МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«Вятский государственный университет»**

Факультет автоматики и вычислительной техники

Кафедра электронных вычислительных машин

ТЕХНОЛОГИЯ WI-FI

Доклад по дисциплине

«Интерфейсы периферийных устройств»

Выполнила студентка группы ИВТ-42\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Метелёва М.Д./

Проверил ассистент кафедры ЭВМ\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Гагарский К.Н./

Киров 2017

1. **Введение**

Wi-Fi – это возможность передачи данных между устройствами на короткие дистанции без помощи проводов. Устройства, подключенные по беспроводной технологии, образуют сеть.

Технология Wi-Fi одна из самых перспективных на сегодняшний день в области компьютерной связи. Wi-Fi (Wireless Fidelity) — в переводе с английского — «беспроводная точность». Технологией Wi-Fi называют один из форматов передачи цифровых данных по радиоканалам.

Изначально устройства Wi-Fi были предназначены для корпоративных пользователей, чтобы заменить традиционные кабельные сети. Для проводной сети требуется тщательная разработка топологии сети и прокладка вручную многих сотен метров кабеля.

Сеть WLAN (Wireless Local Area Network — беспроводная локальная сеть) — вид локальной вычислительной сети (LAN), использующий для связи и передачи данных между узлами высокочастотные радиоволны, а не кабельные соединения. Это гибкая система передачи данных, которая применяется как расширение — или альтернатива — кабельной локальной сети внутри одного офиса, здания или в пределах определенной территории.

Данная технология позволяет экономить средства за счет отсутствия необходимости прокладывать метры кабеля, а простота установки не отнимает время на сложные ремонто-технические работы. Расширение и реконфигурация сети для WLAN не является сложной задачей: пользовательские устройства можно интегрировать в сеть, установив на них беспроводные сетевые адаптеры.

Беспроводные сети используют радиочастоты, поскольку радиоволны внутри помещения проникают через стены и перекрытия. Диапазон или область охвата большинства систем WLAN достигает 160 м, в зависимости от количества и вида встреченных препятствий. Беспроводные сети обычно более надежны, чем кабельные. Скорость работы сравнима со скоростью кабельной сети. Точно так же, как и в обычной сети, пропускная способность сети WLAN зависит от ее топологии, загрузки, расстояния до точки доступа и т.д. Количество пользователей практически неограниченно. Его можно увеличивать, просто устанавливая новые точки доступа. С помощью перекрывающихся точек доступа, настроенных на разные частоты (каналы), беспроводную сеть можно расширить за счет увеличения числа пользователей в одной зоне. Ядром такой сети является точка доступа (Access Point). Вокруг неё образуется территория радиусом 50-100 метров, называемая хот-спотом, или зоной Wi-Fi.

Все чаще в последнее время в мировых ИТ-новостях встречаются сообщения о компаниях, использующих технологию Wi-Fi в повседневной работе или предоставляющих Wi-Fi услуги клиентам, а также анонсы различных устройств со встроенной поддержкой Wi-Fi, будь то мобильные телефоны или ноутбуки. Освоение этой технологии осуществляется гигантскими темпами, и многие аналитики давно предрекают ей сказочный успех, который может кардинально изменить сегодняшний подход к использованию компьютеров и мобильных устройств.

Стандарт Wi-Fi появился еще в середине 90-х и начал активно продвигаться с 2000 года. Данная технология сейчас развивается гигантскими темпами: внедрение Wi-Fi происходит повсеместно во всем развитом мире.

1. **История**

Отцом-основателем Wi-Fi является австралийский инженер Джон О’Салливан, который в 1991 году разработал первую версию протокола. В этом же году американская компания At&t выпускает первое устройство беспроводной передачи данных, которое работает на частоте 2.4gHz. Устройство назвали WaveLan. Стоит отметить, что скорость передачи данных составляла не более 2 Мбит/с.

Основные даты в истории развития технологии:

* в***1997*** году выходит спецификация 802.11, которая не имела особых отличий от WaveLan, скорость передачи данных не более 2 Мбит/с;
* в ***2000*** году появляется новая спецификация 802.11b, скорость передачи данных до 11 Мбит/с;
* ***2002*** год — выходит новая версия — 802.11a, передача данных на частоте 5 ГГц, скорость обмена до 54 Мбит/с;
* ***2003*** год ознаменован появлением 802.11g, 54 Мбит/с теперь возможно и на частоте 2.4 ГГц, появился протокол шифрования WPA;
* ***2004*** год — шифрование переходит на новый уровень безопасности, мир увидел WPA2;
* ***2009*** год — официально представлены устройства с поддержкой стандарта 802.11n, скорость передачи данных до 600 Мбит/с на частотах 5 ГГц и 2.4 ГГц, данный стандарт используется в большинстве современных смартфонов 2016 года.
* ***2014*** год — появляется стандарт 802.11ac, скорость передачи данных более 1 Гбит/с;
* ***2016*** год — ведется разработка стандарта 802.11ad, скорость передачи данных от 7 Гбит/с, работа в диапазоне 60 Г Гц.

1. **Принцип работы**

Для осуществления передачи информации требуется соблюдение всего трех обязательных условий: наличие сети интернет, точки доступа, роль которой выполняет Wi-Fi роутер, а также устройства, имеющего доступ к роутеру посредством Wi-Fi модуля (этим устройством может быть ноутбук, планшет, смартфон и т. п.).

Используемые в сетях Wi-Fi устройства похожи на используемые в мобильных телефонах и работают по аналогичному принципу. Главное отличие заключается в разнице частот: Wi-Fi устройства функционируют на частотах 2,4 ГГц или 5 ГГц, это намного больше, чем в мобильных устройствах.

Обычно схема Wi-Fi сети содержит не менее одной точки доступа и не менее одного клиента. Также возможно подключение двух клиентов в режиме точка-точка, когда точка доступа не используется, а клиенты соединяются посредством сетевых адаптеров «напрямую». Точка доступа передаёт свой идентификатор сети (SSID) с помощью специальных сигнальных пакетов на скорости 0.1 Мбит/с каждые 100 мс. Так что 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, приёмник может выбирать между ними на основании данных об уровне сигнала. Расстояние передачи информации посредством Wi-Fi роутера колеблется и зависит от мощности передатчика. В среднем этот показатель равняется двумстам метрам, однако существуют очень мощные роутеры, которые позволяют передавать сигнал на расстояние до одного километра. В основном такие Wi-Fi роутеры используются в офисных зданиях, в общественных местах и других подобного рода пространствах.

На скорость передачи информации значительным образом влияет количество работающих в конкретной сети абонентов. Чем выше число пользующихся услугами конкретной Wi-Fi точки доступа устройств, тем выше вероятность падения скорости потока интернет. Поэтому существует два пути решения данной проблемы: защита сети индивидуальным паролем или расстановка приоритетов. Второй способ очень часто используется в крупных компаниях.



*Рисунок 1 – Принцип работы Wi-Fi*

1. **Основные элементы сети**

К основным элементам сети относят:

* ***Беспроводные клиенты***. Это компьютеры и другое оборудование (принтеры, проекторы, устройства хранения данных и т. д.), которое взаимодействует с Wi-Fi сетью.
* ***Точка доступа или роутер (маршрутизатор)***. Точка доступа – это устройство, которое принимает входящий интернет-трафик по кабелю или по беспроводному каналу и раздает его на несколько клиентов. В список его функций могут входить присвоение входящим в сеть компьютерам IP-адресов, обеспечение сетевой защиты, маршрутизация пакетов данных, ограничение скорости трафика и т. д.

Антенны являются частью точек доступа, и основным их предназначением является усиление сигнала передатчика. Антенны могут быть, как интегрированными (внутренними), так и внешними. Последние, в свою очередь, делятся на несколько видов:

1. всенаправленные (OMNI)
2. панельные
3. секторные
4. параболические (тарелки или с сетчатым рефлектором)

* ***Адаптеры***. Это устройства, которые подключаются к компьютерам для приема и передачи данных по беспроводным каналам. Все современные мобильные устройства и некоторые модели стационарных ПК уже оснащены встроенными Wi-Fi адаптерами, для их подключения к точке доступа или роутеру.
* ***Беспроводные мосты***. Это оборудование, которое используется для объединения двух и более клиентов в локальную беспроводную сеть.
* ***Контроллеры***. Это оборудование используется для управления масштабными беспроводными сетями, например, Wi-Fi сетью большого офисного центра или промышленного комплекса. Контроллер беспроводных точек доступа не только выполняет функцию управления, но и отвечает за безопасность сети, мониторинг, распределение нагрузки между точками доступа, обеспечение бесшовного покрытия, реализацию гостевого доступа и т. д. Использование контроллера позвонить расширить функционал и производительность Wi-Fi сети, сократив время локализации устранения неисправностей, тем самым снизив эксплуатационные расходы по обслуживанию беспроводной сети.
* ***Зона обслуживания* (*****Service******Set* – SS)**. Логически сгруппированные устройства, обеспечивающие подключение к беспроводной сети.
* ***Базовая зона обслуживания* (*****Basic******Service******Set* –*****BSS*)**. Группа станций, которые связываются друг с другом по беспроводной связи. Технология BSS предполагает наличие особой станции, которая называется точкой доступа (access point).

Помимо обязательного оборудования в состав компонентов беспроводной сети могут входить Wi-Fi видеокамеры, серверы печати, стереосистемы и другая дополнительная техника.

1. **Стандарты беспроводных сетей**

Разработкой стандартов WiFi 802.11 занимается организация IEEE (Институт инженеров электротехники и электроники — IEEE (англ. Institute of Electrical and Electronics Engineers; I triple E — «Ай трипл и») — международная некоммерческая ассоциация специалистов в области техники, мировой лидер в области разработки стандартов по радиоэлектронике, электротехнике и аппаратному обеспечению вычислительных систем и сетей.)

* ***IEEE 802.11*** – базовый стандарт для сетей Wi-Fi, который определяет набор протоколов для самых низких скоростей передачи данных (transfer).

Существует несколько разновидностей WLAN-сетей, которые различаются схемой организации сигнала, скоростями передачи данных, радиусом охвата сети, а также характеристиками радиопередатчиков и приемных устройств. Наибольшее распространение получили беспроводные сети стандарта IEEE 802.11b, IEEE 802.11g и IEEE 802.11n.

Первыми в 1999 г. были утверждены спецификации 802.11a и 802.11b, тем не менее наибольшее распространение получили устройства, выполненные по стандарту 802.11b.

* Стандарт ***802.11b*** основан на методе широкополосной модуляции с прямым расширением спектра (Direct Sequence Spread Spectrum, DSSS). Весь рабочий диапазон делится на 14 каналов, разнесенных на 25 МГц для исключения взаимных помех. Данные передаются по одному из этих каналов без переключения на другие. Возможно одновременное использование всего 3 каналов. Скорость передачи данных может автоматически меняться в зависимости от уровня помех и расстояния между передатчиком и приемником.

Стандарт IEEE ***802.11b*** реализует максимальную теоретическую скорость передачи 11 Мбит/с, что сравнимо с кабельной сетью 10 BaseT Ethernet. Следует учитывать, что такая скорость возможна при передаче данных одним WLAN-устройством. Если в среде одновременно функционирует большее число абонентских станций, то полоса пропускания распределяется между всеми и скорость передачи данных на одного пользователя падает.

* Стандарт ***802.11a*** был принят в 1999 году, тем не менее нашел свое применение только с 2001 года. Данный стандарт используется, в основном, в США и Японии. В России и в Европе он не получил широкого распространения.

 В стандарте 802.11a применяется схема модуляции сигнала - мультиплексирование с разделением по ортогональным частотам (Orthogonal Frequency Division Multiplexing, OFDM). Основной поток данных разделяется на несколько параллельных субпотоков с относительно низкой скоростью передачи, и затем для их модуляции применяется соответствующее число несущих. Стандартом определены три обязательные скорости передачи данных (6, 12 и 24 Мбит/с) и пять дополнительных (9, 18, 24, 48 и 54 Мбит/с). Также имеется возможность одновременного использования двух каналов, что повышает скорость передачи данных в 2 раза.

* Стандарт ***802.11g*** окончательно был утверждён в июне 2003г. Он является дальнейшим усовершенствованием спецификации IEEE 802.11b и реализует передачу данных в том же частотном диапазоне. Главным преимуществом этого стандарта является повышенная пропускная способность - скорость передачи данных в радиоканале достигает 54 Мбит/с по сравнению с 11 Мбит/с у 802.11b. Как и IEEE 802.11b, новая спецификация функционирует в диапазоне 2,4 ГГц, однако для повышения скорости используется та же схема модуляции сигнала, что и в 802.11a - ортогональное частотное мультиплексирование (OFDM).

 Стандарт 802.11g совместим с 802.11b. Так адаптеры 802.11b могут работать в сетях 802.11g (но при этом не быстрее 11 Мбит/с), а адаптеры 802.11g могут снижать скорость передачи данных до 11 Мбит/с для работы в старых сетях 802.11b.

Стандарт 802.11n был ратифицирован 11 сентября 2009. Он увеличивает скорость передачи данных практически в 4 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. Максимальная теоретическая скорость передачи данных составляет 600 Мбит/с, применяя передачу данных сразу по четырём антеннам. По одной антенне – до 150 Мбит/с.

* Устройства ***802.11n*** функционируют в частотных диапазонах 2,4 – 2,5 или 5,0 ГГц.

Большинство функционала стандарта IEEE 802.11n позаимствовано из стандарта 802.11a, тем не менее в стандарте IEEE 802.11n имеется возможность применения как частотного диапазона, принятого для стандарта IEEE 802.11a, так и частотного диапазона, принятого для стандартов IEEE 802.11b/g. Таким образом, устройства, поддерживающие стандарт IEEE 802.11n, могут функционировать в частотном диапазоне либо 5, либо 2,4 ГГц, причем конкретная реализация зависит от страны. Для России устройства стандарта IEEE 802.11n будут поддерживать частотный диапазон 2,4 ГГц.

Увеличение скорости передачи в стандарте IEEE 802.11n достигается за счет: удвоения ширины канала с 20 до 40 МГц.

Более кратко:

* IEEE ***802.11*** - определяет набор протоколов для самых низких скоростей передачи данных и является базовым стандартом WLAN.
* IEEE ***802.11a*** - Протокол не совместим с 802.11b и несет в себе более высокие скорости передачи чем 11b. Использует частотные каналы в спектре 5GHz. Максимальная пропускная способность до 54Мбит/c.
* IEEE ***802.11b*** - стандарт использует более быстрые скорости передачи и вводит больше технологических ограничений. Использует частотные каналы в спектре 2.4GHz. Максимальная пропускная способность до 11Мбит/c.
* IEEE ***802.11g*** - стандарт использует скорости передачи данных эквивалентные 11а. Используются частотные каналы в спектре 2.4GHz. Протокол совместим с 11b. Максимальная пропускная способность до 54Мбит/c.
* IEEE ***802.11n*** - на данный момент это cамый передовой коммерческий Wi-Fi стандарт, который использует частотные каналы в спектрах 2.4GHz и 5GHz. Совместим с 11b/11a/11g. Максимальная пропускная способность до 300 Мбит/c.

1. **Режимы работы точки доступа**

* **Access Point Mode** (Точка доступа) - Режим Access Point предназначен для беспроводного подключения к точке доступа портативных компьютеров, настольных ПК и PDA. Беспроводные клиенты могут обращаться к точке доступа только в режиме Access Point.
* **Access Point Client / Wireless Client Mode** (Беспроводной клиент) - Режим AP Client или Wireless Client позволяет точке доступа стать беспроводным клиентом другой точки доступа. По существу, в данном режиме точка доступа выполняет функции беспроводного сетевого адаптера. Вы можете использовать данный режим для обмена данными между двумя точками доступа. Обмен данными между беспроводной платой и точкой доступа в режиме Access Point Client / Wireless Client Mode невозможен.
* **Point-to-Point / Wireless Bridge** (Беспроводной мост point-to-point) - Режим Point-to-Point / Wireless Bridge позволяет беспроводной точке обмениваться данными с другой точкой доступа, поддерживающей режим беспроводного моста point-to-point. Однако имейте в виду, что большинство производителей используют свои собственные оригинальные настройки для активации режима беспроводного моста в точке доступа. Обычно данный режим используется для беспроводного соединения аппаратуры в двух разных зданиях. Беспроводные клиенты не могут обмениваться данными с точкой доступа в этом режиме.
* **Point-to-Multipoint / Multi-point Bridge** (Беспроводной мост point-to-multipoint) - Режим Point-to-Multi-point / Multi-point Bridge аналогичен режиму Point-to-point / Wireless Bridge с той лишь разницей, что допускает использование более двух точек доступа. Беспроводные клиенты также не могут обмениваться данными с точкой доступа в этом режиме.
* **Repeater Mode** (Репитер) - Функционируя в режиме беспроводного репитера, точка доступа расширяет диапазон действия беспроводной сети посредством повтора сигнала удаленной точки доступа. Для того чтобы точка доступа могла выполнять функции беспроводного расширителя радиуса действия другой точки доступа, в её конфигурации необходимо указать Ethernet MAC-адрес удаленной точки доступа. В данном режиме беспроводные клиенты могут обмениваться данными с точкой доступа.
* **WDS** (Wireless Distribution System) - позволяет одновременно подключать беспроводных клиентов к точкам, работающим в режимах Bridge (мост точка-точка) или Multipoint Bridge (мост точка-много точек), однако при этом уменьшается скорость работы.

Все точки доступа и беспроводные маршрутизаторы, продаваемые в настоящее время, легко конфигурируются через web-интерфейс, для чего необходимо при первом подключении их к сети обратиться через web-браузер по определённому IP-адресу, указанному в документации к устройству (в некоторых случаях потребуются специальные настройки протокола TCP/IP на компьютере, используемом для конфигурирования точки доступа или маршрутизатора, также указанные в документации). Оборудовнаие многих производителей также комплектуется специальным ПО, позволяющим облегчить процедуру настройки для пользователей.      Специфичные сведения, необходимые для настройки роутера для работы с вашим провайдером практически всегда можно узнать на сайте самого провайдера.

1. **Частотные полосы и каналы Wi-Fi**

***Используемые частоты и каналы в диапазоне 2.4 ГГц***

Для беспроводной Wi-Fi связи используется определенный диапазон частот, причем в зависимости от страны, этот диапазон может быть различным. Весь диапазон частот разбит на несколько каналов, на которых может работать оборудование. Стандарты 802.11b, 802.11g и 802.11n определяют следующие каналы таблица 1.

*Таблица 1 – Используемые частоты и каналы в диапазоне 2.4 ГГц*

|  |  |  |
| --- | --- | --- |
| ***Канал*** | ***Частота, ГГц*** | ***Страны*** |
| *1* | 2,412 | США, Европа, РФ, Япония |
| *2* | 2,417 | США, Европа, РФ, Япония |
| *3* | 2,422 | США, Европа, РФ, Япония |
| *4* | 2,427 | США, Европа, РФ, Япония |
| *5* | 2,432 | США, Европа, РФ, Япония |
| *6* | 2,437 | США, Европа, РФ, Япония |
| *7* | 2,442 | США, Европа, РФ, Япония |
| *8* | 2,447 | США, Европа, РФ, Япония |
| *9* | 2,452 | США, Европа, РФ, Япония |
| *10* | 2,457 | США, Европа, РФ, Япония |
| *11* | 2,462 | США, Европа, РФ, Япония |
| *12* | 2,468 | Европа, РФ, Япония |
| *13* | 2,472 | Европа, РФ, Япония |
| *14* | 2,484 | Япония |

Из таблицы 1 видно, что шаг каналов в диапазоне 2.4 ГГц составляет 5 МГц, а ширина канала составляет 20МГц. Таким образом, спектр рабочих частот оборудования перекрывается и независимых каналов, работа на которых возможна без взаимных помех, всего три – например 1 (2,412 ГГц), 6 (2,437 ГГц) и 11 (2,462 ГГц), частоты которых отличаются более чем на 20 МГц. Можно также использовать как независимые каналы 2, 7, 12 или 3, 8, 13.

***Используемые частоты и каналы в диапазоне 5 ГГц***

Для беспроводной Wi-Fi связи в диапазоне 5 ГГц используется два диапазона частот 5150МГц–5350МГц (нижний диапазон) и 5470МГц–5850МГц (верхний диапазон).

Стандарт 802.11а определяет следующие каналы таблица 2.

*Таблица 2 – Используемые частоты и каналы в диапазоне 5 ГГц*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Канал*** | *34* | *36* | *38* | *40* | *42* | *44* | *46* | *48* | *50* | *52* | *54* | *56* | *58* | *60* |
| ***Частота, ГГц*** | 5,170 | 5,180 | 5,190 | 5,200 | 5,210 | 5,220 | 5,230 | 5,240 | 5,250 | 5,260 | 5,270 | 5,280 | 5,290 | 5,300 |
| ***Канал*** | *62* | *64* | *100* | *104* | *108* | *112* | *116* | *120* | *124* | *128* | *132* | *136* | *140* | *147* |
| ***Частота, ГГц*** | 5,310 | 5,320 | 5,500 | 5,520 | 5,540 | 5,560 | 5,580 | 5,600 | 5,620 | 5,640 | 5,660 | 5,680 | 5,700 | 5,735 |
| ***Канал*** | *149* | *15* | *152* | *153* | *155* | *157* | *159* | *160* | *161* | *163* | *165* | *167* | *171* | *173* |
| ***Частота, ГГц*** | 5,745 | 5,755 | 5,760 | 5,765 | 5,775 | 5,785 | 5,795 | 5,800 | 5,805 | 5,815 | 5,825 | 5,835 | 5,855 | 5,865 |
| ***Канал*** | *177* | *180* |  |  |  |  |  |  |  |  |  |  |  |  |
| ***Частота, ГГц*** | 5,885 | 5,905 |  |  |  |  |  |  |  |  |  |  |  |  |

Из таблицы 2 видно, что шаг каналов в диапазоне 5 ГГц составляет 5 - 20 МГц, а ширина канала составляет 20МГц. Таким образом, спектр рабочих частот оборудования перекрывается и независимых каналов, работа на которых возможна без взаимных помех – 22.

1. **Безопасность в сети Wi-Fi**

Изначально для обеспечения безопасности в сетях 802.11 применялся алгоритм **WEP** (Wired Equivalent Privacy), включавший в себя алгоритм шифрования RC4 c 40-битным или 104-битным ключом и средства распределения ключей между пользователями, однако в 2001 году в нём была найдена принципиальная уязвимость, позволяющая получить полный доступ к сети за конечное (и весьма небольшое время) вне зависимости от длины ключа. Категорически не рекомендуется к использованию в настоящее время.

Поэтому в 2003 году была принята программа сертификации средств беспроводной связи под названием **WPA** (Wi-Fi Protected Access), устранявшая недостатки предыдущего алгоритма. С 2006 года все WiFi-устройства обязаны поддерживать новый стандарт **WPA2**, который отличается от WPA поддержкой более современного алгоритма шифрования **AES** с 256-битным ключом. Также в WPA появился механизм защиты передаваемых пакетов с данными от перехвата и фальсификации. Именно такое сочетание (WPA2/AES) рекомендуется сейчас к использованию во всех закрытых сетях.

У WPA есть два режима авторизации пользователей в беспроводной сети - при помощи RADIUS-сервера авторизации (ориентирован на корпоративных пользователей и крупные сети) и **WPA-PSK** (Pre Shared Key), который предлагается использовать в домашних сетях, а также в небольших офисах.

В этом режиме авторизация по паролю (длиной от 8 до 64 символов) производится на каждом узле сети (точке доступа, роутере или эмулирующем их работе компьютере, сам пароль предварительно задаётся из меню настроек точки доступа или иным специфичным для вашего оборудования способом).

Также во многих современных бытовых Wi-Fi устройствах применяется режим Wi-Fi Protected Setup (**WPS**), также именуемый Wi-Fi Easy Setup, где авторизация клиентов на точке доступа осуществляется при помощи специальной кнопки или вводом pin-кода, уникального для устройства.

Для случаев, когда в сети эксплуатируется фиксированный набор оборудования (т.е. например, мост, созданный при помощи двух точек доступа или единственный ноутбук, подключаемый к беспроводному сегменту домашней сети) наиболее надёжным способом является ограничение доступа по MAC-адресу (уникальный адрес для каждого Ethernet устройства, как проводного, так и беспроводного, в Windows для всех сетевых устройств эти адреса можно прочесть в графе Physical Address после подачи команды ipconfig /all) посредством прописывания в меню точки доступа списка MAC-адресов «своих» устройств и выбор разрешения доступа в сеть только устройствам с адресами из этого списка.

Также у любой беспроводной сети есть уникальный идентификатор – **SSID** (service set identifier), который собственно и отображается как имя сети при просмотре списка доступных сетей, который задаётся при настройке используемой точки доступа (или заменяющего его устройства). При отключении рассылки (broadcast) SSID сеть будет выглядеть для просматривающих доступные сети пользователей как безымянная, а для подключения необходимо знать и SSID, и пароль (в случае использования WPA-PSK, однако само по себе отключение SSID не делает сеть более устойчивой к несанкционированному проникновению извне.

1. **Безопасна ли для здоровья беспроводная связь?**

В последнее время в средствах массовой информации много говорят о том, что продолжительное использование беспроводных сетевых устройств может спровоцировать серьезные заболевания. Однако, на сегодняшний день научные данные, которые подтверждали бы предположения о том, что СВЧ-сигналы (*сверхширокополосные сигналы*) оказывают негативное влияние на здоровье человека, отсутствуют.

Несмотря на недостаток научных данных, предполагается, что беспроводные сети более безопасны для здоровья человека, чем мобильные телефоны. Частотный диапазон сигналов типичной домашней беспроводной сети совпадает с частотным диапазоном сигналов микроволновых печей, но мощность сигналов микроволновых печей и даже мобильных телефонов в 100 - 1000 раз превышает мощность сигналов беспроводных сетевых адаптеров и точек доступа.

В целом, в данном вопросе можно с уверенностью утверждать одно: интенсивность воздействия на человека СВЧ-излучения беспроводных сетей несравнимо меньше воздействия других СВЧ-устройств.

Порядок регистрации радиоэлектронных средств (РЭС) описан в постановлениях Правительства Российской Федерации от 12 октября 2004 г.*№ 539 «О порядке регистрации радиоэлектронных средств и высокочастотных устройств»* и от 25 июля 2007 г. *№ 476 «О внесении изменений в постановление Правительства Российской Федерации от 12 октября 2004 г. № 539 «О порядке регистрации радиоэлектронных средств и высокочастотных устройств»»*.

Согласно постановлению №476 от 25 июля 2007 г. **пользовательское (оконечное) оборудование радиодоступа (беспроводного доступа) в полосе радиочастот 2400 - 2483,5 МГц с мощностью излучения передающих устройств до 100 мВт включительно ИСКЛЮЧЕНО из перечня радиоэлектронных средств и высокочастотных устройств, подлежащих регистрации.** Штатная мощность передатчика всех продаваемых в настоящее время пользовательских Wi-Fi устройств находится в пределах этой цифры, а установка любых антенн, не имеющих активных элементов, её не увеличивает.

1. **Достоинства и недостатки**

***Преимущества Wi-Fi***

* Позволяет развернуть сеть без прокладки кабеля, может уменьшить стоимость развёртывания и расширения сети. Места, где нельзя проложить кабель, например, вне помещений и в зданиях, имеющих историческую ценность, могут обслуживаться беспроводными сетями.
* Wi-Fi-устройства широко распространены на рынке. А устройства разных производителей могут взаимодействовать на базовом уровне сервисов.
* Wi-Fi сети поддерживают роуминг, поэтому клиентская станция может перемещаться в пространстве, переходя от одной точки доступа к другой.
* Wi-Fi - это набор глобальных стандартов. В отличие от сотовых телефонов, Wi-Fi оборудование может работать в разных странах по всему миру.

***Недостатки Wi-Fi***

* Частотный диапазон и эксплуатационные ограничения в различных странах неодинаковы; 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, например, Испания, запрещают использование низкочастотных каналов. Более того, некоторые страны, например, Италия, требуют регистрации всех Wi-Fi сетей, работающих вне помещений, или требуют регистрации Wi-Fi-оператора. В России и Украине также обязательна регистрация сетей Wi-Fi.
* Довольно высокое по сравнению с другими стандартами потребление энергии, что уменьшает время жизни батарей и повышает температуру устройства.
* Самый популярный стандарт шифрования, Wired Equivalent Privacy или WEP, может быть относительно легко взломан даже при правильной конфигурации (из-за слабой стойкости ключа). Несмотря на то, что новые устройства поддерживают более совершенный протокол Wi-Fi Protected Access (WPA), многие старые точки доступа не поддерживают его и требуют замены. Многие организации используют дополнительное шифрование (например, VPN) для защиты от вторжения.
* Wi-Fi имеют ограниченный радиус действия. Типичный домашний Wi-Fi маршрутизатор стандарта 802.11b или 802.11g имеет радиус действия 45 м в помещении и 90 м снаружи. Расстояние зависит также от частоты. Wi-Fi в диапазоне 2.4 ГГц работает дальше, чем Wi-Fi в диапазоне 5 ГГц, и имеет радиус меньше, чем Wi-Fi (и пре-Wi-Fi) на частоте 900 МГц.
* Наложение сигналов закрытой или использующей шифрование точки доступа и открытой точки доступа, работающих на одном или соседних каналах может помешать доступу к открытой точке доступа. Эта проблема может возникнуть при большой плотности точек доступа, например, в больших многоквартирных домах, где многие жильцы ставят свои точки доступа Wi-Fi.
* Неполная совместимость между устройствами разных производителей или неполное соответствие стандарту может привести к ограничению возможностей соединения или уменьшению скорости.