СОДЕРЖАНИЕ

1 Методы и устройства для глушения радиоканала

В этой главе рассмотрены профессиональные и самодельные устройства для подавления связи в разных диапазонах радиочастот.

1.1. Радиосвязь и диапазоны частот

В начале этой книги будем рассматривать особенности распространения радиоволн (в различных диапазонах) не во всем свободном пространстве, а над земной поверхностью. Это понимание распространения радиоволн даст ключ и к раскрытию темы книги – возможностей глушения аппаратными методами самих излучающих радиоволны устройств, будь то передатчики радиосигналов специального предназначения, датчики, использующие взаимосвязи по Wi-Fi или различной мощности или, к примеру, сотовые телефоны. Как показывают опыт и теория, это влияние различно – для волн разной длины и для разных расстояний между передатчиком и приемником. Способы распространения радиоволн существенно зависят от длины волны, от освещенности земной атмосферы Солнцем и от ряда других факторов.

В процессе распространения радиоволны испытывают ослабление, связанное с рядом причин. По мере удаления от передатчика энергия распространяется все в большем объеме, следовательно, плотность потока энергии уменьшается. Среда, в которой распространяются радиоволны, также вызывает их ослабление. Это связано с поглощением энергии волн вследствие тепловых потерь и уменьшением напряженности поля волны при огибании препятствий в виде выпуклости земного шара или возвышенностей на местности.

Распространение радиоволн подчиняется определенным общим законам.

Прямолинейное распространение в однородной среде, то есть среде, свойства которой во всех точках одинаковы. Отражение и преломление при переходе из одной среды в другую. Угол падения равен углу отражения.

Дифракция. Встречая на своем пути непрозрачное тело, радиоволны огибают его. Дифракция проявляется в разной мере в зависимости от соотношения геометрических размеров препятствия и длины волны.

Рефракция. В неоднородных средах, свойства которых плавно изменяются от точки к точке, радиоволны распространяются по криволинейным траекториям. Чем резче изменяются свойства среды, тем больше кривизна траектории.

Полное внутреннее отражение. Если при переходе из оптически более плотной среды в менее плотную угол падения превышает некоторые критические значения, то луч во вторую среду не проникает и полностью отражается от границы раздела сред. Критический угол падения называют углом полного внутреннего отражения.

Интерференция. Это явление наблюдается при сложении в пространстве нескольких волн. В различных точках пространства получается увеличение или уменьшение амплитуды результирующей волны в зависимости от соотношения фаз складывающихся волн.

Радиоволны, распространяющиеся у поверхности земли и, вследствие дифракции, частично огибающие выпуклость земного шара, называются поверхностными волнами. Распространение поверхностных волн сильно зависит от свойств земной поверхности.

Радиоволны, распространяющиеся на большой высоте в атмосфере и возвращающиеся на землю вследствие отражения от атмосферных неоднородностей, называются пространственными волнами.

Помимо ослабления, происходит также изменение структуры поля волны.

Рельеф земной поверхности также влияет на распространение радиоволн. Это влияние зависит от соотношения между высотой неровностей поверхности, горизонтальной протяженностью и углом падения волны на поверхность.

Поэтому высокие холмы, горы, кроме того, «возмущают» поле, образуя затененные области. Дифракция радиоволн на горных хребтах иногда приводит к усилению волны из-за интерференции прямых и отраженных от поверхности Земли волн.

1.2. Беспроводная связь

Беспроводные сети связи имеют различную техническую организацию и структуру. Аббревиатура Wi-Fi принадлежит к определению беспроводной сети связи с относительно большим радиусом действия. Таким образом, везде, где вы встречаете такое сокращение, речь идет именно о беспроводных сетях, эффективность, особенности, «плюсы» и «минусы» которых обсудим в книге далее.

Предыстория вопроса такова. Вообще говоря, происхождение электромагнитного поля – одна из величайших загадок природы. Гипотезу об источнике главного магнитного поля (источником его считается своеобразная динамо-машина в ядре Земли) проверить

экспериментально невозможно, а вот гипотезу, объясняющую аномальное магнитное поле Земли электрическими полями океана, удалось проверить и опровергнуть на практике.

Советский ученый-ихтиолог А. Т. Миронов еще в начале 30-х годов XX века, изучая поведение рыб, обнаружил у них хорошо выраженный электротаксис – способность реагировать на электрическое поле. Это навело его на мысль: в морях и океанах должны существовать электрические (теллурические) поля. Измерения, проведенные в заливах у Мурманского побережья, подтвердили эту догадку. Измеренные здесь электрические поля имели характер вариаций с амплитудами в десятки микровольт на метр. А. Т. Миронов считал, что постоянная составляющая теллурических токов помогает рыбам при их массовых миграциях, они якобы ориентируются в воде по линиям тока.

По мнению другого ученого В. В. Шулейкина, электрические поля в океане должны быть порядка сотен или даже тысяч микровольт на метр – это довольно сильные поля. Уже в конце 1957 года стало очевидным, что в поверхностных слоях океана электрическое поле составило не сотни микровольт на метр, а всего 4–9 мкВ/м. С погружением в глубину это электрическое поле, правда, увеличивалось до десятков микровольт на метр (мВ/м).

Результаты этих и других последующих наблюдений не оставили у ученых сомнений в том, что аналога главного магнитного поля Земли в электрическом поле не существует. Магнитотеллурические поля – это индукционные поля с разными амплитудами, периодами и направлениями векторов. Живым организмам, животным и человеку «неуютно» находиться под действием такого поля, и он стремится уйти туда, где оно слабее. Вот почему сегодня много спорят о вреде беспроводных каналов связи, будь то мобильные телефоны и иные приложения или, к примеру, относительно ограниченные по местности сети Wi-Fi.

1.2.1. Безопасность беспроводных каналов связи

В человеческой природе вообще часто встречается особенность замечать нечто, соответствующее ожиданиям, и игнорировать все остальное. В результате часто возникает искушение увидеть больше, чем на самом деле изображено. К примеру, мы видим неясную тень, но домысливаем фрагмент до целой картины, представляя

себе образ «инопланетянина». Мозг пытается выстроить логичную картину мира на основе иррациональных фактов. Для серьезного экспериментатора, который хочет научно объяснить феномен передачи сигналов без проводов, не сбиваясь на ложные выводы, в этом таится большая опасность.

Вопросы воспрепятствования передаче данных по радиоканалу (без проводов) стали актуальными в мире сразу после изобретения возможностей самой беспроводной связи. В разное время к этому вопросу активно присматривались и военные, и политические деятели. К примеру, во время подготовки книги я уточнил, что в Санкт-Петербурге на пересечении Софийской улицы и улицы Димитрова, в «зеленой зоне» находится большой незастроенный участок с высокими мачтовыми антеннами. Также здесь находятся сохранившиеся ДОТы времен Великой Отечественной войны. Это «радиополе» еще с советских времен известно местным жителям как «глушилка». Адрес всей этой территории – Софийская улица, дом 71.

И сегодня здесь находится площадка № 2 Передающего цеха радиовещания № 3 филиала «РТРС» – Санкт-Петербургский Радиопередающий центр. Во второй половине XX века технические возможности Передающего цеха радиовещания № 3 использовались преимущественно для обеспечения магистральных и зоновых радиосвязей, а также в целях противодействия вещанию западных радиостанций на СССР. В настоящее время основной задачей цеха является обеспечение радиовещания в диапазоне средних волн на территории Санкт-Петербурга и близлежащей части Ленинградской области с использованием средневолновых передатчиков суммарной мощностью 10 кВт.

Основной технологический комплекс Передающего цеха № 3 включает в себя 8 средневолновых передатчиков мощностью 10 кВт (4 передатчика, включая 1 резервный – на площадке № 2). Антенное хозяйство площадки № 2 состоит из 4 антенн-мачт типа «Вертикальный цилиндр» высотой 50 метров каждая, включая одну резервную. Все это иллюстрирует фото (рис. 1.1), и в нашей книге такая иллюстрация необходима в целях наиболее полного представления о проблематике и возможностях глушения различных видов беспроводной связи.

К слову, вторая аналогичная площадка в черте Санкт-Петербурга находится на территории воинской части в п. Бугры (в административных границах Санкт-Петербурга).

Но перейдем к возможностям локального глушения беспроводной связи. Итак, в нашем случае в помещении используются элект-

Рис. 1.1. Антенны для «массового» глушения «вражьих голосов» (Санкт-Петербург)

рические поля небольшой мощности. Теоретически злоумышленник может перехватывать информацию или же атаковать пользовательскую сеть, находясь на относительно безопасном расстоянии. В этой области существует множество различных способов защиты, и при условии правильной настройки можно быть уверенным в обеспечении необходимого уровня безопасности. Разберемся в них на конкретных примерах.

Передача сигналов беспроводным способом возможна благодаря электрическому полю. Разумеется, простой «нешифрованный» канал очень скоро станет доступен злоумышленникам, и пользоваться им будет небезопасно. Именно поэтому почти одновременно с системой передачи данных без проводов, в части Wi-Fi, разработаны специальные протоколы шифрования данных.

Известный и некогда популярный WEP – это протокол шифрования, использующий довольно нестойкий алгоритм RC4 на статическом ключе.

Существовали 64-, 128-, 256- и 512- и даже 1024-битное WEP-шифрование. Чем больше бит используется для хранения ключа, тем больше возможных комбинаций ключей, а соответственно, бо-

лее высокая стойкость сети к взлому. Часть wep-ключа является статической (к примеру, 40 бит в случае 64-битного шифрования), а другая часть (24 бит) – динамическая (вектор инициализации) меняющаяся переменная в процессе работы сети. Основной уязвимостью протокола WEP является то, что векторы инициализации повторяются через некоторый промежуток времени, и взломщику потребуется лишь собрать эти повторы и вычислить по ним статическую часть ключа. Для повышения уровня безопасности можно дополнительно к wep-шифрованию использовать стандарт 802.1x или VPN. Неудивительно, что на смену ему в свое время пришел новый, более «защищенный» протокол.

WPA – более стойкий протокол шифрования, чем WEP, хотя используется тот же алгоритм RC4. Более высокий уровень безопасности достигается за счет использования протоколов TKIP и MIC.

TKIP (Temporal Key Integrity Protocol) – протокол динамических ключей сети, которые меняются довольно часто. При этом каждому устройству также присваивается ключ, который тоже меняется.

MIC (Message Integrity Check) – протокол проверки целостности пакетов, защищает от перехвата пакетов и из перенаправления. Также возможно использование 802.1x и VPN, как в случае с wep-протоколом.

На сегодняшний день пользуются популярностью два варианта протокола WPA: WPA-PSK (Pre-shared key).

Для генерации ключей сети и для входа в сеть используется ключевая фраза. Оптимальный вариант для домашней или небольшой офисной сети: WPA-802.1x.

Вход в сеть осуществляется через сервер аутентификации. Оптимально для сети крупной компании.

Усовершенствование протокола WPA активно происходит все предыдущие годы. В отличие от протокола WPA, используется более стойкий алгоритм шифрования AES. По аналогии с WPA, WPA2 также делится на два типа: WPA2-PSK и WPA2-802.1x.

Далее – для сведения – рассмотрим и другие варианты разных стандартов безопасности сети. Все это нам поможет понять, каким образом можно сохранять данные, передаваемые в эфире беспроводным способом, и каким образом злоумышленники проникают в наши пользовательские активы и получают доступ к данным. А это, в свою очередь, поможет нам с разных углов зрения изучить возможности блокирования беспроводных сетей или, при обоснованной необходимости, «заглушать» их.

1.2.2. Зачем нужны глушители сигналов?

В действительности это далеко не риторический вопрос. А популярность различных устройств – глушителей сигналов среди населения только подтверждает его значимость, ибо современная жизнь научила людей не доверять друг другу. Некоторые супруги не доверяют своим половинкам, родители – детям, начальники – подчиненным. Все пытаются разоблачить кого-то, найти компромат. Если ты человек, преуспевающий в бизнесе, значит, хранишь какие-то секреты. Конкуренты пытаются найти уязвимое место, чтобы забрать бизнес или нарушить его. Все это реалии сегодняшнего времени.

Существует много незамысловатых и доступных приборов, которые помогут недоброжелателям раскрыть все секреты. Наиболее популярными являются приборы со спутниковой навигацией, о которых мы поговорим далее.

Эти электронные устройства позволяют не только отследить местонахождение, но и прослушать разговор. Они миниатюрны, и обнаружить их невооруженным глазом не всегда возможно (неопытному человеку – практически невозможно), поскольку их маскируют под бытовые предметы (часы, калькулятор, евророзетки, флеш-накопители и другие «гаджеты»). К примеру, именно в таких случаях подавитель GPS-сигнала станет надежным защитником тому, кто хочет обезопасить себя и свою информацию; ведь верно говорят: «кто владеет информацией – владеет миром».

Но существуют глушители разных частот и разного назначения, равно как и стандарты шифрования каналов связи.

1.2.3. Протоколы разных стандартов безопасности сети

EAP (Extensible Authentication Protocol). Протокол расширенной аутентификации. Используется совместно с RADIUS-сервером в крупных сетях.

TLS (Transport Layer Security). Протокол, который обеспечивает целостность и шифрование передаваемых данных между сервером и клиентом, их взаимную аутентификацию, предотвращая перехват и подмену сообщений.

RADIUS (Remote Authentication Dial-In User Server). Сервер аутентификации пользователей по логину и паролю.

VPN (Virtual Private Network) – виртуальная частная сеть. Протокол был создан для безопасного подключения клиентов к сети

через общедоступные интернет-каналы. Принцип работы VPN – создание так называемых безопасных «туннелей» от пользователя до узла доступа или сервера. Хотя VPN изначально был создан не для WI-Fi, его можно использовать в любом типе сетей. Для шифрования трафика в VPN чаще всего используется протокол IPSec, обеспечивающий практически стопроцентную безопасность. Случаев взлома VPN на данный момент неизвестно. Именно поэтому эту технологию часто используют для корпоративных сетей.

1.2.4. Дополнительные методы защиты пользовательской беспроводной сети

Вместе с тем важное звено в цепочке защиты пользовательской сети – фильтрация канала связи по MAC-адресу: она необходима для максимально возможного обеспечения безопасности работы. MAC-адрес – это уникальный идентификатор устройства (сетевого адаптера), «зашитый» в него производителем. На некотором оборудовании можно задействовать данную функцию и разрешить доступ в сеть необходимым адресам. Это создаст дополнительную преграду взломщику, хотя не очень серьезную – в принципе, MAC-адрес можно подменить.

Приватное скрытие SSID обеспечивает сети еще большую безопасность.

SSID – это идентификатор беспроводной сети. Большинство оборудования позволяет его скрыть, таким образом, при сканировании Wi-Fi-сетей пользовательской сети видно не будет. Хотя это не слишком серьезная преграда, если взломщик использует более продвинутый сканер сетей, чем стандартная утилита в операционной системе Windows.

Запрет доступа к настройкам точки доступа или роутера через беспроводную сеть реализуется следующим образом. Специально активировав эту функцию, можно запретить доступ к настройкам точки доступа через Wi-Fi-сеть, однако в ряде случаев и это не защитит пользователя от перехвата трафика или от проникновения в сеть.

Поэтому неправильная настройка оборудования, поддерживающего даже самые современные технологии защиты, не обеспечит должного уровня безопасности сети.

В каждом стандарте есть дополнительные технологии и настройки для повышения уровня безопасности, которые опытный поль-

зователь умело применяет на практике, не манкируя обеспечением безопасности собственных данных.

Еще более простым способом блокируются данные, передаваемые по каналу Bluetooth.

Это распространенный, самый технически простой и доступный способ беспроводного соединения с компьютером или периферийным оборудованием – через радиоинтерфейс Bluetooth.

Еще более универсальны соединения по встроенному ИК-порту (инфракрасный порт, IRDA).

Инфракрасный порт (ИК-порт) позволяет установить беспроводное соединение мобильного телефона с любым устройством, имеющим ИК-порт (ноутбуком, карманным компьютером, модемом), который находится в прямой видимости от аппарата (не понадобится отдельный кабель для связи с компьютером и загрузки нового логотипа или мелодии на телефон).

В первую очередь ИК-порт нужен для синхронизации с ПК. Вы можете использовать телефон в качестве модема для ноутбука, в том числе и при наличии ИК-порта. Но на самом деле вариантов применения ИК-портов во втором десятилетии XXI века очень много, и этот способ незаслуженно забыли современные пользователи беспроводной связи.

Так, на рис. 1.2 представлена система беспроводной передачи данных чрез ИК-порт, сочетающая в себе передатчик сигналов (подключаемый к телевизору или иному оборудованию, имеющему аудиовыход) и приемник (в наушниках).

ИК-порты более распространены, но пользоваться ими не очень удобно, так как приходится располагать устройства на небольшом

Рис. 1.2. Система беспроводной передачи данных через ИК-порт

расстоянии в области прямой видимости (скорость передачи небольшая). Связь по радио быстрее, и телефон не обязательно доставать из кармана. А можно купить специальную Bluetooth-гарнитуру– тогда можно будет разговаривать по телефону, который лежит, к примеру, в бардачке автомобиля (и даже набирать номера при наличии голосового набора). Итак, Bluetooth – технология радиосвязи малой дальности (около 10 м), которая позволяет установить высокоскоростное беспроводное соединение мобильного телефона с настольным ПК, портативными и карманными компьютерами.

И это та технология, которую можно (в отличие от системы связи через ИК-порт) блокировать с помощью подавителей различных систем радиосвязи, о которых поговорим далее.

1.3. Глушители сигналов и их разновидности

Подавление сигналов сотовой связи осуществляется за счет постановки заградительной помехи, а помеха эта ставится в зависимости от той частоты, на которой работает сотовый телефон, который нам надо заглушить (т. е. зависит от стандарта, на котором работает данный оператор сотовой связи). Ниже дан обзор использующихся стандартов мобильной связи в соответствии с их частотными характеристиками.

Информация к размышлению: в январе 2007 года в городе Сан-Диего начали происходить странные события: перестали работать банкоматы, пропала сотовая связь, нарушилась работа системы мониторинга рейсов в аэропорту.

Хаос длился пару часов, пока не выяснилась причина: возле побережья стояли два военных корабля ВМС США, которые осуществляли учебную отработку действий в условиях потери связи. Для этого была активирована система активных помех GPS. По ошибке сигналы спутниковой связи заглушили не только на кораблях, но и в городе у гражданских лиц.

Вышки сотовой связи, электрические сети, информационные банковские системы и даже фондовая биржа – все они полагаются на сигналы точного времени со спутников GPS.

Зависимость от GPS становится слишком опасной, учитывая исключительную ненадежность этой технологии. Проблема в том, что сигнал со спутника очень слаб, и заглушить его чрезвычайно

легко, если генерировать шум на той же частоте. Сигнал можно заглушить примитивным устройством китайского производства, которое и сегодня продается в интернет-магазинах по цене в пару тысяч российских рублей. Хотя устройство запрещено к использованию в большинстве цивилизованных стран, но спрос на него есть, а значит, появляется и предложение – в Китае такие приборы в массовом производстве уже несколько лет.

Покупатели подобных устройств – обычно водители коммерческого транспорта, которые хотят избежать слежения со стороны работодателя. Устройство применяют и преступники-автоугонщики, чтобы подавить систему слежения в угнанном автомобиле.

Радиус действия автомобильной «глушилки» невелик.

Гипотетически террористы или мошенники могут использовать более мощные приборы, аналогичные тем, что использовались ВМС США возле Сан-Диего. Страшно представить, какой хаос возникнет в современном мегаполисе, если кто-то активирует устройство глушителя достаточной мощности. Ущерб может быть пострашнее любого теракта.

Удивительно, что сейчас различные экстренные службы, включая скорую помощь, МЧС, военных, систему управления авиарейсами и железнодорожным транспортом, системы электроснабжения, перешли (и отрапортовали) на использование спутниковых координат и сигналов времени, кое-где не заботясь о создании резервной системы.

Это интересно!

По оценке журнала GPS World, в 2014 году в мире находилось в использовании более миллиарда приемников GPS, и более 90% из них используются только для получения сигналов точного времени. Интересно, что энтузиасты уже создали работающие образцы нового поколения таких устройств, способных не просто глушить, но и искажать сигналы GPS. Мошенники могут использовать это с целью осуществления малых и крупных афер (к примеру, заявки на фондовой бирже маркируются сигналами точного времени, так что саботаж в сети конкурента позволит манипулировать котировками акций).

Итак, мы выяснили, что можно заглушить слабый сигнал более сильным.

Для этого нужно уметь моделировать работу спутниковой группировки GPS в реальном времени. Специалистов, которые это умеют делать, на самом деле много. Материалов в открытом доступе также достаточно. Задача постройки программно-аппаратного комплекса

силами специалистов вполне решается. Для «кустаря-одиночки» (радиолюбителя) задача кажется сложной, но и здесь существуют варианты решения.

К примеру, давно люди, увлекающиеся радиоэлектроникой, ищут различные схемы и инструкции, чтобы собрать какой-нибудь электронный прибор для личного пользования. Я как автор этой книги также интересовался подобным вопросом – самому сделать глушитель сотовой связи. И расскажу об этом уже в этой главе, ниже.

1.3.1. Как обеспечивается информационная безопасность

Кроме целого ряда возможностей получить доступ к секретной информации с помощью подслушивающих устройств, существуют наиболее распространенные в определенных кругах методы для информационной разведки, а именно – получение информации через сотовый телефон. Действительно, сотовый телефон (который обыватели называют мобильным) стал самым востребованным изобретением еще в XX веке – после пенициллина, а эволюция телефонов в фотоаппараты и мини-компьютеры сделала их незаменимыми для каждого современного человека.

Однако есть у мобильных телефонов один недостаток – они издают звуки. Причем это не просто звуки, они звонят порой в самый неподходящий момент. Особенно неприятно, когда на совещании или деловых переговорах чей-нибудь телефон раздражается неуместной мелодией.

Решение этой проблемы – генераторы зашумления сетей сотовой связи. Они уже давно и активно используются спецслужбами, театрами и мюзик-холлами. Об этих устройствах мы еще поговорим далее.

Технологически устройство может быть встроено в любую имеющуюся в помещении аппаратуру с необходимым источником питания.

С помощью зашумляющего прибора можно говорить по-настоящему спокойно, не опасаясь, не отвлекаясь на неуместные звонки и не опасаясь «подслушки», ведь мобильный телефон может стать прекрасным подслушивающим устройством (даже без ведома его владельца). С точки зрения тактических возможностей мобильный телефон приобрел свойства устройств негласного съема информации – легальных «жучков».

И тем не менее сотовый телефон можно рассматривать не только как подслушивающее устройство. С ним также возникает ряд проблем, к примеру:

- в медицинских учреждениях (телефон не только нарушает покой больных, но и может нарушить правильную работу медицинских приборов);
- использование для подрыва зарядов при проведении терактов: подрывник легко может использовать вибратор «мобильника», для того чтобы в нужный момент подать напряжение на электродетонатор. Тогда взрыв произойдет по звонку, после получения SMS или по таймеру;
- непосредственно при разработке и проведении террористических операций (связь в подобных операциях является очень важным фактором);
- в самолетах (мобильные телефоны могут наводить помехи на определенные радиочастоты электронных устройств самолета);
- во время спектакля или экскурсии, в библиотеке или читальном зале отвлекает не только хозяина мобильного телефона, но и остальных людей вокруг;
- в учреждениях пенициарной системы (зоны, тюрьмы, изоляторы);
- при проведении экзаменов (не только отвлекает остальных, но и ставит под сомнение качество знаний экзаменуемого).

Для специалистов по информационной безопасности эта характеристика означает наличие у мобильного телефона возможности управления дистанционно и возможность включения в действие функции подслушивания в любой момент времени и любом месте, где бы пользователь «мобильника» не находился.

На профессиональном уровне задача борьбы с негласным съемом информации при помощи мобильных телефонов решается успешно, но является весьма дорогостоящим мероприятием и требует привлечения специалистов и широкого круга технических средств.

1.3.2. Сотовый телефон с точки зрения информационной безопасности

Способов несанкционированного доступа к информации очень много, но зачастую их организация и техническое оснащение достаточно дороги и сложны. Кроме того, большинство средств съема информации невозможно приобрести легально. Но в то же время у нас у всех есть доступ к дешевому, миниатюрному (на рынке сотовых

телефонов широко распространены аппараты с размерами, сопоставимыми с размерами спичечного коробка), высококачественному подслушивающему радиоустройству, способному, во-первых, передавать акустическую информацию на сколь угодно большое расстояние. Во-вторых, оно может быть удалено и негласно активировано без какой-либо индикации, без ведома владельца («недекларированные» возможности, про которые не сообщает производитель), даже в выключенном состоянии.

Это устройство – сотовый телефон – миниатюрное радиоустройство, способное передавать акустическую информацию на любое расстояние по каналам сотовой связи. В этом случае телефон переводится в режим передачи по инициативе его владельца.

1.3.3. Способы защиты информации от утечки по каналам сотовой связи

Известен ряд способов защиты информации от утечки по каналам сотовой связи. Один из них – организационно-режимные меры, которые должны обеспечить изъятие сотовых телефонов при попытке вноса в контролируемое помещение.

Опыт борьбы с подслушиванием показывает, что организационно-режимные меры, предотвращающие (или запрещающие) попытку вноса сотовых телефонов на защищаемый объект, широко используются, но эффективность таких мероприятий низка. Проконтролировать исполнение организационно-режимных мероприятий сложно из-за того, что сотовый телефон имеет небольшие размеры и может быть закамуфлирован практически под любой предмет обихода.

Другой способ защиты – это технические методы и средства:

- пассивное блокирование сигналов сотовой связи (экранирование помещений);
- акустическое зашумление тракта передачи речевой информации при попытке негласной дистанционной активации микрофона трубки сотового телефона (например, устройства типа «Кокон», см. рис. 1.3).

Рис. 1.3. Устройство «Кокон»

Среди пассивных средств защиты информации от утечки по каналам сотовой связи на первом месте стоят индикаторы электромагнитного излучения и экранирование помещений.

Акустические устройства защиты сотовых телефонов от негласной дистанционной активизации

Строго говоря, акустические устройства защиты сотовых телефонов от негласной дистанционной активизации (НДВ) предназначены для защиты речевой информации, циркулирующей в местах пребывания владельца сотового телефона, в случае его негласной дистанционной активизации – с целью прослушивания через канал сотовой связи.

При этом единственным демаскирующим признаком является изменение напряженности электромагнитного поля (передатчик сотового телефона несанкционированно включается на передачу). Это изменение фиксируется индикатором электромагнитного поля, входящим в состав устройства, который дает команду на автоматическое включение акустического шумогенератора, расположенного внутри объема изделия в непосредственной близости от микрофона сотового телефона.

Принцип работы

Трубка сотового телефона помещается во внутренний объем футляра или в стакан. В случае негласной дистанционной активации телефона в режим прослушивания единственным демаскирующим признаком является изменение напряженности электромагнитного поля (передатчик сотового телефона несанкционированно включается на передачу).

Это изменение фиксируется индикатором поля, входящим в состав устройства, который дает команду на автоматическое включение акустического шумогенератора, расположенного внутри объема изделия. Уровень акустического шума на входе микрофона трубки сотового телефона таков, что обеспечивается гарантированное закрытие этого канала утечки информации и зашумляется весь тракт передачи речевой информации таким образом, что на приемном конце отсутствуют какие-либо признаки речи.

В табл. 1.1 рассмотрены технические характеристики устройств «Ладья» и «Кокон».

Во всех описанных устройствах реализован автоматический контроль разрядки батареи. Признаком разряда батарей является пре-