые соки, моча, молоко и некоторые другие натуральные вещества. Их опыт не был забыт: наверное, многие помнят, как в советских школах детям рассказывали о вожде всех гегемонов, который писал, кажется молоком, между строк обычного письма нечто важное своим соратникам. При нагревании невидимый текст проявлялся. Так что не будь стеганографии, возможно, не было бы и октябрьского переворота.

Во время Второй мировой войны немцами применялась «микроточка», представлявшая собой микрофотографию размером с типографскую точку, которая при увеличении давала четкое изображение печатной страницы стандартного размера. Такая точка или несколько точек вклеивались в обыкновенное письмо и, помимо сложности обнаружения, обладали способностью передавать большие объемы информации, включая чертежи.

Распространение стеганографии во время войны и тотальная шпиономания вызвали появление многих цензурных ограничений, которые сегодня могут вызвать лишь улыбку. В США были запрещены к международной почтовой пересылке шахматные партии, инструкции по вязанию и шитью, вырезки из газет, детские рисунки. Запрещалось посылать телеграммы с указанием доставить определенный сорт цветов к определенной дате, а впоследствии американским и английским правительствами были запрещены вообще все международные телеграммы, касающиеся доставки и заказа цветов.

Ориентирующими примерами данных методик (оставив в стороне возможности, даваемые электроникой) могут служить:

- запись наколом букв в конкретном месте какой-то книги или газеты (концы слов отмечаются при этом наколом между буквами);
- сообщение каких-то данных (набор товаров, оптовые цены) в определенном порядке;
- письмо посредством узелков, где каждая из букв кодируется размером в сантиметрах (А-1 см, Б-2 см...) или в диаметрах мизинца и отмечается отдельным узелком на нитке или на обвязывающем сверток шпагате; читают текст наматывая нитку на палец;
- запись на боковой поверхности колоды карт, подобранных в конкретном порядке (колода после этого тасуется);
- записи на оборотной стороне этикеток флаконов, банок или бутылок;
- текст под наклеенной почтовой маркой;
- запись на внутренней поверхности спичечной коробки, которая для этого разламывается, а после склеивается по новой;
- запись внутри вареного яйца (берут смесь квасцов, чернил и уксуса, записывают ею то, что необходимо, на скорлупе обычного яйца, которое потом выдерживают в крепком рассоле или уксусе, чтобы стравить следы с его поверхности; яйцо затем варят вкрутую, причем весь текст оказывается сверху белка под скорлупой);
- использование «испорченной» пишущей машинки, в которой некоторые буквы ставятся выше или ниже строки (учитывают здесь порядок и количество этих букв, а также промежутки их появления; в коде возможен вариант азбуки Морзе);
- записи от руки нот в нотной тетради (ноты имеют здесь значение по азбуке Морзе или иному коду);
- записи в виде кардиограммы или же графика некого технологического процесса (здесь, при использовании азбуки Морзе, пики повыше означа-

ют, скажем, точки, а те, что ниже, — тире, черточки между зубцами сообщают о разделе между буквами, разрывы линии фиксируют конец слова);

- записи лишь в вертикальных столбцах цельно заполненного кроссворда (горизонтальные строки при этом заполняются произвольно, само же сообщение может быть либо прямым, либо кодированным);
- записи по трафарету, при этом на лист почтовой бумаги накладывают трафарет с вырезанными в нем окошками, следуя по которым и вписывают истинное сообщение; все остальное пространство здесь тщательно заполняется «пустым» содержанием так, чтобы слова подлинной информации четко входили в текст ясного маскировочного послания;
- шифр «Аве Мария», в кодовом варианте которого каждому слову, а порой и фразе ставятся в соответствие несколько слов явной религиозной тематики, так что передаваемое сообщение выглядит как специфический текст духовного содержания.

Развитие компьютерной технологии и средств коммуникации сделали бесполезными подобные ограничения. Сегодня каждый может воспользоваться теми преимуществами, которые дает стеганография, как в области скрытой передачи информации, что особенно полезно в странах, где существует запрет на стойкие средства криптографии, так и в области защиты авторских прав. Рассмотрим практические применения этой науки.

Компьютерная стеганография (стеганографические программные продукты), например, базируется на двух принципах. Первый заключается в том, что файлы, содержащие оцифрованное изображение или звук, могут быть до некоторой степени видоизменены без потери своей функциональности, в отличие от других типов данных, требующих абсолютной точности. Второй принцип состоит в неспособности органов чувств человека различить незначительные изменения в цвете изображения или качестве звука.

Это особенно легко использовать применительно к объекту, несущему избыточную информацию, будь то 16-битный звук, 8-битное или еще лучше 24-битное изображение. Так, если речь идет об изображении, то некоторое изменение значений наименее важных битов, отвечающих за цвет, не приводит к какому-нибудь заметному для человеческого глаза изменению цвета.

Одной из лучших и самых распространенных продуктов в этой области для платформы Windows95/NT является программа S-Tools (имеет статус freeware). Программа позволяет прятать любые файлы как в изображениях формата gif и bmp, так и в звуковых файлах формата wav. При этом S-Tools — это стеганография и криптография «в одном флаконе», потому что файл, подлежащий сокрытию, еще и шифруется с помощью одного из криптографических алгоритмов с симметричным ключом: DES, тройной DES или IDEA. Работа программы заключается в следующем. Файл-носитель перетаскивается в окно программы, затем в этот файл перетаскивается файл с данными любого формата, вводится пароль, выбирается алгоритм шифрования — и перед вами результат, который впечатляет! Внешне графический файл остается практически неизменным, ме-

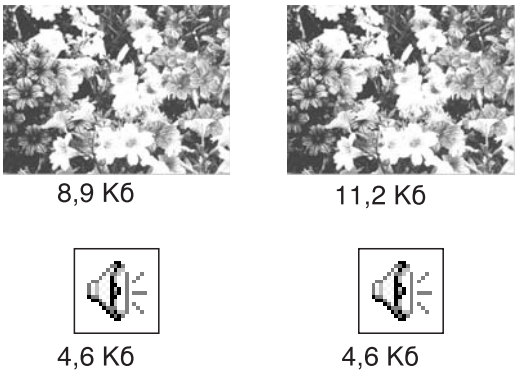


Рис. 4.14. Пример использования стеганографии

няются лишь кое-где оттенки цвета. Звуковой файл также не претерпевает заметных изменений. Для большей безопасности следует использовать неизвестные широкой публике изображения, изменения в которых не бросятся в глаза с первого взгляда, а также изображения с большим количеством полутонов и оттенков (пестрые картинки). Для этого подойдет, например, осенний пейзаж, букет цветов, фотография вашего песика и т. п. Рассмотрим один из примеров, представленный на рис. 4.14.

В первом ряду левое изображение (8,9 Кб) не содержит зашифрованной информации, правое же (11,2 Кб) содержит небольшой текст, поэтому его конечный размер увеличился. Во втором ряду первый звуковой файл (4,6 Кб) также «чист», а второй вместил в себя 0,5 Кб текста, при этом не увеличив свой размер! Поразительно, правда? Нет практически никаких отличий. Соотношение между размером файла с изображением или звуком и размером текстового файла, который можно спрятать, зависит от конкретного случая. Иногда размер текстового файла даже превышает размер графического. Впрочем, даже если подозрения у кого-то и возникнут, то их придется оставить при себе: не зная пароля, сам факт использования S-Tools установить и доказать нельзя.

Другая распространенная стеганографическая программа — Steganos for Windows95 (shareware). Она обладает практически теми же возможностями, что и S-Tools, но использует другой криптографический алгоритм (HWY1) и, кроме того, способна прятать данные не только в файлах формата bmp и wav, но и в обычных текстовых и HTML-файлах, причем весьма оригинальным способом — в конце каждой строки добавляется определенное количество пробелов.

Если рассматривать коммерческие приложения стеганографии, то одним из наиболее перспективных направлений ее развития являются цифровые водяные знаки (digital watermarking). Создание невидимых глазу водяных знаков используется для защиты авторских прав на графические и аудиофайлы. Такие помещенные в файл цифровые водяные знаки могут быть распознаны только специальными программами, которые извлекут из файла много полезной информации: когда создан файл, кто владеет авторскими правами, как вступить в контакт с автором. При том повальном воровстве, которое происходит в Интернете, польза этой технологии очевидна.

Сегодня на рынке существуют довольно много фирм, предлагающих продукты для создания и детектирования водяных знаков. Один из лидеров — фирма Digimarc, программы которой, если верить предоставленной самой фирмой информации, установили себе более миллиона пользователей. Фир-

ма предлагает сгрузить с сайта PictureMarc, подключаемый модуль для Photoshop и CorelDraw, или отдельно стоящий ReadMarc.

Казалось бы, наступает золотая эра честности, авторы больше не страдают от воровства, воры берут в руки фотоаппараты, кисти, мыши и учатся творить прекрасное в Photoshop'е — и вот тут некритичность файлов с изображениями к некоторым видоизменениям играет с ними плохую шутку. Несмотря на все заверения создателей соответствующих продуктов, цифровые водяные знаки оказались нестойкими. Они могут перенести многое — изменение яркости и контраста, использование спецэффектов, даже печать и последующее сканирование, но они не могут перенести хитрое воздействие специальных программ-стирателей, таких, как UnZign или StirMark, которые появились в Интернете, причем очевидно не с целью насолить Digimarc, Signum Technologies и другим, а для того, чтобы дать пользователям возможность сделать правильный выбор, основываясь на независимой оценке стойкости водяных знаков. А оценка эта на сегодняшний день малоутешительна — водяные знаки всех производителей уничтожаются без заметного ухудшения качества изображения.

4.4. Организация защиты информации в компьютерных сетях

К сожалению, пока законодательство в области защиты информации далеко от совершенства. Но при правильном использовании уже имеющихся законодательных и целого ряда подзаконных актов можно добиться весьма ощутимых успехов в области возмещения своих убытков и в то же время не попасть под карающий меч государственных структур.

Чтобы свести к минимуму риск в коммерческой деятельности, нужно оценивать всевозможные угрозы безопасности с учетом двух факторов:

- возможной частоты действия угроз;
- возможного ущерба от их действия.

Поэтому очень важно четко уяснить, какая используемая в вашем учреждении информация, пусть даже не принадлежащая вам, подлежит обязательной защите. Начать надо с проведения предварительного анализа имеющейся у вас информации. От этого в дальнейшем будет зависеть выбор степени ее защиты.

Документирование информации проводится по строго определенным правилам. Основные из них изложены в ГОСТ 6.38-90 «Система организационно-распорядительной документации. Требования к оформлению документов», ГОСТ 6.10.4-84 «Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники» и некоторых других. Надо отметить, что эти ГОСТы предполагают 31 реквизит, который делает информацию

документом, но необязательно, чтобы присутствовали все предлагаемые реквизиты. Главный реквизит — это текст. Поэтому любая информация, изложенная в виде связного текста без каких-либо дополнительных реквизитов, уже может рассматриваться как документ, для придания определенной юридической силы которому необходимы также такие важные реквизиты, как дата и подпись.

Особый порядок существует только для документов, полученных из автоматизированных информационных систем. При этом в определенных случаях применяется процедура заверения информации, полученной от удаленного объекта, электронной подписью.

Защита информации — удовольствие достаточно дорогое, поэтому одним из принципов построения системы защиты должен стать принцип дифференциации степени защиты информации по ее важности и ценности.

Анализ мирового и отечественного опыта обеспечения безопасности свидетельствует о необходимости создания целостной системы безопасности учреждения, взаимоувязывающей организационные, оперативные и оперативно-технические меры защиты с использованием современных методов прогнозирования, анализа и моделирования ситуаций.

При организации защиты информации необходимо придерживаться определенного курса, следуя некоторым советам.

Совет первый:

- проанализируйте информацию, которая циркулирует в вашем учреждении;
- выделите сведения ограниченного доступа;
- оцените коммерческую важность информации;
- составьте перечень сведений, содержащих коммерческую тайну, утвердите его и ознакомьте с ним исполнителей;
- определите объем информации, составляющей государственную тайну.

Все это позволит вам дифференцировать мероприятия по обеспечению безопасности информации и тем самым сократить расходы.

Совет второй:

- убедитесь в лояльности сотрудников службы безопасности;
- принимая сотрудника на работу, постарайтесь всеми доступными средствами навести о нем справки;
- продумайте систему морального и материального поощрения сотрудников за соблюдение лояльности;
- регулярно тестируйте сотрудников, которые соприкасаются с информацией ограниченного доступа;
- обязательно оговаривайте в договоре или контракте с сотрудником условия сохранения служебных тайн не только на период совместной работы, но и на определенный срок после завершения ваших взаимоотношений;

- старайтесь всегда соблюдать принцип комплексного подхода к решению проблемы защиты информации;
- придерживайтесь правила «доверяй, но проверяй». Это вселит в вас уверенность, что в критический момент система безопасности не даст сбоя;
- учитывайте пространственные факторы: введение контролируемых (охраняемых) зон, правильный выбор помещений и расположение объектов между собой и относительно границ контролируемой зоны;
- учитывайте временные факторы: ограничение времени обработки защищаемой информации, доведение времени обработки информации с высоким уровнем конфиденциальности до узкого круга лиц.

Совет третий:

- создайте концепцию информационной безопасности;
- увяжите эту концепцию с общей концепцией безопасности вашего учреждения.

Концепция — это официально принятая система взглядов на проблему информационной безопасности и пути ее решения с учетом современных тенденций развития информатизации вашей компании. Она является методологической основой вашей политики в разработке практических мер по ее реализации. На основе сформулированных в концепции целей, задач и возможных путей их решения формируются конкретные планы обеспечения информационной безопасности.

Выявление вмешательства в компьютерную систему часто весьма затруднено вследствие того, что злоумышленникам чаще всего удается скрыть следы проникновения в систему. Все попытки взлома систем обнаруживаются обычно совершенно случайно. Например, администратор сети заметил пропуск в файле протокола или вхождение в систему в отсутствие пользователя. Или он был предупрежден другими администраторами безопасности о присутствии постороннего в сети.

Для выявления несанкционированного доступа необходимо:

- регулярно проверять файлы протоколов, особенно протоколов входа в систему;
- отслеживать подсоединение неизвестных пользователей в непривычное время;
- обращать внимание на идентификаторы пользователей, которые оставались какое-то время неиспользованными и оказались снова задействованными.

Как правило, злоумышленники используют для своей работы нерабочее время (обычно с 18.00 до 8.00), а также выходные и праздничные дни.

Одним из способов выявления постороннего присутствия в сети является запуск каждые 10 мин обычной процедуры, написанной на языке shell, которая фиксирует все процессы и соединения по сети в отдельном файле. Эта

программа формирует списки пользователей, всех текущих процессов и сетевых подключений.

Способы защиты от проникновения в вычислительную систему приводятся во многих изданиях. Обобщив приведенную в них информацию, можно предложить общие рекомендации по обеспечению безопасности сетей:

- удаляйте все шаблоны из списка гостевых систем;
- используйте файлы .rhosts правильно, позволяя входить в вашу систему только тем, кому вы действительно доверяете;
- необходимо закрыть доступ для всех пользователей к файлу .netrc, содержащему пароли в незашифрованном виде, и его резервным копиям, создаваемым некоторыми редакторами;
- открывая доступ удаленным машинам к пользовательской файловой системе, установите режим «только для чтения».

Для эффективной защиты информации в компьютерных сетях предприятий, организаций и т. п. необходимо создавать службы администратора безопасности информации, на сотрудников которых возлагается решение следующих основных задач:

- организация и поддержание контролируемого доступа пользователей к ресурсам компьютерной сети на всех этапах ее жизненного цикла;
- слежение за состоянием безопасности компьютерной сети и оперативное реагирование на происходящие в ней несанкционированные действия пользователей.

Так как механизмы защиты, встроенные в распространенные операционные системы, например MS-DOS/Windows 3.X, Novell Netware, Windows 95, не обеспечивают надежной защиты информации, то решать упомянутые выше задачи в них просто невозможно.

На рынке средств защиты сегодня представлено большое разнообразие систем защиты информации. Перед администратором безопасности встает вопрос определения необходимости и порядка их применения. Очевидно, что далеко не все компьютеры организации необходимо оснащать дополнительными системами защиты информации, так как это требует новых материальных затрат и может только затруднить эксплуатацию всей компьютерной сети в целом.

Применение средств защиты информации целесообразно в следующих случаях:

- при размещении на компьютерах средств криптографической защиты данных. Здесь дополнительные средства защиты информации необходимы для защиты ключей электронной цифровой подписи и шифрования;
- при необходимости регламентации и протоколирования действий пользователей, работающих на компьютерах, подключенных к сети. В этом

случае система защиты решает задачу недопущения действий пользователей, не предусмотренных технологией обработки данных;

- при необходимости ограничения доступа пользователей, работающих на компьютере, к его локальным ресурсам (дискам, каталогам, файлам или внешним устройствам), а также исключения возможности самостоятельного изменения состава и конфигурации программных средств, установленных на компьютере.

Применение дополнительных средств защиты предполагает выполнение администратором безопасности предприятия ряда действий. Он должен:

- устанавливать средства защиты информации на компьютеры;
- настраивать средства защиты информации путем задания прав доступа пользователей к ресурсам как компьютеров, так и сети;
- контролировать состояние защищенности компьютерной сети путем оперативного мониторинга и анализа системных журналов.

В большинстве случаев средства защиты информации устанавливаются на уже реально функционирующую систему. Так как защищаемая компьютерная система обычно используется для решения важных задач (часто в непрерывном технологическом цикле), ее владельцы и пользователи неодобрительно относятся к любому, даже кратковременному, перерыву в ее работе, необходимому для установки и настройки системы защиты информации.

Следует учитывать, что с первого раза правильно настроить систему защиты практически невозможно. Обычно это связано с отсутствием в организации полного детального списка всех аппаратных, программных и информационных ресурсов системы, подлежащих защите, и готового противоречивого перечня прав доступа и полномочий каждого пользователя. Поэтому этап внедрения системы защиты информации обязательно включает действия по первоначальному выявлению, последовательному уточнению и соответствующему изменению настроек, устанавливаемых в этой системе.

Очевидно, что те же самые действия администратору безопасности придется неоднократно повторять и на этапе эксплуатации системы защиты информации при изменениях состава технических средств, программного обеспечения и. т. д. Такие изменения происходят довольно часто, поэтому средства управления этой системы должны обеспечивать удобство осуществления необходимых при этом настроек.

В этом случае, если средства управления не приспособлены к этому, а сами системы защиты информации не обладают достаточной гибкостью, то очень скоро они становятся не помощником, а обузой для всех, и в первую очередь для администраторов безопасности. В конце концов такие системы защиты информации обречены на отторжение.

Деятельность администратора безопасности на этапе эксплуатации системы защиты информации состоит в корректном и своевременном внесении из-

менений в полномочия пользователей и настройки защитных механизмов на компьютерах сети. С увеличением масштаба защищаемой компьютерной сети и при сохранении неизменным количества людей, отвечающих за ее информационную безопасность, изменяются требования к способам управления этой системой. Как показывает практика, решения, приемлемые для одного компьютера или небольшой сети из 10—15 рабочих станций, как правило, не устраивают обслуживающий персонал и администраторов безопасности больших сетей, объединяющих сотни машин.

Проблемы по управлению полномочиями пользователей и настройками системы защиты информации в компьютерной сети могут быть решены, например, на основе использования системы, централизованного управления доступом к сети.

Принцип реализации такой системы состоит в применении специального сервера управления доступом, работающего на основном файловом сервере сети, который осуществляет автоматическую синхронизацию центральной базы данных защиты с локальными базами данных защиты, размещенных на рабочих станциях пользователей.

Введение распределенной базы данных защиты (центральной и локальных) гарантирует, что выход из строя сети или сервера управления доступом не будет препятствовать нормальному функционированию средств защиты на рабочих станциях.

При данной системе управления доступом полномочия пользователя меняются периодически в центральной базе данных защиты, а их изменение на конкретных компьютерах обеспечивается во время очередного сеанса синхронизации.

Кроме того, при смене пользователем своего пароля на одной из рабочих станций новое значение пароля этого пользователя автоматически отражается в центральной базе данных защиты, а также передается на рабочие станции, на которых данному пользователю разрешено работать.

Администратору безопасности необходимо контролировать состояние компьютерной сети как оперативно (путем слежения за состоянием защищенности компьютеров сети), так и не оперативно (путем анализа содержимого журналов регистраций событий системы защиты информации).

Использование сервера управления доступом для оперативного контроля за состоянием рабочих станций и работой пользователей позволяет отказаться от постоянного присутствия в сети администратора безопасности. В этом случае сервер управления доступом автоматически регистрирует несанкционированные действия, происходящие в сети, и всегда обладает оперативной информацией о состоянии станций сети.

Увеличение количества рабочих станций и использование программных средств, включающих большое количество разнообразных компонентов, приводит к существенному увеличению объемов журналов регистрации событий в системе защиты информации. Объем сведений, хранящийся в журналах,

может стать настолько большим, что администратор уже физически не сможет полностью проанализировать их содержимое за приемлемое время.

Для облегчения работы администратора по контролю за состоянием безопасности сети предлагаются следующие рекомендации:

- оперативный контроль за состоянием рабочих станций сети и работой пользователей, регистрация событий несанкционированного доступа в специальном журнале;
- селекция определенных событий (по имени пользователя, дате, времени происшедшего события, его категории и т. п.) из системных журналов;
- хранение системных журналов каждой рабочей станции по принципу «день/месяц/год» с автоматическим ограничением срока их хранения. По истечении установленного срока журналы автоматически уничтожаются;
- семантическое сжатие данных в журналах регистрации, позволяющее увеличивать регистрируемые события без существенной потери их информативности;
- автоматическая подготовка отчетных документов установленной формы о работе станций сети и имевших место нарушениях, благодаря чему существенно снижается рутинная нагрузка на администратора безопасности.

Большинство пользователей рано или поздно сталкивается с проблемой вирусов. Обычно первое «знакомство» сопровождается определенными потерями программ и данных, а также времени на их восстановление. Уменьшить угрозу заражения компьютера или компьютерной сети можно применением совокупности организационных и профилактических мероприятий, которые получили название «компьютерная гигиена». Компьютерная гигиена предусматривает выполнение следующих рекомендаций:

- использовать только лицензионное программное обеспечение;
- избегать копирования файлов с компьютеров, на которых не соблюдаются требования компьютерной гигиены;
- не использовать программы, поведение которых непонятно или неясны выполняемые программой действия;
- приобретаемые программы перед передачей пользователям должны изучаться системными программистами (специалистами по вирусам);
- новые программы следует испытывать на отдельном компьютере, не содержащем важной информации, в течение определенного промежутка времени (период карантина);
- подвергать программы, источники которых ненадежны, усиленному карантину;
- проверенное новое программное обеспечение должно дублироваться на заведомо «чистом» компьютере. Оригинал должен быть защищен от записи и храниться отдельно;
- ограничить доступ посторонних к компьютерам;

- обнаружив симптомы наличия вируса, предупредить всех пользователей и системного программиста (специалиста по вирусам).

Защита от компьютерных вирусов в настоящее время основывается на применении организационных мероприятий и программных средств, которые практически включают в себя аппаратные возможности IBM совместимых компьютеров, программных средств, системного программного обеспечения и специальных программных средств защиты.

Организационные средства позволяют минимизировать риск заражения компьютеров вирусами, а при заражении — сразу же информировать пользователя и облегчить уничтожение вируса и его последствий. Организационные меры защиты включают следующие основные мероприятия:

- резервирование;
- наличие всех основных компонентов операционной системы и программного обеспечения в архивах;
- копирование таблиц распределения файлов дисков;
- ежедневное ведение архивов изменяемых файлов;
- профилактику;
- систематическую выгрузку содержимого активной части винчестера на дискеты;
- раздельное хранение компонентов программного обеспечения и программ пользователей;
- хранение неиспользуемых программ в архивах;
- ревизию;
- обследование вновь получаемых программ на дискетах на наличие вирусов;
- систематическую проверку длин файлов, хранящихся на винчестере;
- использование и постоянную проверку контрольных сумм при хранении и передаче программного обеспечения;
- проверку содержимого загрузочных секторов винчестера и используемых дискет системных файлов;
- фильтрацию;
- разделение винчестера на логические диски с различными возможностями доступа к ним;
- использование резидентных программных средств слежения за файловой системой;
- защиту, основанную на использовании специальных программных средств.

Все эти мероприятия в той или иной степени включают использование различных программных средств защиты. К их числу необходимо отнести программы-архиваторы, программы резервирования важных компонентов файловой системы, просмотра содержимого файлов и загрузочных секторов, подсчета контрольных сумм и собственно программ защиты.

ГЛАВА ПЯТАЯ

ОРГАНИЗАЦИЯ ПРОТИВОДЕЙСТВИЯ КОММЕРЧЕСКОЙ РАЗВЕДКЕ

Читателю, ознакомившемуся с содержанием предыдущих глав, нет необходимости доказывать, какое большое внимание должно быть уделено защите от несанкционированного получения информации с помощью технических средств.

Во многих организациях, действующих на территории бывшего СССР, большое внимание уделяется вопросам сохранения коммерческой тайны. Однако недостаток информации о возможностях технических средств разведки, простота получения с их помощью нужной информации зачастую оставляют возможность беспрепятственного доступа к информации, нуждающейся в защите.

Естественно, формы, способы и конкретные устройства противодействия технической коммерческой разведке по той же причине недостатка информации очень часто остаются вне сферы внимания многих заинтересованных лиц.

Защита информации или противодействие технической коммерческой разведке в общем случае представляет собой комплекс мероприятий организационного и технического характера.

Технические мероприятия, чему и посвящена эта книга, включают:

- поиск и уничтожение технических средств разведки;
- кодирование (шифрование) информации или передаваемого сигнала;
- подавление технических средств постановкой помехи;
- мероприятия пассивной защиты: экранирование, развязка, заземление, звукоизоляция и т. д.
- системы ограничения доступа, в том числе биометрические системы опознавания личности;
- применение детекторов лжи.

Для гарантированной защиты нужно иметь в виду, что применение технических средств должно носить как можно более комплексный характер и, кроме того, обязательно сочетаться с мероприятиями организационного характера.

5.1. Внешний осмотр проверяемых помещений

Как указывалось ранее, главным инструментом того, кто ищет, является здравый смысл и аналитический ум. На втором месте — набор специальных инструментов и приборов, необходимых для проведения визуальных осмотров.

Внимательный осмотр помещений, в которых производится проверка, часто дает положительные результаты. При осмотре отмечают предметы, которые стоят не на своем месте, следы царапин, сделанные инструментами, или протечки жидкости — свежей краски, лака и т. п. Осматривают вещи и предметы, которые недавно трогали. Особое внимание следует уделять местам возможной установки устройств съема информации (рис. 5.1).

Один из способов — разборка предметов. Известно, что во многих предметах фабричного изготовления есть пустые пространства, в которых могут быть спрятаны устройства съема информации. Разборка может быть простой, не требующей специальных инструментов: например, открыть портативный приемник и посмотреть, находятся ли в батарейном отсеке батарейки или что-нибудь другое.

Бывают и более сложные случаи, когда для разборки требуются инструменты. Набор специальных инструментов необходим для проведения любой серьезной работы. Ведь обнаружить мелкий предмет, который может быть тщательно замаскирован в стену, перегородку и т. п., можно только при помощи специальных устройств. В жилых и служебных помещениях «жучки» можно спрятать в хорошо доступных и абсолютно неожиданных местах: выключателях, розетках, под плинтусами, водопроводных трубах, сантехнических устройствах и т. п. Любой бытовой прибор в доме — это потенциальное для них место.

Специальные инструменты и приборы для проведения поисковых мероприятий

Основным инструментом при проведении внешнего осмотра является поисковое зеркало. Оно может быть маленьким, примерно как у зубного врача, может быть и гораздо больше. Зеркало (рис. 5.2) крепится на длинной, в несколько десятков сантиметров, ручке.

В наше время существуют очень маленькие, портативные рентгеновские приборы, которыми пользуются многие сотрудники службы безопасности для обнаружения различных устройств съема информации.

Принципиальный недостаток рентгеновских приборов состоит в том, что излучение экранируется любыми металлическими предметами. Даже небольшие металлические детали могут замаскировать искомый предмет.

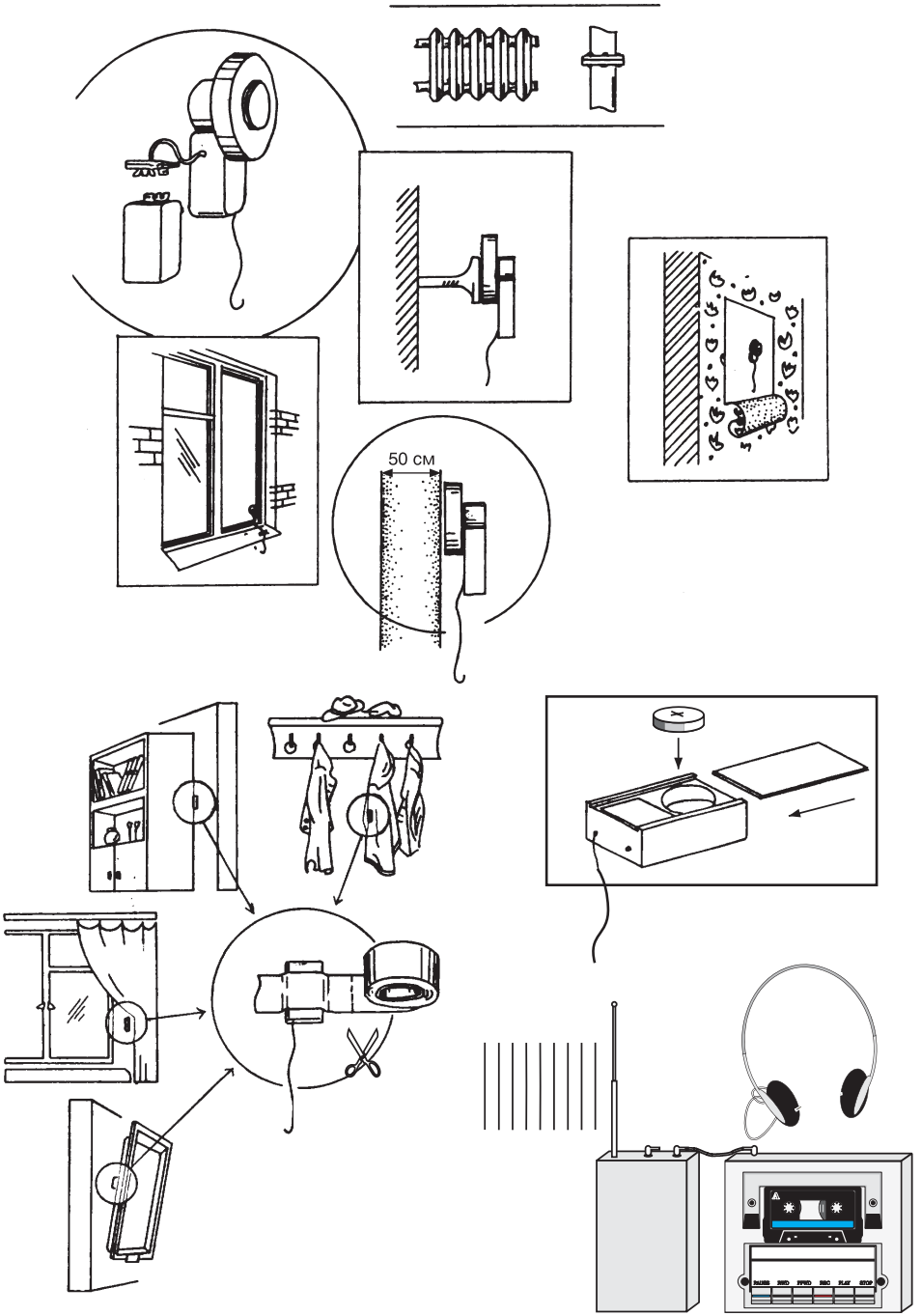


Рис. 5.1. Возможные места установки устройств съема информации

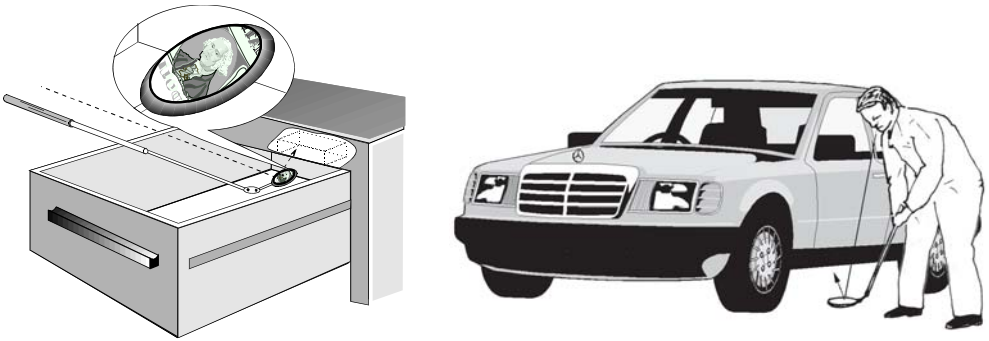


Рис. 5.2. Поисковое зеркало

Современные телевизионные и оптические системы включают в себя эндоскопическое и портативное телевизионное оборудование, а также специальные оптические приборы и зеркала. Они существенно расширяют возможности специалистов по поиску устройств негласного съема информации.

С эндоскопами знакомо большинство людей, страдающих заболеваниями или проходящих обследование желудочно-кишечного тракта. Трудно забыть неприятные ощущения, связанные с кабинетом эндоскопического обследования, когда вам в пищевод врач засовывает гибкий шланг длиной около 1 м с лампочкой и объективом на конце. Но порой только так можно добраться в разные труднодоступные места и хорошо их осмотреть.

Портативные телевизионные системы также используются для быстрого поиска и осмотра помещений. Оптические приборы и зеркала дополняют собой возможности эндоскопического и телевизионного оборудования, а кроме того, имеют некоторые самостоятельные применения: например, зеркала используются для осмотра автомобилей.

Современный технический уровень средств дистанционного визуального наблюдения достаточно высок. Ассортимент эндоскопической продукции включает в себя целую гамму гибких волоконно-оптических фиброскопов (рис. 5.3), жестких бароскопов, гибких видеоскопов, систем передачи изображения, портативных видеосистем и видеоанализаторов, позволяющих осуществлять осмотр труднодоступных мест с получением изображения высокого качества. Общим и главным для всех этих устройств является миниатюрный объектив, помещаемый на конце тонкого гибкого рукава или жесткой трубки, внутри которых изображение передается по оптоволоконному жгуту или посредством многокомпонен-

Рис. 5.3. Промышленный фиброскоп

Рис. 5.4. Промышленный бароскоп

тных линз к окуляру. Рядом с объективом может располагаться ПЗС-матрица, сигнал с которой по кабелю передается к блоку преобразования сигнала и к телевизионному монитору. Гибкие эндоскопы легко проходят сквозь сложные изгибы различных каналов. Бароскопы, в отличие от гибких эндоскопов, вместо гибкого рукава оборудованы жесткой штангой, на конце которой размещен объектив и (или) ПЗС-матрица (рис. 5.4). Бароскопы используются для осмотра узлов, к которым может быть осуществлен доступ через узкие прямолинейные каналы.

Видеоскопы идеально подходят для осмотра удаленных зон. Изображение выводится на ТВ-монитор в реальном масштабе времени, с одновременным фото- и видеодокументированием. Все эти возможности эндоскопических систем в полной форме реализованы, например, в серийной продукции фирмы Olympus (Япония). Вместе с тем это оборудование не вполне удовлетворяет требованиям оперативности проведения осмотра. Практически все промышленные эндоскопические системы рассчитаны скорее на статическое скрупулезное обследование, чем на быстрый оперативный осмотр.

Эти системы имеют многомодульную конфигурацию с кабельными соединениями, их функциональные блоки не минимизированы по весу и габаритам. Очевидны также проблемы с быстрой подготовкой к работе, переносом системы и сохранением ее целостности. Еще одна существенная особенность заключается в не всегда приемлемом качестве наблюдаемого через окуляр изображения.

Видеоскопы (рис. 5.5) позволяют вести наблюдение через миниатюрную ПЗС-матрицу на удалении до 22 м. Сигнал по кабелю поступает на блок преобразования и далее — на ТВ-монитор. Разрешающая способность и, как следствие, качество изображения в видеоскопах значительно выше, чем то, которое достигается с помощью фиброскопов. По ТВ-монитору следить за осмотром может практически неограниченное количество наблюдателей. В то же время подобное оборудование не может использоваться одним оператором и не приспособлено для быстрой смены места осмотра и обхода объектов. Для этого больше подходят портативные эндоскопические устройства типа фиброскопов МР-660В или ММ-013С.

Рис. 5.5. Промышленный видеоскоп

Рис. 5.6. Система S-1000 («Кальмар»)

Соединить преимущества высокого качества изображения с максимальным удобством пользования оборудованием при досмотре позволяют портативные телевизионные системы. Это достигается путем конструктивного объединения в едином устройстве миниатюрной телевизионной камеры, регулируемой штанги и телевизионного монитора. Угловое положение камеры изменяется с помощью гибкой концевой части штанги или фиксируемого шарнира. Телевизионный сигнал и питание передаются по кабелю, пропущенному внутри штанги. В телескопических штангах обеспечивается подмотка избыточного кабеля на встроенный подпружиненный барабан. Монитор для наблюдения изображения крепится на рукоятке штанги посредством регулируемого кронштейна. Характерными особенностями телевизионных портативных систем являются следующие:

- цилиндрический корпус камеры со встроенной инфракрасной подсветкой обеспечивает максимально возможную для этого оборудования способность проникать в труднодоступные места. Герметизация корпуса камеры позволяет вести наблюдение в жидких средах;
- телескопическая штанга имеет широкий диапазон регулирования фиксируемых положений, обеспечивая свободный доступ как к более, так и к менее удаленным от оператора местам обследования без необходимости манипулирований кабелями, разъемами, модулями, принадлежностями и т. п.;
- компактный монитор с электронно-лучевой трубкой, съемно устанавливаемый на штанге, создает наиболее удобные для оператора условия визуального наблюдения и качество изображения, достаточное для проведения осмотра;
- конструкция изделия обеспечивает минимальное время для подготовки прибора к работе. Пылевлагозащитный и ударопрочный корпус предохраняет устройство от влияния окружающей среды и позволяет использовать его практически в любых условиях.

Примером реализации этих особенностей может служить система типа S-1000 («Кальмар»), внешний вид которой показан на рис. 5.6. В некоторых случаях для выполнения досмотра приемлемы более простые телевизионные системы. Их конструкции могут широко варьироваться по длине и исполнению штанги, типу монитора, способу установки и параметрам камеры, ресурсу автономного питания и другим характеристикам. Эффективность применения телевизионных систем, как и эндоскопического оборудования, во многом зависит от точного выбора обору-

Рис. 5.7. Система «Кальмар» в работе

дования в соответствии с объектом осмотра и условиями применения. Особенно удобны портативные телевизионные системы для операций таможенного досмотра всевозможных транспортных средств и контейнеров.

При всем отличии рассмотренных выше технических средств можно заметить, что каждое из них в отдельности имеет определенный предел в своем развитии. Хотя можно и нужно улучшать качество отдельных элементов, вносить полезные усовершенствования и дополнения, оптимизировать комплектацию и т. д., но все же наиболее перспективный путь повышения эффективности подобных систем, как показывают примеры из других областей техники, заключается в объединении возможностей различного оборудования. Таким образом, например, существенно возросли возможности бесконтактного выявления у людей скрытно проносимых предметов за счет совмещения стационарных металлодетекторов с детектированием паров взрывчатых веществ, обнаружением радиоактивных материалов и нелинейной локацией радиоэлектронных устройств.

В сфере средств визуального осмотра (рис. 5.7) также можно кое-что усовершенствовать. Наиболее очевиден путь взаимного усиления достоинств эндоскопических и телевизионных систем. Например, телескопическая штанга с установленной на ней телевизионной системой типа «Кальмар» позволяет свободно выносить гибкую часть эндоскопа на значительное расстояние, устраняя длинные свисающие кабели передачи сигнала и подсветки, а использование компактного носимого монитора вместо окуляра делает более удобным визуальное наблюдение. Дополнительные преимущества таким системам придает модуль радиоканала для передачи видеоизображения на пост дистанционного наблюдения или контроля.

Следующий шаг связан с объединением возможностей визуального и детекторного исследования. При визуальном осмотре осуществляется прямое зрительное распознавание предметов, которое требует длительной повышенной концентрации внимания оператора и не всегда дает надежный результат. Под детекторным исследованием понимается применение аппаратуры, которая контактным или бесконтактным способом может воспринимать определенные физические свойства, свидетельствующие о наличии в обследуемом месте некоторых аномалий в виде неоднородностей, характерных излучений или конкретных веществ. С точки зрения эффективности обследования с применением детекторов существенно то, что они вырабатывают сигнал в случае превышения заданного порога чувствительности, тем самым не только выявляя, но и локализуя искомое устройство или материал. В результате объеди-

Рис. 5.8. Система для досмотра автотранспорта S-1100 («Дозор»)

нения визуального и детекторного методов поиска повышается вероятность обнаружения и сокращается время осмотра.

Основная проблема состоит в том, чтобы при всех усовершенствованиях сохранить легкость и удобство обращения с оборудованием. Для этого, в частности, требуется, чтобы чувствительный элемент детектора, выносимый на конец досмотровой штанги, имел минимально возможные габариты и вес. Для ВЧ-аппаратуры важно обеспечить безопасные, но эффективные параметры излучения. Необходимо также решить проблемы функциональной и конструктивной совместимости различных технических средств.

Примером успешного решения этих и многих других трудностей служит система для досмотра автотранспорта S-1100 («Дозор»), позволяющая осуществлять одновременно локацию объекта и вести телевизионное наблюдение за обследуемой зоной (рис. 5.8). В легкий малогабаритный антенный блок системы, осуществляющий ВЧ-зондирование, встроена миниатюрная телевизионная камера, сориентированная по диаграмме направленности антенны, что позволяет точно наблюдать зону отклика при получении сигнала локации. Конструкция прибора позволяет обследовать самые труднодоступные места (рис. 5.9).

Такую систему можно дополнить малогабаритным дозиметром, детектором взрывчатых веществ и наркотиков, приборами для обнаружения часовых механизмов и магнитов и другими средствами обследования.

Рис. 5.9. Система «Дозор» в работе

Если количество аппаратуры и приспособлений или особенности выполняемых задач превысят возможности применения стандартного оборудования, на помощь придут радиоуправляемое шасси с манипуляторами, средства нейтрализации и другое оборудование, рассмотрение которого выходит за рамки данной книги.

Металлодетекторы

Стационарные металлоискатели мы все видели в аэропортах и на крупных стадионах. Но есть и другие, портативные приборы. Ручной металлоискатель применяют для быстрой и скрытной проверки на наличие оружия, диктофонов и других устройств.

Срабатывание металлоискателя зависит как от массы металлического предмета, так и от расстояния до него. Чтобы обнаружить мелкий предмет, прибор должен находиться очень близко от него. При этом более крупные предметы будут экранировать мелкие, и последние останутся незамеченными. На практике это означает, что мимо металлоискателя можно пронести миниатюрные «жучки», если спрятать их достаточно глубоко. Определить нужную глубину можно методом проб и ошибок, используя металлоискатель того типа, которым будет производиться проверка.

Металлодетектор предназначен для поиска металлических предметов из черных и цветных металлов в непроводящих и слабо проводящих средах (дерево, одежда, пластмасса и т. п.). Существует множество промышленных конструкций металлодетекторов. Внешний вид одного из них представлен на рис. 5.10.

Прибор имеет звуковую и световую сигнализацию. Дальность обнаружения металлических предметов от 20 до 200 мм.

Стационарный арочный металлодетектор «Поиск-3М»

Стационарный селективный вихревой металлодетектор «Поиск-3М» (рис. 5.11) предназначен для осуществления контроля посетителей на наличие под одеждой огнестрельного или холодного оружия и средств негласного съема информации на объектах с контролируемым доступом.

Он имеет возможность настраиваться на различные массы металла. Прост в монтаже и настройке, отделан под ценные породы дерева и гармонично встраивается в любой дверной проем. Предусмотрена световая и звуковая сигнализация. В модели «Поиск-3МР» предусмотрен встроенный датчик ионизирующего излучения, что позволяет изделию кроме выполнения основной функции контролировать пронос на охраняемый объект источников радиоактивного излучения.

Основные характеристики

Ширина прохода, м 0,8
Скорость следования через проход, м/с ..... до 2
Вероятность обнаружения оружия, % 0,95
Вероятность ложных тревог, % 0,02

Рис. 5.10. Ручной металлодетектор «Metor 22»

Рис. 5.11. Стационарный селективный вихревой металлодетектор «Поиск-3М»

Портативный металлодетектор «COMET»

Портативный ручной металлоискатель «COMET» представляет собой ручной полупроводниковый прибор (рис. 5.12).

Изделие выполняет следующие функции:

- определяет наличие металлических включений в строительных конструкциях, мебели, почтовой корреспонденции и одежде человека;
- идентифицирует токоведущие проводники за неметаллическими преградами.

Прибор имеет малые габариты, световую и звуковую индикацию обнаружения металлических предметов, низкое энергопотребление, устойчивость к внешним помехам, что делает его очень удобным в использовании.

Наряду с профессиональными промышленными образцами, которые стоят довольно дорого, для решения ваших задач можно использовать и приборы, изготовленные самостоятельно. Они имеют достаточно высокие характеристики, подчас не уступающие промышленным образцам. Ниже описываются несколько таких устройств.

Практические схемы металлодетекторов (металлоискателей)

Рис. 5.12. Портативный металлодетектор «COMET»

Принцип действия описываемых ниже приборов основан на сравнении значений частоты колебаний двух генераторов: образцового и перестраиваемого, частота которого изменяется под воздействием на его колебательный контур искомого металлического предмета. По сравнению с другими известными методами — мостовым (регистрируется разбаланс измерительного моста, в одно из плеч которого включена поисковая катушка), сдвига фаз (измеряется фазовый сдвиг колебаний образцового и перестраиваемого генераторов), передатчик-приемник (регистрируется переизлучаемая металлическим предметом радиочастотная энергия) — метод сравнения значений частоты (иными словами, метод биений) менее эффективен, однако более прост в реализации. Построенные с его использованием металлоискатели компактны, не требуют тщательной настройки и мер по жесткой стабилизации частоты, неприхотливы в эксплуатации, благодаря чему и получили широкое распространение.

Предлагаемые вашему вниманию устройства выполнены на доступной элементной базе и могут быть с успехом использованы не только при оборудовании тайников, но и в строительстве, коммунальном хозяйстве, для поиска скрытых под слоем земли мусора или снега, люков и крышек колодцев, решеток водостока и т. п. Кроме того, эти приборы можно с успехом использовать для обнаружения тайников и скрытых металлических предметов.

Металлоискатель на одной микросхеме

Металлоискатель, принципиальная схема которого изображена на рис. 5.13, собран всего на одной микросхеме К176ЛП2. Один из ее элементов *(DD1.1)* использован в образцовом генераторе, другой *(DD1.2)* — в перестраиваемом. Колебательный контур образцового генератора состоит из катушки *L1* и конденсаторов *C1*, *C2*, а перестраиваемого — из поисковой катушки *L2* и конденсатора *C4*; первый перестраивают переменным конденсатором *C1*, второй — подбором емкости конденсатора *C4*.

На элементе *DD1.3* выполнен смеситель колебаний образцовой и переменной частот. С нагрузки этого узла — переменного резистора *R5* — сигнал разностной частоты поступает на вход элемента *DD1.4*, а усиленное им напряжение звуковой частоты — на головные телефоны *BF1.*

Прибором можно обнаружить пятикопеечную монету (доперестроечную денежную единицу) на глубине до 60 мм. А крышку канализационного колодца — на глубине до 0,6 м.

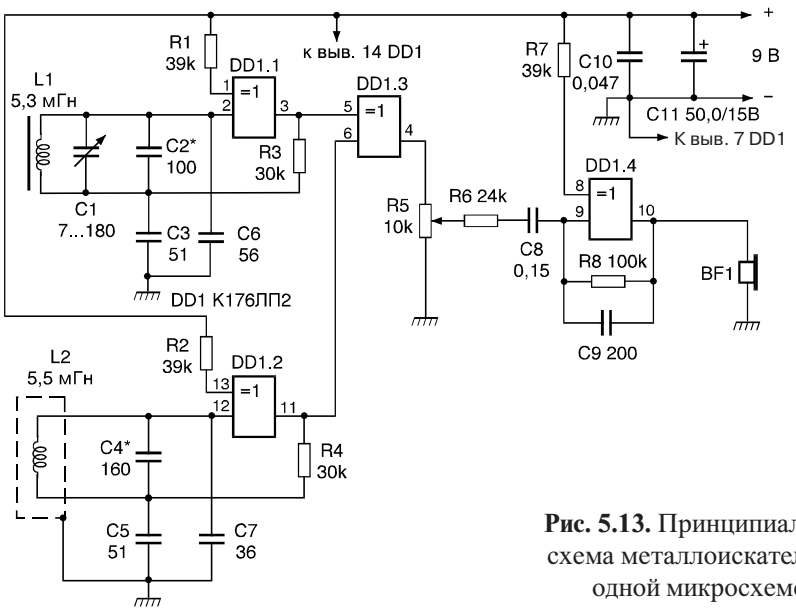


Рис. 5.13. Принципиальная схема металлоискателя на одной микросхеме

Металлоискатель на двух микросхемах

Несколько большей чувствительностью обладает металлоискатель, собранный по схеме, приведенной на рис. 5.14. Здесь в качестве смесителя и усилителя колебаний разностной частоты применена микросхема К118УН1Д. Образцовый и перестраиваемый генераторы этого прибора также идентичны по схеме, каждый из них выполнен на двух инверторах (DD1.1, DD1.2 и DD2.1, DD2.2 соответственно), элементы DD1.3 и DD2.3 — буферные (ослабляют влияние смесителя на генераторы). Образцовый генератор настраивают на заданную частоту переменным конденсатором *C1*, перестраиваемый — подбором емкости конденсатора *C2*.

Металлоискатель повышенной чувствительности

Повысить чувствительность металлоискателя, в котором использован метод биений, можно, настроив образцовый генератор на частоту в 5—10 раз большую, чем частота перестраиваемого. В этом случае возникают биения между колебаниями образцового генератора и ближайшей по частоте (5—10-й) гармоникой перестраиваемого генератора. Расстройка последнего, скажем, всего на 10 Гц приводит к увеличению частоты разностных колебаний на 50—100 Гц.

Именно таким способом достигнута повышенная чувствительность прибора, схема которого изображена на рис. 5.15. Пятикопеечную монету с его помощью можно обнаружить на глубине до 100 мм, а крышку колодца — на глубине до 0,65 м.

Образцовый генератор металлоискателя выполнен на двух элементах микросхемы *DD2* и настроен на частоту 1 МГц. Требуемую стабильность частоты обеспечивает кварцевый резонатор *ZQ1*.

В перестраиваемом генераторе использованы два элемента микросхемы *DD1*. Его колебательный контур *L1C2*С3*VD1* настроен на частоту в несколько раз меньшую, чем образцовый генератор. Для настройки контура использован варикап *VD1*, напряжение на котором регулируют переменным резистором *R2*.

Смеситель выполнен на элементе *DD1.4*, в качестве буферных использованы элементы *DD1.3* и *DD2.3*.

Как и в обеих предыдущих конструкциях, индикатором поиска служат головные телефоны *BF1*.

Каждый из металлоискателей (два предыдущих и рассматриваемый) смонтирован на печатной плате из фольгированного стеклотекстолита толщиной 1,5 мм. Платы рассчитаны на установку постоянных резисторов МЛТ-0,125 (МЛТ-025, ВС-0,125), конденсаторов КТ-1 (*C2—C7* — в первом; *C2*, *C5—C8* — во втором; *C2*, *C3*, *C5—C7* — в третьем), КМ-4 или К-10-7В (соответственно *C8—C10; C3, C4, C9—C12, C15, C16; C2, C3, C5—C7*) и К50-6 (остальные).

Для перестройки генераторов по частоте применены переменные конденсаторы с твердым диэлектриком от малогабаритных транзисторных приемников «Мир» (в первом устройстве) и «Планета» (во втором). Разумеется, воз-

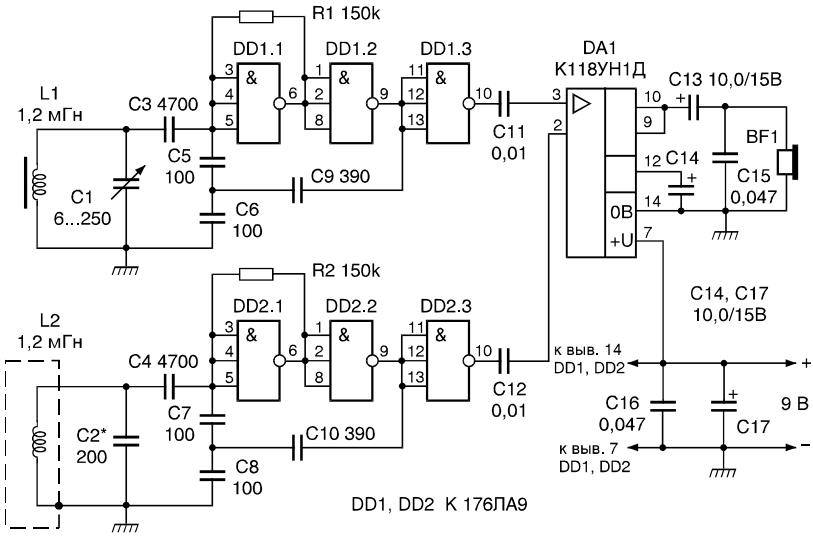


Рис. 5.14. Принципиальная схема металлоискателя на двух микросхемах

можно использование и любых других подходящих по габаритам и значениям минимальной и максимальной емкости конденсаторов, в том числе и подстроечных КПК-3 емкостью 25—150 пФ.

Переменные резисторы *R5* (рис. 5.13) и *R2* (рис. 5.15) — малогабаритные любого типа.

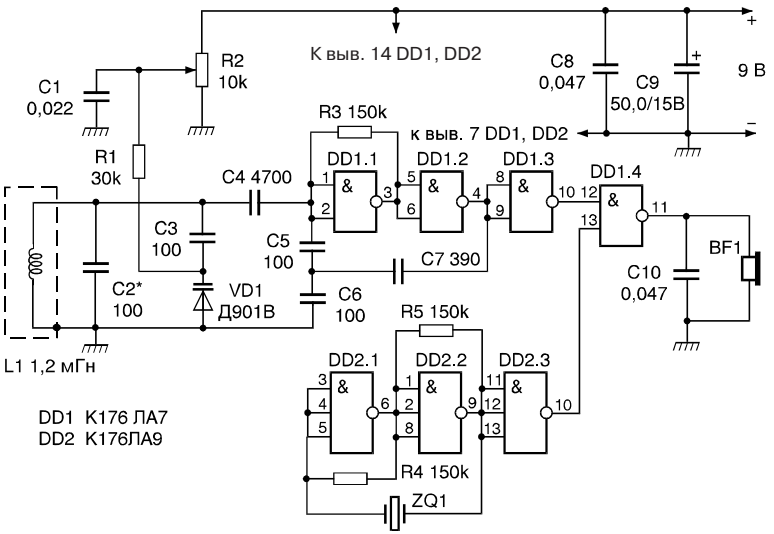


Рис. 5.15. Принципиальная схема металлоискателя повышенной чувствительности

С целью уменьшения размера смонтированных плат по высоте оксидные конденсаторы *C11* первого металлоискателя и *C9* третьего установлены параллельно платам (их выводы согнуты под углом 90°). Кварцевый резонатор смонтирован на отдельной плате из стеклотекстолита, закрепленной параллельно основной со стороны деталей.

Катушки *L1* металлоискателей, собранных по схемам на рис. 5.13 и 5.14, намотаны на ферритовых (600НН) кольцевых магнитопроводах типоразмера К8′6′2. В первом катушка содержит 180 витков провода ПЭЛШО 0,14 мм, во втором — 50 витков ПЭЛШО 0,2 мм. Намотка в обоих случаях — равномерная по всему периметру магнитопровода. В первом устройстве катушка приклеена клеем БФ-2 непосредственно к печатной плате, во втором (из-за недостатка места) — к небольшому уголку, согнутому из листового полистирола толщиной 1,5 мм и приклеенному этим же клеем к плате.

Поисковая катушка каждого из трех металлоискателей намотана в кольце, согнутом из винилопластовой трубки внешним диаметром 15 и внутренним 10 мм. Наружный диаметр кольца первого прибора — 250 мм, второго и третьего — 200 мм, количество витков — соответственно 100 и 50, провод — ПЭЛШО 0,27 мм. После намотки кольцо обернуто лентой из алюминиевой фольги для электрического экранирования (необходимого для устранения влияния емкости между катушкой и землей). При намотке ленты следует помнить, что электрический контакт между ее концами недопустим (в противном случае образуется замкнутый виток).

Для защиты от повреждений фольгу обматывают одним-двумя слоями поливинилхлоридной изоляционной ленты.

Следует отметить, что диаметр поисковой катушки может быть как меньше, так и больше указанных значений. С его уменьшением площадь зоны обнаружения сужается, но прибор становится более чувствительным к мелким предметам, с увеличением же, наоборот, зона обнаружения расширяется, а чувствительность к мелким предметам снижается. Для индикации поиска во всех приборах применены головные телефоны ТОН-2.

Питать металлоискатели можно от батареи «Крона» или 7Д-0,115, а если не смущают габариты, то и от соединенных последовательно двух батарей 3336 или шести элементов 316, 332.

Вместе с источником питания смонтированную плату и органы управления помещают в небольшую плоскую металлическую коробку (латунь, луженая жесть толщиной 0,4—0,6 мм) и закрепляют последнюю на штанге, изготовленной из дюралюминиевой трубы внешним диаметром 16—20 мм.

Универсальный металлоискатель

Металлоискатели, о которых рассказывалось ранее, рассчитаны на обнаружение в основном сравнительно больших металлических предметов на расстоянии нескольких десятков сантиметров. С их помощью практически невозможно определить точное местоположение, скажем, гвоздей, скрытой про-

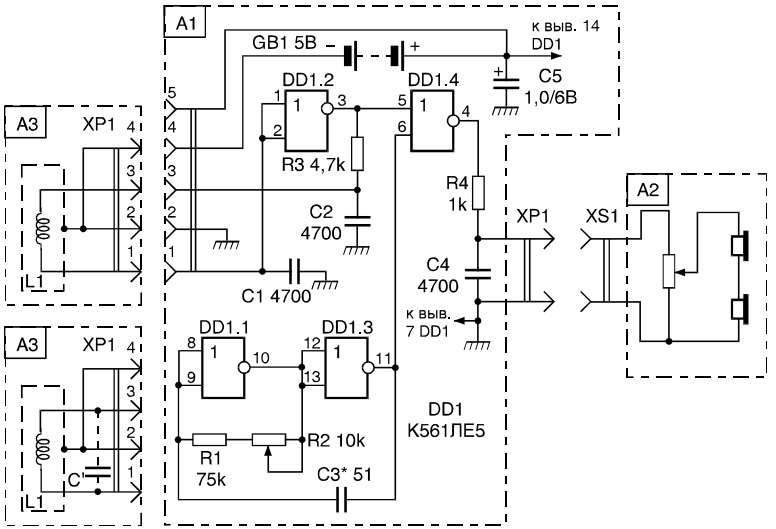


Рис. 5.16. Принципиальная схема универсального металлоискателя

водки в стене или полу, поскольку разрешающая способность металлоискателя низка из-за громоздкости выносной катушки (диаметр 200 мм). К примеру, с такой катушкой группа близко расположенных гвоздей может восприниматься как некий большой предмет из металла. Кроме того, более удаленные массивные предметы могут экранировать близлежащие мелкие, например те же гвозди в деревянном настиле на железобетонных плитах. На рис. 5.16 представлен универсальный металлоискатель, способный обнаруживать как мелкие, так и крупные металлические предметы. Он снабжен несколькими сменными катушками диаметром от 25 до 250 мм, что позволяет обнаруживать местоположение мелких предметов с точностью до миллиметра на расстоянии нескольких сантиметров, а крупные предметы — на расстоянии нескольких десятков сантиметров.

Принцип работы металлоискателя — традиционный. Он содержит эталонный генератор, собранный на логических элементах *DD1.1* и *DD1.3* с частотой генерации примерно 100 кГц, и перестраиваемый генератор, выполненный на элементе *DD1.2* и одной из выносных катушек индуктивности, подключаемых к генератору через разъем *XS1*. Сигналы обоих генераторов поступают на смеситель, собранный на элементе *DD1.4*. К выходу смесителя через фильтр *R4C4,* ослабляющий высшие частоты, подключены головные телефоны (узел *A2*). Для получения большей громкости звука капсюли телефонов соединены последовательно.

Пока вблизи выносной (сменной или поисковой) катушки нет металла, в телефонах будет звук вполне определенной тональности, установленной переменным резистором *R2*. При приближении же катушки к металлическому предмету тональность звука будет изменяться. Металлоискатель питается от батареи

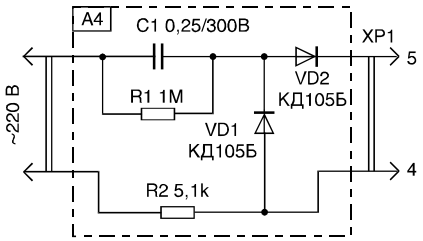


Рис. 5.17. Принципиальная схема зарядного устройства для металлоискателя

GB1, но выключателя питания в ее цепи нет — питающее напряжение подается на микросхему через контакты *2, 4* при подключении сменной катушки.

Кроме указанной на схеме можно применить микросхемы К561ЛА7, К561ЛА7, К564ЛЕ5. Постоянные резисторы — МЛТ-0,125, переменный *R2* — СП5-2 или другой малогабаритный. Оксидный конденсатор *C5* может быть К50-6, К53-1, остальные конденсаторы — КЛС, КМ. Головные телефоны — ТОН-2А с регулятором громкости. Их нужно немного доработать: установить на корпусе регулятора громкости гнездо *XS2* от малогабаритных телефонов (в это гнездо вставляют вилку *XP2* от таких же телефонов), удалив предварительно провод с вилкой. И, конечно, соединить капсюли последовательно.

Источник питания, батарею *GB1*, составляют из четырех последовательно соединенных аккумуляторов Д-0,1 или Д-0,06. Поскольку аккумуляторы со временем истощаются, для подзарядки батареи используют простое зарядное устройство (узел *A4* на рис. 5.17), включаемое в разъем *XS1* с помощью пятиштырьковой вилки.

Детали узла *A1* металлоискателя, кроме разъемов, батареи и переменного резистора, смонтированы на небольшой печатной плате, которая вместе с батареей аккумуляторов размещена в небольшом корпусе — коробке из-под лекарств. На крышке коробки крепят разъем, а через отверстие в дне пропускают двухпроводный шнур, концы проводов которого припаивают к разъему *XP2*. Переменный резистор *R2* крепят на боковой стенке коробки.

Сменные катушки диаметром до 100 мм изготавливают так. Сначала на оправке необходимого диаметра наматывают обмотку, которую обматывают слоем лакоткани, а поверх — медной луженой фольгой. Начало и конец обмотки из фольги не должны касаться друг друга, поэтом между ними оставляют зазор в несколько миллиметров.

Затем из фольгированного материала изготавливают основание в виде диска, на котором пайкой крепят разъем. С внутренней стороны на основании оставляют на краю кольцевую фольгированную полоску, не замкнутую на концах, а также полоску-проводник к разъему (с этой полоской соединяют контакты *2* и *4* разъема; см. рис. 5.16). К основанию припаивают фольговую обмотку катушки так, чтобы зазоры обмотки и кольцевой полоски основания совпали. В случае необходимости на основании размещают конденсатор *C′*, выводы которого подпаивают к выводам *3* и *1* разъема, т. е. подключают параллельно катушке индуктивности.

После проверки катушки (омметром) и подбора конденсатора *C1* (при налаживании металлоискателя) припаивают крышку из фольгированного материала, изготовленную наподобие основания с незамкнутой кольцевой полоской.

Катушки диаметром 100 мм и более можно изготовить аналогично описанным выше и соединять их с металлоискателем с помощью кабеля (обязательно экранированного) длиной 1,5—2 м. Индуктивность любой катушки должна быть примерно 1,25 мГн.

Для катушки диаметром (средним) 25 мм обмотка должна содержать 150 витков провода ПЭВ-1 0,1; диаметром 75 мм — 80 витков ПЭВ-1 0,18; диаметром 200 мм — 50 витков ПЭВ1 0,3. Для катушек любого другого диаметра количество витков приближенно определяют по формуле:

$$W = \sqrt{\frac{L}{0{,}025D}},$$

где W — количество витков; L — индуктивность катушки, мкГн; D — средний диаметр катушки, см.

Настраивают металлоискатель в такой последовательности. После изготовления одной из сменных катушек, например самой малогабаритной, ее подключают к разъему *XS1*. Движок резистора *R2* устанавливают в среднее положение и, подключив головные телефоны, подбором конденсатора *C3* добиваются звука низкого тона в них. При приближении к катушке металлического предмета тональность звука должна изменяться. Затем изготавливают катушку другого диаметра и, не припаивая крышку, подключают катушку к разъему *XS1*. Желательно, чтобы индуктивность катушки получилась на 5—10 % меньше ранее изготовленной. Подбором конденсатора *C1* (если это понадобится) добиваются звука примерно такой же тональности, что и в первом случае.

Аналогично изготавливают и настраивают катушки других размеров.

При зарядке батареи аккумуляторов необходимо помнить о правилах безопасности и не касаться токопроводящих частей устройства, например вилки *XP2*. Чтобы сделать этот процесс более безопасным, можно воспользоваться для зарядки сетевым блоком питания с выходным напряжением 9—12 В и подключать его к батарее *GB1* (через контакты *4, 5* разъема *XS1*) через резистор сопротивлением 470—510 Ом.

Использование специальной техники при проверках помещений

Из детективной литературы хорошо известно, что преступник всегда оставляет следы. Так же и любое техническое устройство вносит какие-то изменения в окружающее пространство.

И если задача разведки состоит в том, чтобы сделать эти изменения как можно более незаметными, то задача тех, кто занят поиском подобной техники, состоит в том, чтобы по едва уловимым следам изменения физических параметров пространства обнаружить и обезвредить технические устройства и

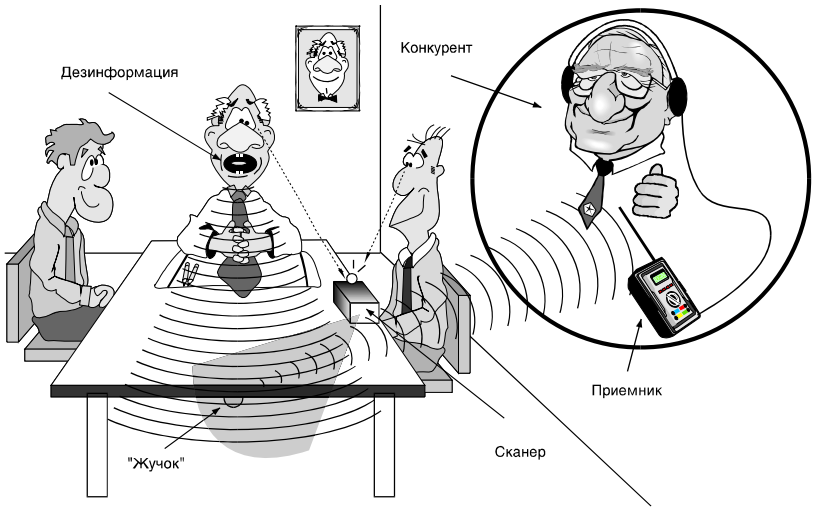


Рис. 5.18. Поведение во время беседы

системы ведения разведки. Задача технической контрразведки усложняется тем, что, как правило, неизвестно, какое конкретное техническое устройство контроля информации применено. Поэтому работа по поиску и обезвреживанию технических средств наблюдения дает обнадеживающий результат только в том случае, если она проводится комплексно, т. е. обследуют одновременно все возможные пути утечки информации.

Приведем достаточно условную классификацию устройств поиска технических средств разведки.

I. Устройства поиска активного типа, т. е. исследующие отклик на какое-либо воздействие:

- нелинейные локаторы исследуют отклик на воздействие электромагнитным полем;
- рентгенметры просвечивают с помощью рентгеновской аппаратуры;
- магнитно-резонансные локаторы используют явление ориентации молекул в магнитном поле;
- акустические корректоры.

II. Устройства поиска пассивного типа:

- металлоискатели;
- тепловизоры;
- устройства и системы поиска по электромагнитному излучению;
- устройства поиска по изменению параметров телефонной линии (напряжения, индуктивности, емкости, добротности);
- устройства поиска по изменению магнитного поля (детекторы записывающей аппаратуры).

В силу различных причин практическое применение нашли далеко не все из перечисленных технических средств. Например, рентгеновская аппаратура очень дорога и громоздка и применяется исключительно специальными государственными организациями. То же, но в меньшей степени, относится к магнитно-резонансным локаторам. Тепловизоры, приборы, которые могут обнаруживать разницу температур, измеряемую сотыми долями градуса, могут регистрировать тепловую мощность порядка 1 мкВт. Эти относительно дешевые приборы, в состав которых входит компьютер, могли бы стать очень эффективными и универсальными с точки зрения поиска технических средств коммерческой разведки, так как любое техническое средство при своей работе выделяет в окружающее пространство тепло. Скорее всего, появление на рынке подобных устройств является делом недалекого будущего.

Для противодействия конкурирующим фирмам и преступным группам необходимо прежде всего определить порядок ведения деловых бесед по телефону; определить круг лиц, допускаемых к тем или иным секретам; запретить сотрудникам вести служебные разговоры по домашним телефонам. Для передачи материалов, содержащих коммерческую тайну, использовать только устойчивые каналы связи (с нарочным, с использованием компьютерных шифраторов).

Если вы почувствовали, что за вами установлен контроль (рис. 5.18), во время беседы используйте систему условностей и сознательной дезинформации. Никогда не называйте фамилию, отчество собеседника, если это позволяет этикет. Назначая место и время встречи, переходите на условности, которые должны органически вписываться в контекст вашего разговора. Приучите к определенному порядку ведения телефонных переговоров членов вашей семьи: они не должны сообщать никому о том, где вы находитесь и когда вернетесь домой. При шантаже преступными группами не пытайтесь тотчас же звонить в милицию. Целесообразно «взять паузу» и, убедившись, что за вами нет слежки, позвонить с телефона-автомата в соответствующую организацию, причем лучше всего, чтобы это сделал ваш друг и, не называя истинной причины, организовал встречу (помните, что телефоны милиции тоже могут прослушиваться).

Литература

1. **Алексеенко В. Н., Сокольский Б. Е.** Система защиты коммерческих объектов// Технические средства защиты.— М., 1992.
2. **Андрианов В. И., Бородин В. А., Соколов А. В.** «Шпионские штучки» и устройства для защиты объектов и информации. — СПб.: Лань, 1996. — 272 с.
3. **Андрианов В. И., Соколов А. В.** «Шпионские штучки», или Как сберечь свои секреты. — СПб.: Полигон, 1997. — 272 с.
4. **Андрианов В. И., Соколов А. В.** Средства мобильной связи. — СПб.: BHV— Санкт-Петербург, 1998. — 256 с.
5. **Атражев М. П.** и др. Борьба с радиоэлектронными средствами.— М.: Воениздат, 1972. — 272 с.
6. **Барсуков В. С., Дворянкин С. В., Шеремет И. А.** Безопасность связи в каналах телекоммуникаций — М.: НИФ «Электронные знания», 1992.
7. **Батурин Ю. М., Жодзишский А. М.** Компьютерная преступность и компьютерная безопасность. — М.: Юрид. лит., 1991. — 160 с.
8. **Безруков Н. Н.** Компьютерная вирусология: Справ. руководство. — К.: УРЕ, 1991.— 416 с.
9. **Бержье Ж.** Промышленный шпионаж.— М.: Международные отношения, 1972.
10. **Бертсекас Д., Галлагер Р.** Сети передачи данных. — М.: Мир, 1989. — 542 с;. Бизнес и безопасность.— М.: КМЦ «Центурион», 1992.
11. **Вакин С. А., Шустов Л. Н.** Основы радиопротиводействия радиотехнической разведке.— М.: Сов. радио, 1968.
12. **Вартанесян В. А.** Радиоэлектронная разведка.— М.: Воениздат, 1991.— 255 с.
13. **Волин М. Л.** Паразитные связи и наводки.— М.: Сов. радио, 1965. — 296 с.
14. **Гавриш В.** Практическое пособие по защите коммерческой тайны.— Симферополь, «Таврида», 1994.
15. **Гайкович В. Ю., Ершов Д. В.** Основы безопасности информационных технологий. — М.: МИФИ, 1995. — 365 с.
16. **Галлагер Р.** Теория информации и надежная связь. — М.: Сов. радио, 1974. — 534 с.
17. **Герасименко В. А.** Защита информации в АСОД. — М.: Энергоатомиздат, 1994.
18. **Герасименко В. А., Размахнин М. К.** Криптографические методы в автоматизированных системах//Зарубежная радиоэлектроника. 1982. № 8. — С. 97— 124.
19. **Гроувер Д.** и др. Защита программного обеспечения. — М.: Мир, 1992.
20. **Давыдовский А. И., Максимов В. А.** Введение в защиту информации// Интеркомпьютер. 1990. №1.
21. **Жельников В.** Криптография от папируса до компьютера. — М.: ABF, 1997. — 336 с.

22. **Замарин А., Андреев А., Ковалевский В.** Битва за информацию. Стратегия защиты//Безопасность. Достоверность. Информация. 1995. №2. — С. 21—23.
23. Защита информации в компьютерных системах//Под ред. Шмакова Э.М. — СПб.: СПбГТУ, 1993. — 100 с.
24. **Иванов В., Залогин Н.** Активная маскировка побочных излучений вычислительных систем/Компьютер Пресс. 1993. № 10.
25. **Касперский Е.** Компьютерные вирусы в MS-DOS. — М.: Эдэль, 1992. — 176 с.
26. **Каторин Ю. Ф., Куренков Е. В., Лысов А. В., Остапенко А. Н.** Энциклопедия промышленного шпионажа/Антишпионские штучки. — СПб.: Полигон, 1999.— 512 с.
27. **Кащеев В. И.** Мониторинг телефонной сети//Системы безопасности. 1995. № 1; **Киселев А. Е.** и др. Коммерческая безопасность.— М.: Инфо Арт, 1993.
28. **Ковалевский В. Э., Максимов В. А.** Криптографические методы// Компьютер Пресс. 1993. №5.—С. 31—34.
29. Лаборатория спецтехники. Каталог, 1994.
30. **Лысов А. В., Остапенко А. Н.** Промышленный шпионаж в России: методы и средства.— СПб., Бум Техно, 1994.
31. **Лысов А. В., Остапенко А. Н.** Телефон и безопасность.— СПб., Лаборатория ППШ, 1995.
32. **Максимов Ю. Н.** и др. Организационно-технические методы контроля защиты информации в объектах ЭВТ: Учебное пособие. — СПб.: ВИККА, 1994. — 77 с.
33. **Мельников В. В.** Защита информации в компьютерных системах.— М., Финансы и статистика, 1997. — 364 с.
34. **Миронычев С.** Коммерческая разведка и контрразведка, или Промышленный шпионаж в России и методы борьбы с ним.— М.: Дружок, 1995.
35. **Михайлов А. С.** Измерение параметров ЭМС РЭС.— М.: Связь, 1980.— 200 с.
36. **Наумов А.** Алло! Вас подслушивают//Деловые люди, 1992.
37. **Никулин О. Ю., Петрушин А. Н.** Системы телевизионного наблюдения.— М.: «Оберег РБ», 1997; Предпринимательство и безопасность/Под ред. Долгополова Ю. Б.— М.: Универсум, 1991; **Сапожников М. А.** Электроакустика.— М.: Связь, 1978.
38. Терминология в области защиты информации: Справочник. — М.: ВНИИ стандарт, 1993. — 49 с.
39. Технические средства разведки/Под ред. Мухина В. И.—М.: РВСН, 1992; Технический шпионаж и борьба с ним.— Минск: ТГО, 1993.
40. Технология электронных коммуникаций. Безопасность в телекоммуникационных сетях. — М., 1992, т. 20.
41. **Хори Д.** Усовершенствуй свой телефон/Пер. с англ.— М.: БИНОМ, 1995. — 305 с.
42. **Хофман Л. Д.** Современные методы защиты информации.— М.: Сов. радио, 1980.
43. **Гурвич И. С.** Защита ЭВМ от внешних помех.— М.: Энергоатомиздат, 1984.
44. **Ярочкин В.** Проблемы информационной безопасности//Частный сыск и охрана. 1993. № 9.
45. **Ярочкин В. И.** Технические каналы утечки информации.— М.: ИПКИР, 1994.