

СОДЕРЖАНИЕ

1	Аспекты организации сети Wi-Fi	5
1.1.	Особенности Wi-Fi.....	7
1.2.	Преимущества и недостатки перед другими формами передачи данных на небольшие расстояния	8
1.2.1.	Общеизвестные преимущества Wi-Fi.....	8
1.2.2.	Недостатки	8
1.3.	Защита от вторжения: разные варианты	9
1.4.	Перспективы технологии Wi-Fi на разных уровнях	12
1.5.	Взаимодействие сетей Wi-Fi и сотовой связи	12
1.6.	Вопросы взаимодействия программного обеспечения ПК и сетей Wi-Fi	17
1.7.	Регистрация оборудования: нужна ли она?.....	18
1.8.	Принудительное подавление Wi-Fi с помощью специальных генераторов	20
1.8.1.	Техническое описание портативного подавителя сотовой, Wi-Fi- и Bluetooth-связи «Скорпион 120А-Pro» (Noname)	21
1.8.2.	Преимущества устройства	22
1.8.3.	Принцип работы и комплектация устройства	22
1.9.	Безопасность здоровья.....	23
1.10.	Рекомендации по безопасности информации, передаваемой через сети Wi-Fi	24
1.11.	Распределение Wi-Fi-сигнала посредством ноутбука	28
1.12.	Варианты выбора и технические характеристики оборудования	30
2	Управление по Wi-Fi своими руками	34
2.1.	Устройства управления по сети Wi-Fi.....	35
2.1.1.	Умная управляемая электрическая Wi-Fi-модель HL0107	35
2.1.2.	Альтернативный вариант: модель Orvibo WiWo-S20	35
2.1.3.	Беспроводная Wi-Fi-розетка BePlug 15	39
2.1.4.	Устройство DSP-W215.....	42
2.2.	Практические решения для самостоятельного повторения	45

2.2.1. Интернет в «обычной» розетке для скрытого монтажа.....	45
2.2.2. Многофункциональная розетка с дистанционным управлением Wi-Fi своими руками	48
2.3. О чем не говорят громко.....	52
2.4. Варианты совершенствования системы.....	54
2.5. Практика изготовления антенны для работы в сети Wi-Fi.....	55
2.6. Особенности организации домашней сети Wi-Fi.....	58
2.6.1. Настройка роутера для Интернета без драйвера	61
2.6.2. Настройка параметров соединения на компьютере.....	61
2.6.3. Настройка оборудования	63
2.7. «Тонкая» настройка выносных антенн Wi-Fi на местности.....	67
2.7.1. Кабели и фидеры (особенности)	67
2.7.2. Как определить полезный материал для самостоятельного изготовления корпуса антенны Wi-Fi	68
<hr/>	
3 Пошаговые рекомендации	69
3.1. Пошаговая настройка домашней сети Wi-Fi.....	70
3.2. Как подключить телевизор к компьютеру по Wi-Fi.....	70
3.2.1. Проигрывание фильмов с компьютера на телевизоре по Wi-Fi (DLNA)	71
3.2.2. Как настроить DLNA-сервер в ОС Windows 7 и Windows 8.....	73
3.3. Программы для настройки DLNA-сервера в Windows.....	79
3.4. Разбор проблемных вопросов.....	80
3.4.1. Как настроить только изображение без звука.....	82
3.4.2. Как использовать телевизор в качестве беспроводного монитора в сети Wi-Fi	83
3.4.3. Подключаем по Wi-Fi обычный телевизор без беспроводного адаптера.....	84
3.4.4. Как преобразовать загрузочную флэшку.....	85
3.4.5. Как подключить телевизор вторым монитором через ТВ-приставку с Wi-Fi	85
3.4.6. Как отключить сетевое обнаружение и общий доступ к файлам?	85
3.4.7. Связь по Wi-Fi «телевизор–телевизор».....	85
3.4.8. Подключение жесткого диска через Wi-Fi.....	86
Использованная литература	87

1 **Аспекты организации сети Wi-Fi**

2	Управление по Wi-Fi своими руками	34
3	Пошаговые рекомендации	69

Довольно распространенная сегодня аббревиатура Wi-Fi расшифровывается как торговая марка Wi-Fi Alliance для беспроводных сетей на базе стандарта IEEE 802.11. Под аббревиатурой Wi-Fi (от английского словосочетания Wireless Fidelity (перевод – «беспроводное качество» или «беспроводная точность»)) уже несколько лет высокими темпами развивается целое семейство стандартов передачи цифровых потоков данных по радиоканалам. Отчасти и поэтому любое оборудование, соответствующее стандарту IEEE 802.11, может быть протестировано в Wi-Fi Alliance и получить соответствующий сертификат и право нанесения логотипа Wi-Fi. По другой версии, термин «Wi-Fi» изначально был придуман как игра слов для привлечения внимания потребителя «намеком» на Hi-Fi (англ. High Fidelity – высокая точность). Несмотря на то что поначалу в некоторых пресс-релизах WECA фигурировало словосочетание «Wireless Fidelity» («беспроводная точность»), на данный момент от такой формулировки отказались, и термин «Wi-Fi» никак не расшифровывается.

История создания Wi-Fi такова. В 1991 году NCR Corporation/AT&T (впоследствии – Lucent Technologies и Agere Systems) в Сига, Нидерланды, разработали новый продукт, предназначавшийся для систем кассового обслуживания, который был выведен на рынок под маркой WaveLAN и обеспечивал скорость передачи данных от 1 до 2 Мбит/с. Один из создателей Wi-Fi – Вик Хейз (Vic Hayes) – разработчик таких стандартов, как IEEE 802.11b, IEEE 802.11a и IEEE 802.11g, покинул компанию в 2003 году, и Agere Systems не смогла конкурировать на равных с другими, несмотря на то что продукция занимала нишу относительно бюджетных Wi-Fi-решений. 802.11abg all-in-one-чипсет Agere (кодовое имя: WARP) плохо продавался, и Agere Systems решила уйти с рынка Wi-Fi еще в конце 2004 года.

Широко известный сегодня стандарт IEEE 802.11n утвержден 11 сентября 2009 года. Его применение позволило повысить скорость передачи данных практически в четыре раза, по сравнению с устройствами стандартов 802.11g (максимальная скорость которых равна 54 Мбит/с), при условии использования в режиме 802.11n с другими устройствами 802.11n. Теоретически 802.11n способен обеспечить скорость передачи данных до 600 Мбит/с [2]. С 2011 по 2013 год разрабатывался стандарт IEEE 802.11ac, окончательное принятие стандарта было запланировано на начало 2014 года. Скорость передачи данных при использовании 802.11ac может достигать нескольких Гбит/с. Большинство ведущих производителей оборудования уже анонсировали устройства, поддерживающие данный

стандарт. Эволюция продолжалась, и в 2011 году Институт инженеров электротехники и электроники (IEEE) выпустил официальную версию стандарта IEEE 802.22. Системы и устройства, поддерживающие этот стандарт, позволят принимать данные на скорости до 22 Мбит/с в радиусе 100 км от ближайшего передатчика.

1.1. Особенности Wi-Fi

Блок-схема сети Wi-Fi содержит не менее одной точки доступа и не менее одного клиента. Также возможно подключение двух клиентов в режиме точка-точка (Ad-hoc), когда точка доступа не используется, а клиенты соединяются посредством сетевых адаптеров «напрямую». Точка доступа передает свой идентификатор сети (SSID) с помощью специальных сигнальных пакетов на скорости 0,1 Мбит/с каждые 100 мс. Поэтому 0,1 Мбит/с – наименьшая скорость передачи данных для Wi-Fi. Зная SSID сети, клиент может выяснить, возможно ли подключение к данной точке доступа. При попадании в зону действия двух точек доступа с идентичными SSID приемник может выбирать между ними на основании данных об уровне сигнала. Стандарт Wi-Fi дает клиенту полную свободу при выборе критериев для соединения. Более подробно принцип работы описан в официальном тексте стандарта. Однако сей стандарт не описывает всех аспектов построения беспроводных локальных сетей Wi-Fi. Поэтому каждый производитель оборудования решает эту задачу по-своему, применяя те подходы, которые он считает наилучшими с той или иной точки зрения. Поэтому возникает необходимость классификации способов построения беспроводных локальных сетей.

По способу объединения точек доступа в единую систему можно выделить:

- автономные точки доступа (называются также самостоятельные, децентрализованные, умные);
- точки доступа, работающие под управлением контроллера (называются также «легковесные», централизованные);
- бесконтроллерные, но не автономные (управляемые без контроллера).

По способу организации и управления радиоканалами можно выделить беспроводные локальные сети:

- со статическими настройками радиоканалов;
- с динамическими (адаптивными) настройками радиоканалов;
- со «слоистой» или многослойной структурой радиоканалов.

1.2. Преимущества и недостатки перед другими формами передачи данных на небольшие расстояния

1.2.1. Общеизвестные преимущества Wi-Fi

Беспроводной Интернет позволяет развернуть сеть без прокладки кабеля, что может уменьшить стоимость развертывания и/или расширения сети. Места, где нельзя проложить кабель, к примеру вне помещений и в зданиях, имеющих историческую ценность, могут обслуживаться беспроводными сетями. Также такое решение позволяет иметь доступ к сети мобильным устройствам. Для всех Wi-Fi-устройств гарантируется совместимость оборудования благодаря обязательной сертификации оборудования с логотипом Wi-Fi. Другим отличительным фактором использования Wi-Fi-устройств и сетей являются их доступность в бытовом плане, легкий монтаж и мобильность. Пользователь больше не привязан к одному месту и может пользоваться Интернетом в комфортной для вас обстановке. В пределах Wi-Fi-зоны в сеть Интернет могут выходить несколько пользователей с компьютеров, ноутбуков, телефонов и т. д. Излучение от Wi-Fi-устройств в момент передачи данных на порядок (в 10 раз) меньше, чем у сотового телефона. И тем не менее мы еще вернемся к вопросу безопасности применения Wi-Fi в этом разделе далее, поскольку с медицинской точки зрения известны несколько противоречий на сей счет.

1.2.2. Недостатки

Как ни странно, но недостатки Wi-Fi тоже имеют место быть.

В диапазоне 2,4 ГГц работает множество устройств, таких как устройства, поддерживающие Bluetooth, и др., и даже микроволновые печи, что ухудшает электромагнитную совместимость. Производителями оборудования указывается скорость на L1 (OSI), в результате чего создается иллюзия, что производитель оборудования завышает скорость, но на самом деле в Wi-Fi весьма высоки служебные «накладные расходы». Получается, что скорость передачи данных на L2 (OSI) в Wi-Fi-сети всегда ниже заявленной скорости на L1 (OSI). Реальная скорость зависит от доли служебного трафика, которая зависит уже от наличия между устройствами физических преград (мебель, стены), наличия помех от других беспроводных

устройств или электронной аппаратуры, расположения устройств относительно друг друга и т. п.

Частотный диапазон и эксплуатационные ограничения в различных странах не одинаковы. Во многих европейских странах разрешены два дополнительных канала, которые запрещены в США; в Японии есть ещё один канал в верхней части диапазона, а другие страны, к примеру Испания, запрещают использование низкочастотных каналов. Более того, некоторые страны, к примеру Россия, Белоруссия и Италия, требуют регистрации всех сетей Wi-Fi, работающих вне помещений, или требуют регистрации Wi-Fi-оператора. О том, как можно заглушить Wi-Fi, тоже будет рассказано далее.

Внимание, важно!

Добавлю, что в России точки беспроводного доступа, а также адаптеры Wi-Fi с ЭИИМ, превышающей 100 мВт (20 дБм), подлежат обязательной регистрации.

1.3. Защита от вторжения: разные варианты

Стандарт шифрования WEP может быть относительно легко взломан даже при правильной конфигурации (из-за слабой стойкости алгоритма). Новые устройства поддерживают более совершенные протоколы шифрования данных WPA и WPA2. Принятие стандарта IEEE 802.11i (WPA2) в июне 2004 года сделало возможным применение более безопасной схемы связи, которая доступна в новом оборудовании. Обе схемы требуют более стойкого пароля, чем те, которые обычно назначаются пользователями. Многие организации используют дополнительное шифрование (VPN) для защиты от вторжения.

Сегодня основным методом взлома WPA2 является подбор пароля, поэтому рекомендуется использовать сложные цифробуквенные пароли, для того чтобы максимально усложнить задачу подбора пароля. В режиме точка-точка (Ad-hoc) стандарт предписывает лишь реализовать скорость 11 Мбит/сек (802.11b). Шифрование WPA(2) недоступно, только «легковзламываемый» WEP.

Актуальные вопросы безопасности беспроводных сетей

Безопасности беспроводных сетей стоит уделять особое внимание. Ведь Wi-Fi является беспроводной сетью с относительно боль-

шим радиусом действия. Соответственно, злоумышленник может перехватывать информацию или же атаковать пользовательскую сеть, находясь на относительно безопасном расстоянии. Существует множество различных способов защиты, и при условии правильной настройки можно быть уверенным в обеспечении необходимого уровня безопасности. Разберемся в них предметно.

WEP – это протокол шифрования, использующий довольно нестойкий алгоритм RC4 на статическом ключе. Существует 64-, 128-, 256- и 512-битное WEP-шифрование. Чем больше бит используется для хранения ключа, тем больше возможных комбинаций ключей, а соответственно, более высокая стойкость сети к взлому. Часть вер-ключа является статической (40 бит в случае 64-битного шифрования), а другая часть (24 бит) – динамическая (вектор инициализации), то есть меняющаяся 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.

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 и в случае с wep-протоколом.

Существует два вида 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 WPA, используется более стойкий алгоритм шифрования AES. По аналогии с WPA, WPA2 также делится на два типа: WPA2-PSK и WPA2-802.1x.

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. Он обеспечивает практически стопроцентную безопасность. Случаев взлома VPN на данный момент неизвестно. Мы рекомендуем использовать эту технологию для корпоративных сетей.

Дополнительные методы защиты пользовательской сети

Фильтрация по MAC-адресу – важное звено в обеспечении безопасности работы. MAC-адрес – это уникальный идентификатор устройства (сетового адаптера), «защитый» 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 вашей беспроводной сети. Большинство оборудования позволяет его скрыть, таким образом, при сканировании Wi-Fi-сетей вашей сети видно не будет. Но опять же, это не слишком серьезная преграда, если взломщик использует более продвинутый сканер сетей, чем стандартная утилита в Windows.

Запрет доступа к настройкам точки доступа или роутера через беспроводную сеть реализуется следующим образом. Активацией этой функции можно запретить доступ к настройкам точки доступа

через Wi-Fi-сеть, однако 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 пользователь умело применяет на практике, не манкируя обеспечением безопасности собственных данных.

1.4. Перспективы технологии Wi-Fi на разных уровнях

На промышленном уровне суперсовременные технологии Wi-Fi предлагаются пока ограниченным числом поставщиков. Так, несколько лет назад компания Siemens Automation & Drives предложила Wi-Fi-решения для своих контроллеров SIMATIC в соответствии со стандартом IEEE 802.11g в свободном ISM-диапазоне 2,4 ГГц, обеспечивающем максимальную скорость передачи 54 Мбит/с. Данные технологии применяются для управления движущимися объектами и в складской логистике, а также в тех случаях, когда по какой-либо причине невозможно прокладывать проводные сети Ethernet. Использование Wi-Fi-устройств на предприятиях обусловлено высокой помехоустойчивостью, что делает их применимыми на предприятиях со множеством металлических конструкций. Wi-Fi электронные устройства не создают существенных помех для узкополосных радиосигналов. Технология находит широкое применение на удаленном или опасном производстве, там, где нахождение оперативного персонала связано с повышенной опасностью или вовсе затруднительно. К примеру, для задач телеметрии на нефтегазодобывающих предприятиях, а также для контроля за перемещением персонала и транспортных средств в шахтах и рудниках, для определения нахождения персонала в аварийных ситуациях.

На рис. 1.1 представлена иллюстрация организации сети Wi-Fi.

1.5. Взаимодействие сетей Wi-Fi и сотовой связи

Теоретически и перспективно Wi-Fi и подобные ему технологии со временем могут заменить сотовые сети, такие как GSM. Препятствия-

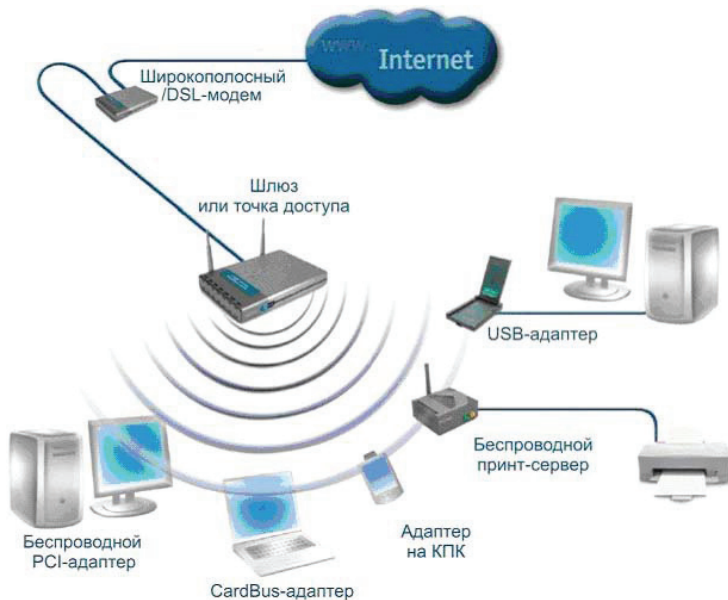


Рис. 1.1. Организации сети Wi-Fi

ми для такого развития событий в ближайшем будущем являются отсутствие глобального роуминга, ограниченность частотного диапазона и сильно ограниченный радиус действия Wi-Fi. Более правильным выглядит сравнение сотовых сетей с другими стандартами беспроводных сетей, таких как UMTS, CDMA или WiMAX. Тем не менее уже сегодня Wi-Fi пригоден для использования VoIP в корпоративных сетях или в среде SOHO. Первые образцы оборудования появились еще в начале 2000-х, они серийно вышли на широкий рынок в 2005 году. Тогда такие компании, как Zyxel, UT Starcomm, Samsung, Hitachi, и многие другие представили на рынок VoIP Wi-Fi-телефоны по «разумным» ценам. В те далекие годы ADSL ISP-провайдеры начали предоставлять услуги VoIP своим клиентам (ISP XS4All). Когда звонки с помощью VoIP стали очень дешёвыми, а зачастую вообще бесплатными, провайдеры, способные предоставлять услуги VoIP, получили возможность открыть новый рынок – услуг VoIP. Телефоны GSM с интегрированной поддержкой возможностей Wi-Fi и VoIP стали выводиться на рынок, и потенциально они планировались такими, чтобы заменить проводные телефоны. Но сегодня непосредственное сравнение Wi-Fi и сотовых сетей нецелесообразно

по целому ряду причин. Телефоны, использующие только Wi-Fi, имеют очень ограниченный радиус действия, поэтому развертывание таких сетей обходится довольно дорого. И тем не менее развертывание подобных сетей может быть наилучшим решением для локального использования, например в корпоративных сетях. Однако устройства, поддерживающие несколько стандартов, могут занять значительную долю рынка. При наличии в данном конкретном месте покрытия как GSM, так и Wi-Fi, экономически намного более выгодно использовать Wi-Fi, разговаривая посредством сервисов интернет-телефонии. К примеру, программное обеспечение – клиент Skype давно существует в версиях как для смартфонов, так и для КПК.

Всех пользователей Wi-Fi сегодня условно можно разделить на три категории:

- *linus* – выделяющие бесплатный доступ в Интернет;
- *bills* – продающие свой частотный диапазон;
- *aliens* – использующие доступ через *bills*.

Таким образом, система аналогична пиринговым сервисам. Несмотря на то что FON получает финансовую поддержку от таких компаний, как Google и Skype, лишь со временем можно уточнить, будет ли эта идея действительно работать.

У этого сервиса есть три основные проблемы. Первая заключается в том, что для перехода проекта из начальной стадии в основную требуется больше внимания со стороны общественности и СМИ. Нужно также учитывать тот факт, что предоставление доступа к вашему интернет-каналу другим лицам может быть ограничено вашим договором с интернет-провайдером. Поэтому интернет-провайдеры будут пытаться защитить свои интересы. Так же, скорее всего, поступят звукозаписывающие компании, выступающие против свободного распространения MP3.

Возможные решения по организации беспроводного доступа представлены на рис. 1.2.

Внимание, важно!

По ряду причин в России основное количество точек доступа сообщества FON расположено в Московском регионе. Посему говорить о распространении и какой-либо перспективе развертывания системы по всей стране, полагаю, преждевременно.

Wi-Fi совместим с игровыми консолями и КПК и позволяет вести сетевую игру через любую точку доступа или в режиме точка-точка.



Рис. 1.2. Возможные решения организации беспроводного доступа

Все игровые консоли нового поколения имеют поддержку стандартов Wi-Fi IEEE 802.11g. Пока коммерческие сервисы пытаются использовать существующие бизнес-модели для Wi-Fi, многие группы, сообщества, города и частные лица строят свободные сети Wi-Fi, часто используя общее пиринговое соглашение, для того чтобы сети могли свободно взаимодействовать друг с другом, а также широко используют возможности Wi-Fi в ограниченном пространстве для управления бытовыми приборами в системе «Умный дом», о чем я подробно расскажу в следующих разделах.

Одна из конкретных возможностей – ячеистая сеть. Схема создания ячеистой сети (mesh-network) с использованием оборудования Wi-Fi предполагает следующие уточнения.

OLSR (en) – один из протоколов, используемых для создания свободных сетей. Некоторые сети применяют статическую маршрутизацию, другие полностью полагаются на OSPF. В Израиле разрабатывается протокол WiPeer для создания бесплатных P2P-сетей на основе Wi-Fi. Несколько лет назад в Wireless Leiden разработали собственное программное обеспечение для маршрутизации под названием LVrouteD для объединения Wi-Fi-сетей, построенных на полностью беспроводной основе. Большая часть сетей построена на основе ПО

с открытым кодом, или публикуют свою схему под открытой лицензией (превращает любой ноутбук с установленной Mac OS X и Wi-Fi-модулем в открытый узел Wi-Fi-сети). Также следует обратить внимание на netsukuku – разработка всемирной бесплатной mesh-сети.

Внимание, важно!

Любопытно, что во многих странах мира уже обеспечивают свободный доступ к хот-спотам Wi-Fi и доступ к Интернету через Wi-Fi по месту жительства для всех. Такие системы работают и на транспорте. Свободный Wi-Fi можно «получить» на АЗС почти по всему миру, в том числе в России, в кафе, в университетах и некоторых основных школах, в метро, библиотеках и в других местах. Интересную особенность на этот счет я заметил в Финляндии, где в муниципалитетах имеют большое количество свободных хот-спотов Wi-Fi по всей территории страны. «Раздатчик» доступа Wi-Fi находится в здании администрации муниципалитета или в местной библиотеке, а зона его охвата составляет 1,5 км в радиусе. Это реальный пример в коммуне Раутъярви. Разумеется, жители и гости территории ничего не платят за пользование открытым доступом к Интернету, организованным таким образом. Услуга предоставляется за счет муниципалитета. «Минусом» данной и подобного рода организации является незащищенность доступа, то есть шифрование WEP сегодня настолько небезопасно, что его можно признать как вовсе открытый канал связи.

Огромными возможностями подобное решение обладает в части темы нашей книги, когда (рассмотрено в следующих разделах) с помощью развернутой сети Wi-Fi и планшета (КПК) можно осуществить дистанционное управление всем, чем угодно. Предостережения на этот счет также читайте далее.

Почему так происходит? Возможно, в данном случае Wi-Fi-провайдеры строят свободные хот-споты Wi-Fi и хот-зоны. Они считают, что свободный Wi-Fi-доступ привлечёт новых клиентов и инвестиции вернутся.

Тем не менее вне зависимости от исходных целей (привлечение клиентов, создание дополнительного удобства или чистый альтруизм) почти повсеместно растет количество бесплатных хот-спотов, где можно получить доступ к наиболее популярной глобальной сети (Интернет) совершенно бесплатно. Это могут быть и крупные транспортные узлы, где подключиться можно самостоятельно в автоматическом режиме, и бары, где для подключения необходимо попросить карточку доступа у персонала, и даже просто террито-

рии городского ландшафта, являющиеся местом постоянного скопления людей. Стандартами Wi-Fi не предусмотрено шифрование передаваемых данных в открытых сетях. Это значит, что все данные, которые передаются по открытому беспроводному соединению, могут быть прослушаны злоумышленниками при помощи программ-снифферов. К таким данным могут относиться пары логин/пароль, номера банковских счетов, пластиковых карт, конфиденциальная переписка. Поэтому при использовании бесплатных хот-спотов не следует передавать в Интернет подобные данные.

1.6. Вопросы взаимодействия программного обеспечения ПК и сетей Wi-Fi

Уже давно, примерно с 1998 года, операционные системы (далее – ОС) семейства BSD (FreeBSD, NetBSD, OpenBSD) работают с большинством адаптеров. Драйверы для чипов Atheros, Prism, Harris/Intersil и Aironet (от соответствующих производителей Wi-Fi-устройств) обычно входят в ОС BSD, начиная с версии 03.

Адаптеры производства Apple OS X (прежнее название – Mac OS X) поддерживались изначально с системы Mac OS 9. Примерно 10 лет прошло с тех пор, как все настольные компьютеры и ноутбуки Apple Inc. (и телефоны iPhone, плееры iPod Touch, планшетные компьютеры iPad) штатно оснащаются адаптерами Wi-Fi; сеть Wi-Fi, таким образом, является основным решением Apple для передачи данных и полностью поддерживается OS X. Возможен режим работы адаптера компьютера в качестве точки доступа, что позволяет при необходимости связывать компьютеры Macintosh в беспроводные сети в отсутствие инфраструктуры. Darwin и OS X, несмотря на частичное совпадение с BSD, имеют свою собственную, уникальную реализацию Wi-Fi.

В ОС семейства Microsoft Windows поддержка Wi-Fi обеспечивается в зависимости от версии либо посредством драйверов, качество которых зависит от поставщика, либо средствами самой Windows. Про Microsoft Windows XP, поддерживающую настройку беспроводных устройств, говорить не стану, как про устаревшую. Она включала в себя довольно слабую поддержку, но значительно улучшилась с выходом Service Pack 2, а с выходом Service Pack 3 была добавлена поддержка WPA2. Microsoft Windows Vista содержит улучшенную,

по сравнению с Windows XP, поддержку Wi-Fi. Microsoft Windows 7 поддерживает все беспроводные устройства и протоколы шифрования. В ОС Windows 7 есть возможность создавать виртуальные адаптеры Wi-Fi, что теоретически позволило бы подключаться не к одной Wi-Fi-сети, а к нескольким сразу. На практике в Windows 7 поддерживается создание только одного виртуального адаптера, при условии написания специальных драйверов, а это может быть полезно при использовании компьютера в локальной Wi-Fi-сети и одновременно в Wi-Fi-сети, подключенной к Интернету.

1.7. Регистрация оборудования: нужна ли она?

В России легитимное использование Wi-Fi регулируется правилами и требованиями, выработанными Роскомнадзором. В соответствии с решениями Государственной комиссии по радиочастотам (ГКРЧ) от 7 мая 2007 г. № 07-20-03-001 «О выделении полос радиочастот устройствам малого радиуса действия» и от 20 декабря 2011 г. № 11-13-07-1 использование Wi-Fi без получения частного разрешения на использование частот возможно для организации сети внутри зданий, закрытых складских помещений и производственных территорий в полосах 2400–2483,5 МГц (стандарты 802.11b и 802.11g; каналы 1–13) и 5150–5350 МГц (802.11a и 802.11n; каналы 34–64). Для легального использования внеофисной беспроводной сети Wi-Fi (к примеру, для радиоканала между двумя соседними домами) необходимо получение разрешения на использование частот (как в полосе 2,4 ГГц, так и 5 ГГц) на основании заключения экспертизы о возможности использования заявленных РЭС и их электромагнитной совместимости (ЭМС) с действующими и планируемыми для использования РЭС.

Радиоэлектронные средства подлежат регистрации в Роскомнадзоре в соответствии с установленным порядком, см. постановление № 539 – порядок регистрации РЭС. В соответствии с постановлением Правительства Российской Федерации от 13 октября 2011 г. № 837 «О внесении изменений в Постановление Правительства Российской Федерации от 12 октября 2004 г. № 539» не подлежат регистрации, в частности (из пп. 13, 23, 24 приложения):

- пользовательское (оконечное) оборудование передающее, включающее в себя приемное устройство, малого радиуса дей-

ствия стандартов IEEE 802.11, IEEE 802.11.b, IEEE 802.11.g, IEEE 802.11.n (Wi-Fi), работающее в полосе радиочастот 2400–2483,5 МГц, с допустимой мощностью излучения передатчика не более 100 мВт, в том числе встроенное либо входящее в состав других устройств;

- пользовательское (оконечное) оборудование передающее, включающее в себя приемное устройство, малого радиуса действия стандартов IEEE 802.11a, IEEE 802.11.n (Wi-Fi), работающее в полосах радиочастот 5150–5350 МГц и 5650–6425 МГц, с допустимой мощностью излучения передатчика не более 100 мВт, в том числе встроенное либо входящее в состав других устройств;
- устройства малого радиуса действия, используемые внутри закрытых помещений, в полосе радиочастот 5150–5250 МГц с максимальной эквивалентной изотропно излучаемой мощностью передатчика не более 200 мВт;
- устройства малого радиуса действия в сетях беспроводной передачи данных внутри закрытых помещений в полосе радиочастот 2400–2483,5 МГц с максимальной эквивалентной изотропно излучаемой мощностью передатчика не более 100 мВт при использовании псевдослучайной перестройки рабочей частоты.

Юридический статус Wi-Fi различен в разных странах. В США диапазон 2,5 ГГц разрешается использовать без лицензии, при условии что мощность не превышает определённую величину и такое использование не создаёт помех тем, кто имеет лицензию. В разных странах мира существуют определенные требования к организации сетей Wi-Fi и безопасности доступа пользователей. К примеру, в Украине использование Wi-Fi без разрешения Украинского государственного центра радиочастот (Український державний центр радіочастот) возможно лишь в случае использования точки доступа со стандартной всенаправленной антенной (< 6 дБ, мощность сигнала ≤ 100 мВт на 2,4 ГГц и ≤ 200 мВт на 5 ГГц) для внутренних (использование внутри помещения) потребностей организации (Решение Национальной комиссии по регулированию связи Украины № 914 от 6 сентября 2007 г.). В случае использования внешней антенны необходимо регистрировать передатчик и получить разрешение на эксплуатацию радиоэлектронного средства от ДП УДЦР. Кроме того, для деятельности по предоставлению телекоммуникационных услуг с применением Wi-Fi необходимо полу-

чить лицензию от «НКРЗІ». В Белоруссии действует специализированная Государственная комиссия по радиочастотам (ГКРЧ) (белор. Дзяржаўная камісія па радыёчастотах (ДзКРЧ)). На основе постановления Министерства связи и информатизации Республики Беларусь от 26 августа 2009 г. № 35 «Перечень радиоэлектронных средств и (или) высокочастотных устройств, не подлежащих регистрации» оборудование Wi-Fi не требует регистрации, при условии что его параметры удовлетворяют следующим требованиям:

- абонентские станции широкополосного беспроводного доступа, использующие полосы радиочастот 2400–2483,5 МГц, 2500–2700 МГц, 5150–5875 МГц и не использующие внешних антенн (антенн, устанавливаемых вне зданий и сооружений), а также абонентские станции широкополосного беспроводного доступа сети электросвязи общего пользования, использующие полосы радиочастот 3400–3800 МГц, 5470–5875 МГц [22].

1.8. Принудительное подавление Wi-Fi с помощью специальных генераторов

Внимание, важно!

Существует несколько способов блокировки Wi-Fi-сетей, и чем слабее роутер (мощность его сигнала), тем легче блокировать. В быту для этой цели достаточно применить простейшие «глушилки» из КНР, к примеру ту, что представлена на рис. 1.3.



Рис. 1.3. Устройство-глушитель сигнала Wi-Fi модели TG-120Ф

Устройство-глушитель сигнала Wi-Fi представляет собой генератор «белого шума», реализованный на несущей частоте 2,4 ГГц.

Портативный подавитель сотовой связи «Скорпион PS TG-120A-Pro» предназначен для подавления стандартов сотовой связи, таких как GSM 900/1800 и сети третьего поколения 3G, а также стандартов цифровой передачи данных: Wi-Fi и Bluetooth. Устройство «Скорпион PS TG-120A-Pro» предназначено для людей, которым нужна уверенность, чтобы их конфиденциальная информация не стала доступна третьим лицам через средства прослушки с помощью GSM/3G-жучков. Подавитель можно применять в помещениях малого и среднего размера, где использование сотовых телефонов нежелательно, или для обеспечения рабочей обстановки во время проведения переговоров, совещаний и т. д. Устройство можно использовать для защиты от любого скачивания информации как по сетям мобильного Интернета GPRS/EDGE/3G, так и по каналам Wi-Fi и Bluetooth. Таким образом, подавитель обеспечит защиту от передачи информации по каналам Интернета на удаленный компьютер, а также от утечки информации за пределы помещения.

1.8.1. Техническое описание портативного подавителя сотовой, Wi-Fi- и Bluetooth-связи «Скорпион 120A-Pro» (Noname)

Дальность подавления Wi-Fi: 30 м.

Питание: аккумулятор с возможностью подзарядки с помощью адаптера 220 В – 12 В.

Ширина полосы и каналы подавления: 4 канала.

GSM900: 925–960 МГц.

GSM1800: 1805–1880 МГц.

3G: 2110–2170 МГц.

Wi-Fi/BT: 2400–2500 МГц.

Температурный режим эксплуатации: –10...+50 °С.

Время работы от встроенного аккумулятора: до 90 мин.

Время зарядки устройства: 4–5 ч.

Относительная влажность: 5...80% без конденсата.

Размер: 113×61×31 мм.

Вес: 275 г.

Конец ознакомительного фрагмента.
Приобрести книгу можно
в интернет-магазине
«Электронный универс»
e-Univers.ru