



Кашкаров А.П.



depositphotos



**ЭЛЕКТРОННЫЕ УСТРОЙСТВА  
ДЛЯ ГЛУШЕНИЯ БЕСПРОВОДНЫХ  
СИГНАЛОВ  
(GSM, Wi-Fi, GPS  
и некоторых радиотелефоны)**

**Андрей Петрович Кашкаров**  
**Электронные устройства**  
**для глушения беспроводных**  
**сигналов (GSM, Wi-Fi, GPS и**  
**некоторых радиотелефонов)**

*Текст предоставлен правообладателем*

*[http://www.litres.ru/pages/biblio\\_book/?art=17354621](http://www.litres.ru/pages/biblio_book/?art=17354621)*

*Электронные устройства для глушения беспроводных сигналов (GSM, Wi-Fi, GPS и некоторых радиотелефонов). / Кашкаров А. П.: ДМК*

*Пресс; Москва; 2016*

*ISBN 978-5-97060-210-2*

### **Аннотация**

Информация – это победа. Поэтому внимание к защите информации сегодня обоснованно велико. Кроме ряда возможностей получить доступ к секретной информации с помощью подслушивающих устройств, существуют и распространенные в определенных кругах методы для информационной разведки, а именно получение информации через сотовый телефон и по каналам беспроводной связи. В книге рассмотрены профессиональные и самодельные устройства для подавления устройств беспроводной связи в разных диапазонах радиочастот. Для широкого круга читателей.

# Содержание

1. Методы и устройства для глушения радиоканала	4
1.1. Радиосвязь и диапазоны частот	5
1.2. Беспроводная связь	8
1.2.1. Безопасность беспроводных каналов связи	10
1.2.2. Зачем нужны глушители сигналов?	15
1.2.3. Протоколы разных стандартов безопасности сети	16
Конец ознакомительного фрагмента.	18

# **Андрей Кашкаров Электронные устройства для глушения беспроводных сигналов (GSM, Wi- Fi, GPS и некоторых радиотелефонов)**

## **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 назначения, 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 зем-

ли 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 ампли-

тудами 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 искажение 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 жите-

лям 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 зонавых 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).



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

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

чении 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, более 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 их 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 спутни-

ковой 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, евросеточки, 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.

# Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.