14. УЯЗВИМОСТИ СОВРЕМЕННЫХ ТЕХНИЧЕСКИХ СРЕДСТВ СВЯЗИ

14.1. Радиотелефоны

Стационарный беспроводный радиотелефон объединяет в себе обычный проводной 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 может достигать 3 км.

При работе радиотелефоны 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.

Сложнее перехватить информацию с цифровых радиотелефонов, которые могут использовать при работе от 10 до 30 частот с автоматической их сменой по определенному закону. Однако для специалиста и такой перехват не представляет особой трудности.

14.2. Мобильные телефоны и смартфоны

Мобильные телефоны сотовой связи фактически являются сложной миниатюрной приемо-передающей радиостанцией. При изготовлении каждому сотовому телефонному аппарату присваивают электронный серийный номер, кодируемый в микрочипе телефона, который затем изготовители аппаратуры сообщают специалистам, обслуживающим сотовый телефон. Кроме того, некоторые изготовители указывают этот номер в руководстве 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 обладает большой, а иногда и неограниченной, дальностью действия, которую обеспечивает сотовая структура зон связи. Вся территория, обслуживаемая сотовой системой связи, разделена на прилегающие друг к другу зоны связи, или соты. Телефонный обмен в каждой такой соте управляется базовой станцией, способной принимать и передавать сигналы на многих радиочастотах. 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, за счет чего 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 осуществляются идентификация

конкретного сотового телефона, номера счета его владельца и привязка аппарата к определенной зоне, в которой он находится в данный момент. 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.

К сожалению, бытует мнение, что сотовые радиотелефоны обеспечивают высокую безопасность передачи информации, поскольку каждый выход на 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 компьютером. 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.

Важно знать, что еще на этапе разработки закладываются следующие возможности любой аппаратуры сотовой связи:

— представление информации о точном местоположении абонента;

— запись и прослушивание разговоров;

— фиксация номеров, даты, времени, категории и т. д. вызывающей и принимаю щей вызов стороны;

— дистанционное включение микрофона для прослушивания.

Немногие знают, что наличие мобильного сотового телефона позволяет определить не только текущее местоположение владельца, но и проследить за всеми его перемещениями.

Текущее положение может выявляться двумя способами. Первый из них — обычный метод триангуляции (пеленгования), определяющий направление на работающий передатчик из нескольких (обычно трех) точек и дающий засечку местоположения источника радиосигналов. Необходимая для этого аппаратура обладает высокой точностью и вполне доступна.

Второй метод — через компьютер предоставляющей связь компании, который постоянно регистрирует, где находится абонент в данный момент даже тогда, когда он не ведет никаких разговоров (но идентифицирующим служебным сигналам, автоматически передаваемым телефоном на базовую станцию, о которых мы говорили выше). Точность определения местонахождения абонента в этом случае зависит от следующих 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. 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 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, а также находился 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), информация, передаваемая по сотовой сети, становится легкой добычей для разного рода хакеров и проходимцев.

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. 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 нужна сложная аппаратура. Разговор, ведущийся с сотового телефона, можно прослушать с помощью программируемых приемников-сканеров с полосой приема 30 кГц, способных осуществлять поиск в диапазоне 450-1900 МГц.

Перехватывать информацию с аналоговых неподвижных и стационарных сотовых телефонов легко, с мобильных — труднее, 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 телефона (телефонные номера, номера кредитных карточек или персональные идентификационные номера), то их легко перехватить с помощью того же цифрового сканера.

С развитием технологий беспроводной передачи данных и мобильного доступа в Internet современные сотовые телефоны приобретают свойства персональных компьютеров. В ряде мобильных телефонов имеется своя операционная система, текстовые редакторы, базы данных. Все это дает пользователям возможность создавать файлы и обмениваться ими. С помощью телефонных аппаратов становятся возможными ведение банковских операций, совершение интерактивных покупок, обмен электронными данными.

14.3. Паразитная генерация в узлах технических средств

Паразитная генерация в узлах технических средств, например, в усилителях звуковой частоты различных систем (громкоговорящей связи, систем перевода с иностранного языка и др.

Паразитные высокочастотные колебания в усилителях возникают при образовании между выходом и входом усилителя положительной обратной связи. При попадании через паразитные емкостные и индуктивные связи на вход усилителя сигналов с его выхода с фазой, равной фазе входного сигнала (положительная обратная связь), лавинообразно нарастает амплитуда паразитного колебания на частоте, на которой выполняется равенство фаз. Такая связь возникает за счет конструктивных особенностей схемы или за счет старения элементов.

Если частота паразитной генерации расположена вне диапазона частот усилителя, то этот побочный режим работы усилителя может остаться незамеченным при создании и эксплуатации радиоэлектронного средства.

Самовозбуждение может возникнуть и при отрицательной обратной связи из-за того, что на частоты, где усилитель вместе с цепью обратной связи вносит сдвиг фазы на 180°, отрицательная обратная связь превращается в положительную.

Частота самовозбуждения модулируется акустическим сигналом, поступающим на усилитель, и излучается в эфир как обычным радиопередатчиком. Дальность распространения такого сигнала определяется мощностью усилителя (т.е. передатчика) и особенностями диапазона радиоволн. В качестве защитных мер применяется контроль усилителей на самовозбуждение с помощью радиоприемников типа индикаторов поля, работающих в достаточно широком диапазоне частот, что обеспечивает поиск опасного сигнала.

14.4. Подслушивание с помощью акусто-оптикоэлектронных преобразователей

Лазерные акустические системы разведки (ЛАСР)

Акусто-оптикоэлектронные преобразователи являются основой лазерных акустических систем разведки (ЛАСР), иногда называемых «лазерными микрофонами». Существуют несколько схем построения ЛАСР.

На рис. 14.18 изображен простейший вариант подобной системы. Луч лазера падает на стекло окна под некоторым углом. На границе стекло − воздух происходит модуляция луча звуковыми колебаниями. Отраженный луч улавливается фотодетектором, расположенном на оси отраженного луча, и

осуществляется амплитудная демодуляция отраженного излучения. Система довольно простая, но требует тщательной юстировки и на практике используется довольно редко.

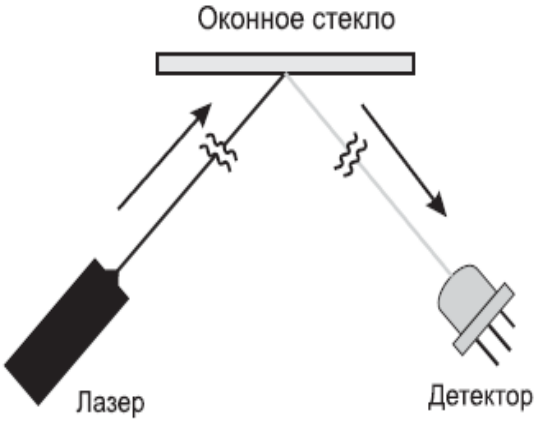

Рисунок 14.18

Второй способ, использующий сплиттер (делитель) пучка, несколько сложнее, но он позволяет совместить лазер и детектор (рис. 14.19). Отпадает необходимость в тщательной юстировке системы. Применение сплиттера позволяет свести падающий и отраженный луч в одну точку.

Принцип работы ЛАСР для систем с разделением луча (Single Split beam) можно представить следующим образом: когерентный луч лазера расщепляется разделительным стеклом (особое стекло со специальным покрытием толщиной в десятки нанометров пропускает 50% и отражает 50% света определенной длины волны) на 2 части: опорный луч и излучаемый. При отражении излучаемого луча от оконного стекла или триппель-призмы, установленной на нем, происходит его модуляция звуковой частотой. Отраженный промодулированный луч направляется на фоторезистор, где интерферирует с опорным лучом. Сигнал с фоторезистора после специальной обработки усиливается и подается для прослушивания на головные телефоны или записывается на цифровой диктофон.

В некоторых ЛАСР используется интерференционная схема, представленная на рис. 14.20.

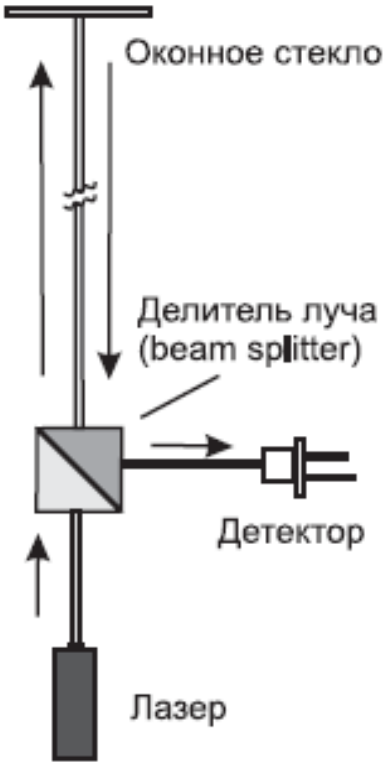

Рисунок 14.19

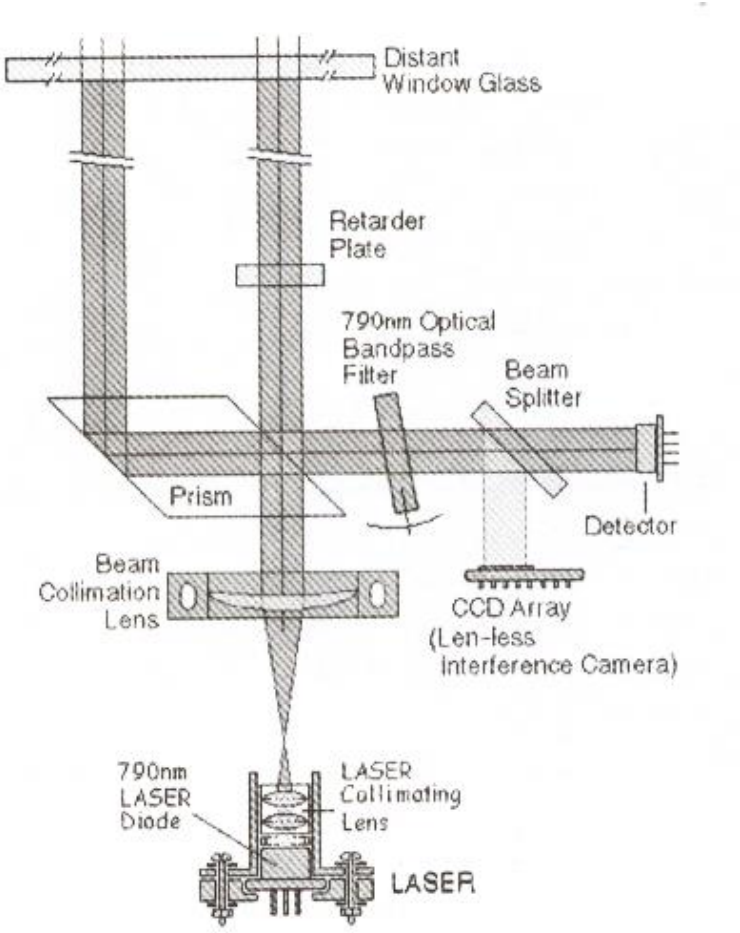

Рис. 14.20

Особенность этой схемы – дифференциальный метод измерения акустической вибрации. Участок оконного стекла, с которого снимается вибрация, имеет малый размер, следовательно, резко ослабляется синфазная помеха, вызываемая низкочастотными колебаниями стекла, например, из-за ветра или уличных шумов.

В целях обеспечения скрытности работы в ЛАСР используются лазеры, работающие в ближнем инфракрасном, не видимом глазу диапазоне длин волн (0,75 – 1,1 мкм).

Дальность действия лазерных акустических систем разведки при приеме диффузно отраженного излучения не превышает нескольких десятков метров. При приеме зеркально отраженного луча дальность разведки может составлять несколько сот метров. Основные характеристики некоторых ЛАСР приведены в табл. 14.10

Таблица 14.10

Характеристика	Тип системы		
	LASR-2000	Laser-3500	MR-7800
Лазерный передатчик			
Тип лазера	полупроводниковый		
Длина волны, мкм	0,75 – 0,84	1,75 – 1,84	0,77 – 0,84
Мощность излучения, мВт	5	5	25
Фокусное расстояние объектива, мм	135	135	135
Питание, В	8×1,5 (AA)	8×1,5 (AA)	8×1,5 (AA)
Время работы, ч	50	40	40
Приемник лазерного излучения			
Тип приемника	малошумящий PIN-диод; ближний ИК		
Фокусное расстояние объектива, мм	500	500	500
Питание, В	9	12	12
Время работы, ч.	15 – 30	15 – 50	40 – 60
Примечание	камуфлируется под стандартную зеркальную камеру; габариты 470×380×220 мм; масса 10,5 кг без батарей и треног		

14.5. Подслушивание с помощью высокочастотного навязывания

Технический канал утечки информации путем “*высокочастотного навязывания*” может быть осуществлен путем: 1) несанкционированного контактного введения токов высокой частоты от соответствующего генератора в линии (цепи), имеющие функциональные связи с нелинейными или параметрическими элементами ТС, на которых происходит модуляция высокочастотного сигнала информационным; 2) электромагнитного облучения цепей, характеристики которых изменяются под действием акустической волны. Это дистанционное ВЧ-воздействие на элементы технических средств.

При использовании первого способа, информационный сигнал в нелинейных и параметрических элементах ТС появляется вследствие электроакустического эффекта - преобразования акустических сигналов в электрические. В силу того, что нелинейные или параметрические элементы ТС для высокочастотного сигнала, как правило, представляют собой несогласованную нагрузку, промодулированный высокочастотный сигнал будет отражаться от нее и распространяться в обратном направлении по линии или излучаться. Для приема излученных или отраженных высокочастотных сигналов используется специальные приемники с достаточно высокой чувствительностью. Для исключения влияния зондирующего и переотраженного сигналов могут использоваться импульсные сигналы, в результате происходит их разделение во времени. Примером такого воздействия может служить схема (рис. 14.12). Этот способ состоит в следующем.

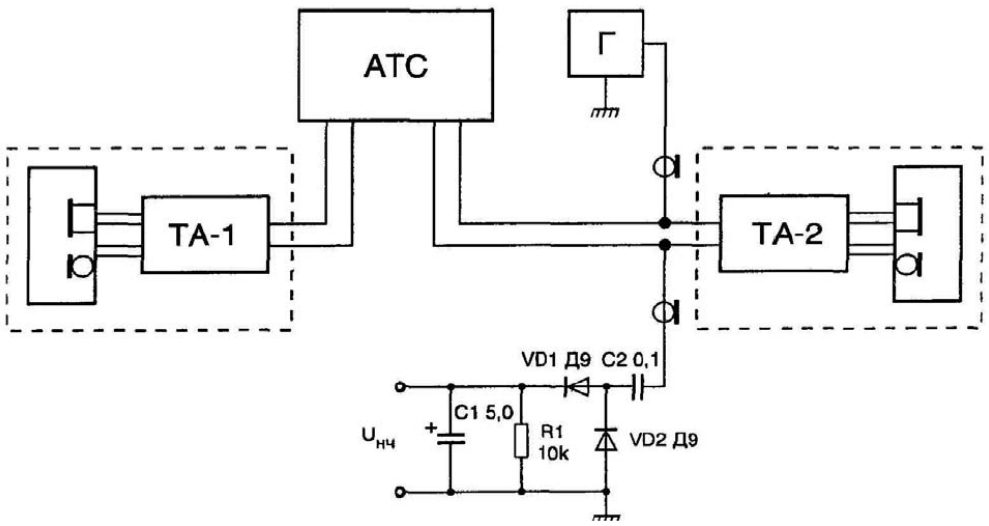

Рис. 14.12. Схема прослушивания помещения высокочастотным навязыванием

На один из проводов телефонной линии, идущий от АТС к телефонному аппарату ТА-2, подаются колебания частотой 150 кГц и выше от генератора Г. К другому проводу линии подключается детектор, выполненный на элементах С1, С2, VD1, VD2 и R1. Корпус передатчика (генератор Г) и приемника (детектор) соединены между собой или с общей землей, например с водопроводной трубой.

Наиболее часто такой канал утечки информации используется для перехвата разговоров, ведущихся в помещении, через телефонный аппарат, имеющий выход за пределы контролируемой зоны. Для исключения воздействия высокочастотного сигнала на аппаратуру АТС в линию, идущую в ее сторону, устанавливается специальный высокочастотный фильтр.

Недостаток этого метода состоит в том, что его случайно может обнаружить всякий, кто позвонит по тому же номеру, а также необъяснимая занятость контролируемой линии для других абонентов.

Другой способ - дистанционное ВЧ-воздействие на цепи охранной и пожарной сигнализации. Такое воздействие осуществляется с помощью внешнего источника излучения электромагнитных волн.

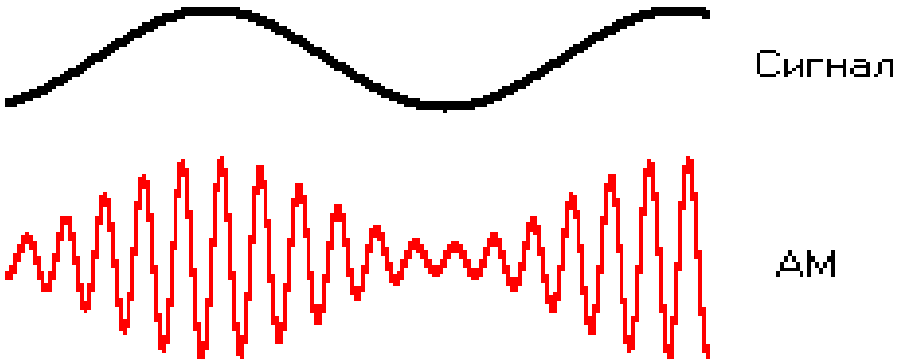

Рис. 14.13

Дистанционное ВЧ-воздействие на полуактивные радиозакладки

Примером полуактивного закладного устройства может служить аудио-транспондер. Он начинает работать только тогда, когда происходит его облучение высокочастотным зондирующим сигналом. Транспондер трудно обнаружить, так как он может быть вмонтирован в стену.

Приемник транспондера принимает зондирующий сигнал и подает его на узкополосный частотный модулятор. Модулирующим является сигнал, поступающий непосредственно от микрофона или от микрофонного усилителя. Модулированный высокочастотный сигнал переизлучается со смещением по частоте относительно опорной. Переизлученный сигнал принимается приемником, в котором осуществляется его демодуляция.

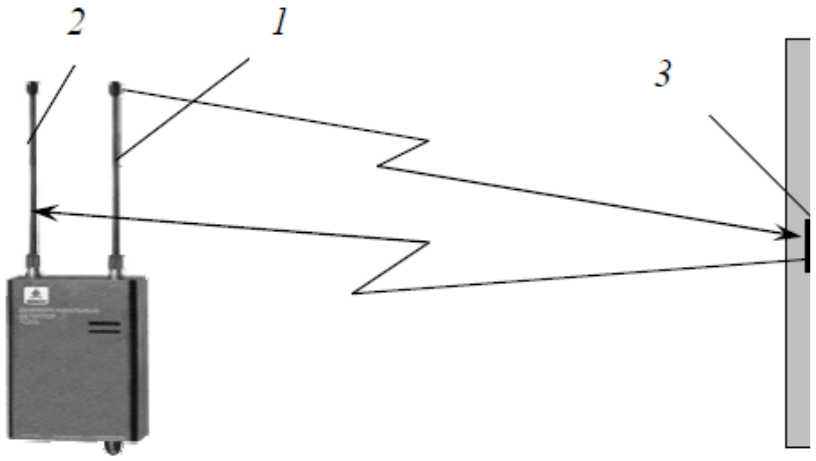

Рисунок 14.14

14.6. Перехват информации с телефонных линий

Одним из основных способов несанкционированного доступа к информации частного и коммерческого характера является прослушивание телефонных переговоров. Для прослушивания телефонных переговоров используются следующие способы подключения:

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).

Параллельное подключение к телефонной линии (Рис. 14.15,а). В этом случае телефонные радиоретрансляторы (телефонные закладки) труднее обнаруживаются, но требуют внешнего источника питания.

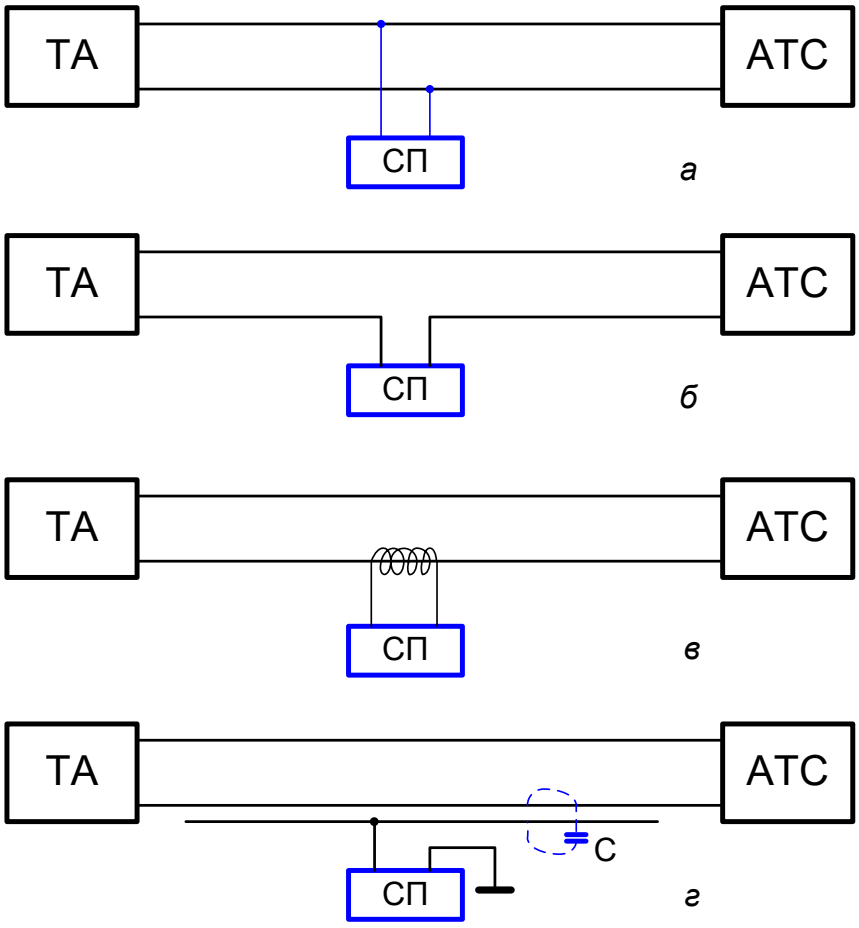

Рис. 14.15. Схемы возможных вариантов подключения к телефонной линии без использования радиоканала

Последовательное включение телефонных радиоретрансляторов в разрыв провода телефонной линии (Рис. 14.15,б). В этом случае питание телефонного радиоретранслятора осуществляется от телефонной линии и на передачу он выходит с момента подъема телефонной трубки абонементом.

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

Дальность действия такой системы из-за затухания ВЧ сигнала в двухпроводной линии не превышает нескольких десятков метров. Имеются системы прослушивания телефонных разговоров, которые не требуют

непосредственного электронного соединения с телефонной линией. Эти системы основаны на индуктивном способе съема информации при помощи специальных катушек (рис.14.15,в).

Данный канал чаще всего используется для съема информации с симметричных высокочастотных кабелей. Непосредственное электрическое подключение аппаратуры перехвата легко обнаруживается специальными контролирующими средствами. Индукционный канал перехвата, не требующий контактного подключения к каналам связи, свободен от этого недостатка. Электромагнитное поле, возникающее вокруг проводников кабеля под действием информационных токовых сигналов, наводит в специальных индукционных датчиках адекватные информационные сигналы.

Современные индукционные датчики способны снимать информацию с кабелей, защищенных не только изоляцией, но и двойной броней из стальной ленты и стальной проволоки, плотно обвивающих кабель.

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