ГБОУ Гимназия №1505

«Московская городская педагогическая гимназия-лаборатория»

**Реферат**

**Беспроводные сети: мифы и реальность**

*автор*: ученица 9 класса «Б»

Точилкина Маргарита

*Руководитель:* Пяткина Г.А.

 Москва

 2015

**Оглавление**

Введение

§1.Причины использования беспроводных сетей и области их применения

§2.Виды беспроводных сетей

§3.Причины различия информационной и полезной скоростей в беспроводных сетях

§4.Безопасность во время подключения к сети

Заключение

Список литературы

***Введение***

*Беспроводные компьютерные сети* (Wireless Area Network) — это технология, позволяющая создавать вычислительные сети, полностью соответствующие стандартам для обычных проводных сетей без использования кабельной проводки[1].В последнее время всё больше и больше устройств оснащается беспроводными модулями передачи данных, так как они позволяют свободно перемещаться в пределах радиоволн и не терять соединение с сетью интернет. С устройствами, использующими беспроводную передачу данных, появилась возможность свободно перемещаться:

1. По комнате или квартире (в случае персональной, реже локальной сети);
2. По офису и другим рабочим помещениям (в случае локальной сети);
3. По зданиям, в которых располагаются государственные учреждения (полиция, больницы и т.д.) (в случае муниципальной или городской сети);
4. По всему городу или стране (в случае глобальной сети).

У каждой такой сети есть свои стандарты, которые определяются в соответствии с радиусом действия и назначением.

Беспроводные персональные сети (Wireless Personal Area Network, WPAN) – сети, стандарт которых разработан рабочей группой IEEE 802.15( *англ. Institute of Electrical and Electronics Engineers) (I triple E — «Ай трипл и») (Институт инженеров по электротехнике и электронике)* [2]. Они применяются для связи различных устройств, включая компьютерную, бытовую и оргтехнику, средства связи и т.д. Радиус их действия составляет от нескольких метров до нескольких десятков сантиметров. К сетевым технологиям WPAN относятся Bluetooth, ZigBee, 6loWPAN, UBW и другие.

Беспроводные локальные сети (Wireless Local Area Network, WLAN) – сети, технологии которых базируются на семействе стандартов IEEE 802.11[3]. Радиус их действия в среднем составляет примерно 200-250 метров. Наиболее распространённым на сегодняшний день способом построения является Wi-Fi.

Беспроводные городские сети (Wireless Metropolitan Area Network, WMAN или жаргонное название WiMAX) – сети стандарта IEEE 802.16[4]. Они предоставляют широкополосный доступ к сети через радиоканал на больших расстояниях для различного спектра устройств. Теоретически эта технология должна обеспечивать покрытые сигналом площади радиусом до 50 км без прямой видимости.

Беспроводные глобальные сети (Wireless Wide Area Network, WWAN) – сети, предназначенные для покрытия сигналом полностью всю страну или даже несколько стран. В стандартах этих сетей принято выделять поколения, которые распределяются по времени их использования. На данный момент основными технологиями являются GSM, LTE, EDGE и GPRS[5].

Но не все знают, что у беспроводных сетей есть свои минусы (некоторые из них являются достаточно серьёзными) и определенные условия для организации точки доступа. В своем реферате я хочу рассмотреть обозначенную проблему .

**Цель исследования** – изучение беспроводных сетей, рассмотрение причин их использования и оценка действительных минусов и плюсов.

**Для выполнения этой цели были поставлены конкретные задачи**:

* Изучить информацию по данной теме реферата
* Объяснить причины использования беспроводных компьютерных сетей
* Изучить виды беспроводных сетей
* Рассмотреть положительные и отрицательные стороны использования беспроводного соединения
* Рассказать о том, как следует обеспечить безопасность во время подключения к сети

 1 Статья "Беспроводные компьютерные сети" интернет ресурса «Диком». [http://dicom.spb.ru/articles/network-and-servers/wireless-computer-networks/](http://dicom.spb.ru/articles/network-and-servers/wireless-computer-networks/%20) Ссылка действительна на 15.03.2015

2 Гусева А.И., Киреев В.С. Вычислительные системы, сети и телекоммуникации: учебник для студенческих учреждений высшего профессионального образования. - М.: Издательский центр "Академия", 2014. C. 101.

3 Там же. С. 105.

4 Там же. С. 108.

5 Там же С. 109-110.**§1**.**Причины использования беспроводных сетей и области их применения**

На данный момент существуют два основных направления применения беспроводных компьютерных сетей:

* Работа в замкнутом объеме (дом, школа, офис и т. п.);
* Соединение удаленных локальных сетей (или удаленных сегментов локальной сети).

Беспроводные сети поддерживают множество приложений, которые выгодны для пользователей тем, что обеспечивают его мобильность и высокую надежность связи в отличие от подверженных сбоев кабельных соединений. Более того, во многих случаях благодаря применению беспроводных сетей достигается существенная экономия средств за счет повышения эффективности труда и уменьшения количества периодов вынужденного бездействия, возникающих при применении проводных сетей. Для использования большинства технологий беспроводных сетей не требуется лицензия, что делает их развертывание довольно простым и экономически выгодным.

В большинстве случаев беспроводная сеть — это расширение уже существующей проводной сети. В этом случае пользователи могут использовать интернет-соединение, находясь в удобном для них месте (в пределах радиуса действия точки беспроводного доступа). Одна из основных причин для развертывания беспроводной сети — необходимость совместного использования одного высокоскоростного канала доступа к Ethernet. При таком типе конфигурирования сети сразу несколько человек могут использовать одно и то же соединение, обеспечиваемое кабельным модемом или цифровой абонентской линией (Digital Subscriber Line, DSL) (рис 1).

*Рис. 1*

Также существует возможность использования беспроводных сетей для обеспечения передачи голосовых сообщений, особенно когда люди приходится очень часто контактировать друг с другом. Локальная беспроводная сеть, рассчитанная на поддержку речевой связи, может полностью заменить проводную телефонную систему в отдельном здании.

Вследствие широкого распространения ноутбуков, PDA (англ. Personal Digital Assistant, КПК, карманный персональный компьютер) и цифровых телефонов наблюдается увеличение потребности в мобильном доступе к Ethernet. Появилась необходимость получать постоянное высокоскоростное мобильное подключение с надежным доступом ко всем информационным ресурсам. Общедоступная беспроводная сеть является средством, позволяющим подключаться к Ethernet людям, находящимся в стадии перемещения из одного места в другое. При использовании беспроводных сетей появилась возможность определять местонахождение людей или предметов. Координаты пользователя могут вводиться в серверную программу, обеспечивающую какой-нибудь сервис, основанный на местонахождении. Системы, реализующие услуги определения местонахождения через беспроводные локальные сети, появляются и на потребительском рынке и пользуются немалой популярностью.

В конечном счете существует три фактора, которые являются причинами для использования беспроводных сетей:

* Фактор мобильности
* Фактор удаленности
* Фактор срочности

**§2.Виды беспроводных сетей**

В этом параграфе я хочу подробнее рассказать о классификациях беспроводных сетей.

1. **WPAN** (англ. *Wireless personal area network*) — беспроводные персональные сети, стандарт которых разработан рабочей группой IEEE 802.15 ( *англ. Institute of Electrical and Electronics Engineers) (I triple E — «Ай трипл и») (Институт инженеров по электротехнике и электронике)* [1]. WPAN применяются для связи различных устройств, включая компьютерную, бытовую и оргтехнику, средства связи и т. д. Физический и канальный уровни основаны на стандарте IEEE 802.15.4. Радиус действия WPAN составляет от нескольких метров до нескольких десятков сантиметров. WPAN используется как для объединения отдельных устройств между собой, так и для связи их с сетями более высокого уровня, например, глобальной сетью интернет. К сетевым технологиям WPAN относятся Bluetooth, ZigBee, 6loWPAN, UBW и другие.
 Беспроводные персональные сети становятся незаменимыми в тех местах, где отсутствует доступ по сотовой мобильной связи или ее использование на территории предприятия запрещено.
Bluetooth (в переводе синий зуб) назван в честь Харальда I Синезубого, правившего в X в. Данией и частью Норвегии и объединив­шего враждовавшие датские племена в единое королевство — про­изводственная спецификация беспроводных персональных сетей WPAN[2]. Bluetooth обеспечивает обмен информацией в радиусе до 100 м другот друга между такими устройствами как персональные ком­пьютеры, мобильные телефоны, принтеры и пр. на надежной, бес­платной, доступной радиочастоте для ближней связи. Принцип действия Bluetooth основан на использовании радиоволн. Его протокол поддерживает не только соединение point-to-point (PPP), но и соединение point-to-multipoint  (P2MP, PTMP или PMP).
 **ZigBee** — спецификация сетевых протоколов верхнего уровня (уровня приложений API*(Интерфейс программирования приложений,англ. application programming interface— набор готовых классов, процедур, функций, структур и констант, предоставляемых приложением (библиотекой, сервисом) для использования во внешних программных продуктах. Используется программистами при написании всевозможных приложений.)*[3] и сетевого уровня), использующих сервисы нижних уровней — уровня управления доступом к среде MAC ( от англ. *Media Access Control* — управление доступом к среде, также *Hardware Address*) — *уникальный идентификатор, присваиваемый каждой единице активного оборудования компьютерных сетей.*[4]) и физического уровня, регламентированных стандартом IEEE 802.15.4.[5] Основными областями применения технологии ZigBee являются беспроводные сенсорные сети, автоматизация жилья («Умный дом» и «Интеллектуальное здание»), медицинское оборудование, системы промышленного мониторинга и управления, а также бытовая электроника и «периферия» персональных компьютеров.
2. **WLAN**  (англ. *Wireless Local Area Network*; WLAN) — беспроводные локальные сети, технологии которых базируются на семействе стандартов IEEE 802.11. [6] При таком способе построения сетей передача данных осуществляется через радиоэфир. Наиболее распространенным является Wi-Fi.
 **Wi-Fi** был создан в 1991 году NCR Corporation/AT&T (впоследствии — Lucent Technologies и Agere Systems) в Ньивегейн, Нидерланды. Продукты, предназначавшиеся изначально для систем кассового обслуживания, были выведены на рынок под маркой WaveLAN и обеспечивали скорость передачи данных от 1 до 2 Мбит/с. Стандарт IEEE 802.11n был утверждён 11 сентября 2009 года. Его применение позволяет повысить скорость передачи данных практически вчетверо по сравнению с устройствами стандартов 802.11g (максимальная скорость которых равна 54 Мбит/с). Теоретически 802.11n способен обеспечить скорость передачи данных до 600 Мбит/с. 27 июля 2011 года Институт инженеров электротехники и электроники (IEEE) выпустил официальную версию стандарта IEEE 802.22. Системы и устройства, поддерживающие этот стандарт, позволят передавать данные на скорости до 22 Мбит/с в радиусе 100 км от ближайшего передатчика.
 Термин «Wi-Fi» изначально был придуман как игра слов для привлечения внимания потребителя «намёком» 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.
3. **WMAN** (Wireless Metropolitan Area Network, или жаргонное название WiMAX(англ. Worldwide Interoperability for Microwave Access) — телекоммуникационная технология, разработанная с целью предоставления универсальной беспроводной связи на больших расстояниях для широкого спектра устройств (от рабочих станций и портативных компьютеров до мобильных телефонов)[7]. Максимальная скорость — до 1 Гбит/с на ячейку. WiMAX является альтернативой прокладке кабеля или линии DSL. Теоретически технология стандарта 802.16 должна обеспечивать покрытие сигналом площади радиусом до 50 км без прямой видимости. В общем виде WiMAX сети состоят из следующих основных частей: базовых и абонентских станций, а также оборудования, связывающего базовые станции между собой, с поставщиком сервисов и с Интернетом. *WiMAX подходит для решения следующих задач:*
1) Соединения точек доступа Wi-Fi друг с другом и другими сегментами Интернета.
2) Обеспечения беспроводного широкополосного доступа как альтернативы выделенным линиям и DSL.
3) Предоставления высокоскоростных сервисов передачи данных и телекоммуникационных услуг.
4) Создания точек доступа, не привязанных к географическому положению.
 Сопоставления WiMAX и Wi-Fi далеко не редкость — термины созвучны, название стандартов, на которых основаны эти технологии, похожи (стандарты разработаны IEEE, оба начинаются с «802.»). Но, несмотря на это, эти технологии направлены на решение абсолютно различных задач.
 **WiMAX** - это система дальнего действия, покрывающая километры пространства, которая обычно использует лицензированные спектры частот для предоставления соединения с интернетом типа точка-точка провайдером конечному пользователю. Разные стандарты семейства 802.16 обеспечивают разные виды доступа, от мобильного (схож с передачей данных с мобильных телефонов) до фиксированного (альтернатива проводному доступу, при котором беспроводное оборудование пользователя привязано к местоположению).
 **Wi-Fi** - это система более короткого действия, обычно покрывающая десятки метров, которая использует нелицензированные диапазоны частот для обеспечения доступа к сети. Обычно Wi-Fi используется пользователями для доступа к их собственной локальной сети, которая может быть и не подключена к Интернету. Если WiMAX можно сравнить с мобильной связью, то Wi-Fi скорее похож на стационарный беспроводной телефон.
4. **WWAN** ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) Wireless Wide Area Network) — беспроводная [глобальная вычислительная сеть](https://ru.wikipedia.org/wiki/%D0%93%D0%BB%D0%BE%D0%B1%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%B2%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C). [8].В стандартах сетей WWAN принято выделять поколения. К первому 1G (The 1-st Generation) относятся аналоговые стандарты, которые постепенно ушли в прошлое. Говоря о втором поколении прежде всего следует сказать о GSM (Global Standard for Mobile Communications) — глобальном стандарте для мобильной сотовой связи. В сотовых цифровых сетях стандарта GSM может передаваться не только оцифрованная речь, но и цифровые данные.
 Возможности мобильного доступа в Интернет были значительно расширены с переходом на использование технологии пакетной передачи данных по радиосетям **GPRS** (General Packet Radio Service), но радикальное увеличение произошло в высокопроизводительных сотовых сетях третьего поколения (3G). Поскольку функциональные возможности сети GPRS меньше, чем у полноценной сети третьего поколения, то данный стандарт получил название 2,5G, что отражает его переходное состояние от второго поколения к третьему.
 **LTE** (Long-Term Evolution) — технология построения сетей беспроводной связи поколения, следующего за 3G, на базе IP-технологий, отличающаяся высокими скоростями передачи данных.[9] Реализация LTE возможна в разных частотных диапазонах — от 1,4 до 20 МГц, а также по различным технологиям разделения — HI FDD (частотное) и TDD (временное). Пиковая скорость в направлении «вверх» может достигать 86,4 Мбит/с на каждую полосу в 20 МГц. Радиус действия базовой станции LTE может быть различным. Оптимальный радиус действия составляет около 5 км, но при необходимости он может достигать 30 км или даже 100 км (при достаточном поднятии антенны). Звонок или сеанс передачи данных, инициированный в зоне покрытия LTE, технически может быть передан без разрыва в сеть 3G (WCDMA), CDMA2000 или в GSM/GPRS/EDGE.

1Гусева А.И., Киреев В.С. Вычислительные системы, сети и телекоммуникации: учебник для студенческих учреждений высшего профессионального образования. - М.: Издательский центр "Академия", 2014. C. 101.
2Там же. С. 101.

3Статья "Интерфейс программирования приложений" интернет - энциклопедии «Википедия». [https://ru.wikipedia.org/wiki/Интерфейс\_программирования\_приложений](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D1%84%D0%B5%D0%B9%D1%81_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F_%D0%BF%D1%80%D0%B8%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B9) Ссылка действительна на 28.03.2015
4Статья "MAC-адрес" интернет - энциклопедии «Википедия». [https://ru.wikipedia.org/wiki/MAC-адрес](https://ru.wikipedia.org/wiki/MAC-%D0%B0%D0%B4%D1%80%D0%B5%D1%81%20) Ссылка действительна на 28.03.2015
5Гусева А.И. Указ. соч. С. 103.

6Там же. С. 100.

7Там же. С. 108.

8Там же. С. 109.

9Там же. С. 110.

**§3.Причины различия информационной и полезной скоростей в беспроводных сетях**

Как известно, в беспроводных сетях в качестве среды распространения сигнала используются радиоволны. В связи с этим на их работу воздействует большее количество различного рода помех. Для начала рассмотрим факторы, которые влияют на работу беспроводных сетей Wi-Fi (IEEE 802.11b/g/n):

1. *Другие Wi-Fi-устройства*, которые работают в радиусе действия основного устройства и используют тот же частотный диапазон (Wi-Fi-устройства подвержены воздействию даже небольших помех).
2. *Bluetooth-устройства*, работающие в зоне покрытия Wi-Fi-устройства.
Они работают в том же частотном диапазоне, что и Wi-Fi-устройства, - 2.4 ГГц, следовательно, могут оказывать влияние на работу беспроводных сетей.
3. *Большие расстояния между Wi-Fi-устройствами.* Беспроводные устройства Wi-Fi имеют ограниченный радиус действия. Например, домашний интернет-центр с точкой доступа Wi-Fi стандарта 802.11b/g имеет радиус действия до 60м в помещении и до 400 м вне помещения.

|  |  |  |
| --- | --- | --- |
| Препятствие | Дополнительные потери (dB) | Эффективное расстояние\* |
| Открытое пространство | 0 | 100% |
| Окно без тонировки (отсутствует металлизированное покрытие) | 3 | 70% |
| Окно с тонировкой (металлизированное покрытие) | 5-8 | 50% |
| Деревянная стена | 10 | 30% |
| Межкомнатная стена (15,2 см) | 15-20 | 15% |
| Несущая стена (30,5 см) | 20-25 | 10% |
| Бетонный пол/потолок | 15-25 | 10-15% |
| Монолитное железобетонное перекрытие | 20-25 | 10% |

1. *Препятствия.* Различные препятствия (стены, потолки, мебель, металлические двери и т.д.), расположенные между Wi-Fi-устройствами, могут частично или значительно отражать/поглощать радиосигналы, что приводит к частичной или полной потере сигнала. Ниже показана таблица потери эффективности сигнала Wi-Fi при прохождении через различные среды (табл.1)[1].

*Табл.1*

**\* Эффективное расстояние** - означает, насколько уменьшится радиус действия после прохождения соответствующего препятствия по сравнению с открытым пространством. Например, если на открытом пространстве радиус действия Wi-Fi до 400 метров, то после прохождения одной межкомнатной стены он уменьшится до 400 м \* 15% = 60 метров. После второй еще раз 60 м \* 15% = 9 метров. А после третьей 9 м \* 15% = 1,35 метров. Таким образом, через три межкомнатные стены, скорее всего, беспроводное соединение установить не получится.

Вне помещений влиять на качество передаваемого сигнала может ландшафт местности (например, деревья, леса, холмы). Атмосферные помехи (дождь, гроза, снегопад) также могут являться причиной уменьшения производительности беспроводной сети (в случае, если радиосигнал передается вне помещений).

1. Различная бытовая техника, работающая в зоне покрытия вашего Wi-Fi-устройства:
* Микроволновые СВЧ-печи. Эти приборы могут ослаблять уровень сигнала Wi-Fi, т.к. обычно также работают в диапазоне 2,4 ГГц.
* Детские радионяни. Эти приборы так же работают в диапазоне 2,4 ГГц .
* Мониторы с ЭЛТ, электромоторы, беспроводные телефоны и другие беспроводные устройства.

Так же, очень часто пользователи путают информационную и полезную скорость беспроводных сетей. На коробках и спецификациях устройств указана теоретически рассчитанная максимальная пропускная способность технологии Wi-Fi для идеальных условий (по сути для вакуума). В реальных условиях пропускная способность и площадь зоны покрытия сети зависят факторов, перечисленных выше. Утилиты операционной системы Windows при подключении по Wi-Fi отображают именно «теоретическую» пропускную способность, а не реальную скорость передачи данных, вводя пользователей в заблуждение (рис.1). Данная цифра отображается драйвером беспроводного адаптера и показывает, какая скорость подключения на физическом уровне используется в настоящее время в рамках выбранного стандарта, то есть операционная система сообщает лишь о текущей (мгновенной) физической скорости подключения. Разница между скоростью подключения, которая отображается в Windows, и реальными показателями объясняется прежде всего большим объемом служебных данных, потерями сетевых пакетов в беспроводной среде и затратами на повторную передачу.

Теоретическая и реальная пропускная способность в сетях Wi-Fi (табл.2)[2].

Рис. 3

*Табл. 2*

|  |  |  |
| --- | --- | --- |
| Стандарт | Максимальная теоретически рассчитанная пропускная способность (Мбит/с) | Максимальная реальная скорость передачи данных (Мбит/с) |
| IEEE 802.11a | До 54 | До 24 |
| IEEE 802.11g | До 54 | До 24 |
| IEEE 802.11n | До 150 | До 50 |
| IEEE 802.11n | До 300 | До 100 |

Одной из наиболее серьезных проблем в беспроводных сетях является проблема скрытого узла, ведущая к существенному падению производительности сети. Узлы беспроводной сети для доступа к среде передачи данных используют алгоритм [CSMA/CA](http://irne.ru/articles/wireless/csma-ca.html) — алгоритм множественного доступа с контролем несущей и предотвращением коллизий. CSMA/CA - Carrier Sense Multiple Access With Collision Avoidance или Carrier sensing multiple access with collision avoidance , "множественный доступ с контролем несущей и избеганием коллизий" или "многостанционный доступ с контролем несущей и предотвращением конфликтов" (перевод в русском тексте рекомендации ITU-R [M.1450](https://ru.wikipedia.org/w/index.php?title=M.1450&action=edit&redlink=1)) — это [сетевой протокол](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB), в котором:

* используется схема прослушивания несущей волны
* станция, которая собирается начать передачу, посылает [jam signal](https://ru.wikipedia.org/wiki/Jam_signal%22%20%5Co%20%22Jam%20signal) (сигнал затора)
* после продолжительного ожидания всех станций, которые могут послать jam signal, станция начинает передачу [фрейма](https://ru.wikipedia.org/wiki/%D0%A4%D1%80%D0%B5%D0%B9%D0%BC_%28%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D0%BE%D0%BC%D0%BC%D1%83%D0%BD%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D0%B8%29)
* если во время передачи станция обнаруживает jam signal от другой станции, она останавливает передачу на отрезок времени случайной длины и затем повторяет попытку[3]

Согласно алгоритма CSMA/CA узел перед началом передачи кадра прослушивает среду, и если среда свободна, он может начать передачу. Если все узлы беспроводной сети способны «слышать» друг друга, вероятность коллизий *(наложение двух и более кадров (пакетов) от станций, пытающихся передать кадр в один и тот же момент времени из-за наличия задержки распространения сигнала по сети или наличия неисправной сетевой платы)*[4] низкая. Проблемы начинаются, когда некоторые узлы не могут «услышать» передачу других узлов, например, по причине большой удаленности. CSMA/CA поддерживает два режима работы: контроль несущей (carrier sense) и контроль виртуальной несущей (virtual carrier sense).

Рассмотрим работу каждого из этих режимов.

1. **Carrier scence**

Этот режим, как правило, используется по умолчанию в беспроводных сетевых устройствах. Любая станция, собирающаяся начать передачу, прослушивает канал, при этом устанавливая таймер обратного отсчета (backoff timer), в течение которого непрерывно прослушивают эту среду. Если канал свободен — станция передает кадр, если нет — ожидает его освобождения. Обнаружение коллизий происходит с помощью механизма подтверждений: есть подтверждение от получателя — данные успешно переданы, нет — произошла коллизия. В данном режиме работы алгоритм CSMA/CA минимизирует количество коллизий в сети, но предотвратить их полностью не может.

1. **Virtual carrier scence**

Этот режим позволяет обойти проблему скрытого узла благодаря использованию механизма запроса/разрешения на передачу. Как правило, он доступен только в более дорогих сетевых картах и точках доступа. Кратко работу CSMA/CA в этом режиме можно описать следующим образом. Перед началом передачи узел отправляет RTS-кадр (Request to Send) — запрос на передачу. Точка доступа получает RTS-кадр и, если среда свободна, отправляет CTS-кадр (Clear to Send) с указанием времени, в течении которого разрешено передавать данные. Все станции в зоне досягаемости точки доступа «услышав» CTS-кадр должны сохранять режим радиомолчания на указанное время. Использование RTS/CTS-кадров позволяет существенно повысить производительность сети, где имеется проблема скрытого узла. Однако, если такой проблемы нет, включение механизма RTS/CTS приводит к дополнительным временным задержкам и накладным расходам, что в свою очередь, наоборот, приводит к падению производительности сети. По умолчанию механизм RTS/CTS в сетевых устройствах отключен.

 1Статья "Что влияет на работу беспроводных сетей Wi-Fi? Что может являться источником помех и каковы их возможные причины?". <http://zyxel.ru/kb/2082> Ссылка действительна на 28.03.2015

# 2 Статья "О влиянии беспроводных маршрутизаторов на скорость Интернет-соединения" интернет-жунрнала «Bytemag». <http://www.bytemag.ru/articles/detail.php?ID=18602> Ссылка действительна на 28.03.20153Статья "CSMA/CA" интернет - энциклопедии «Википедия». [https://ru.wikipedia.org/wiki/CSMA/CA](https://ru.wikipedia.org/wiki/CSMA/CA%20) Ссылка действительна на 28.03.2015

# 4Статья "Коллизия кадров" интернет - энциклопедии «Википедия». [https://ru.wikipedia.org/wiki/Коллизия\_кадров](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BB%D0%BB%D0%B8%D0%B7%D0%B8%D1%8F_%D0%BA%D0%B0%D0%B4%D1%80%D0%BE%D0%B2%20) Ссылка действительна на 28.03.2015

# §4.Безопасность во время подключения к сети

Безопасность очень важна для беспроводных сетей, так как коммуникационные сигналы при их распространении через радиоэфир доступны для перехвата. В конфигурации беспроводных сетей предусмотрено две основные функции, которые обеспечивают безопасность: шифрование (encryption) и аутентификация (authentication). По сути, существуют две главные угрозы: несанкционированное подключение и прослушивание, но их список можно расширить, выделить следующие основные угрозы:

* неконтролируемое использование и нарушение периметра;
* несанкционированное подключение к устройствам и сетям;
* перехват и модификация трафика;
* нарушение доступности;
* позиционирование устройства.

Шифрование изменяет биты каждого пакета данных с тем, чтобы злоумышленник не смог их декодировать. Незашифрованные данные называют открытым текстом (plaintext), который легко декодировать, используя средства для пассивного прослушивания сети. В процессе шифрования открытый текст превращается в зашифрованный, а декодировать его можно только с помощью секретного ключа.

Одним из первых алгоритмов для шифрования является **WEP** (Wired Equivalent Privacy). Он используется для обеспечения конфиденциальности и защиты передаваемых данных авторизированных пользователей беспроводной сети от прослушивания. Существует две разновидности WEP: WEP-40 и WEP-104, различающиеся только длиной ключа. В настоящее время данная технология является устаревшей, так как ее взлом может быть осуществлен всего за несколько минут. Тем не менее, она продолжает широко использоваться. [Wi-Fi Alliance](https://ru.wikipedia.org/wiki/Wi-Fi_Alliance) в 2003 представил свой собственный промежуточный вариант этого стандарта - [WPA](https://ru.wikipedia.org/wiki/WPA) (Wi-Fi Protected Access).

 **WPA** использует протокол целостности временных ключей [TKIP](https://ru.wikipedia.org/wiki/TKIP) (Temporal Key Integrity Protocol). Также в нём используется метод контрольной суммы [MIC](https://ru.wikipedia.org/wiki/%D0%98%D0%BC%D0%B8%D1%82%D0%BE%D0%B2%D1%81%D1%82%D0%B0%D0%B2%D0%BA%D0%B0) (Message Integrity Code), которая позволяет проверять целостность пакетов .

 В 2004 Wi-Fi Alliance выпустили стандарт **WPA2**, который представляет собой улучшенный WPA. Основное различие между WPA и WPA2 заключается в технологии шифрования: TKIP (англ. Temporal Key Integrity Protocol)и AES (англ.Advanced Encryption Standard). WPA2 обеспечивает более высокий уровень защиты сети, так как TKIP позволяет создавать ключи длиной до 128 бит, а AES - до 256 бит.

Другим способом защиты является фильтрация по **MAC- адресу**. MAC-адрес (от англ. *Media Access Control* — управление доступом к среде, также Hardware Address) — это уникальный идентификатор, присваиваемый каждой единице активного оборудования компьютерных сетей[1]. Фильтрация по MAC адресу позволит подключаться к сети только заданным устройствам. Или наоборот - позволит всем кроме заданных MAC-адресов использовать сеть.

Идентификатор сети **SSID** (Server Set Identification) это имя беспроводной сети, которое следует знать всем, кто собирается подключаться к этой сети. Отключение вещания SSID усложнит подключение к точке доступа злоумышленникам.

 **Аутентификация** - выдача определённых прав доступа абоненту на основе имеющегося у него идентификатора[2].
Аутентификация в стандарте IEEE 802.11 ориентирована на аутентификацию абонентского устройства радиодоступа, а не конкретного абонента как пользователя сетевых ресурсов. Процесс аутентификации абонента беспроводной локальной сети IEEE 802.11 состоит из следующих этапов:

1. Абонент (Client) посылает фрейм Probe Request во все радиоканалы.
2. Каждая точка радиодоступа (Access Point - AP), в зоне радиовидимости которой находится абонент, посылает в ответ фрейм Probe Response.
3. Абонент выбирает предпочтительную для него точку радиодоступа и посылает в обслуживаемый ею радиоканал запрос на аутентификацию (Authentication Request).
4. Точка радиодоступа посылает подтверждение аутентификации (Authentication Reply).
5. В случае успешной аутентификации абонент посылает точке радиодоступа фрейм ассоциации (Association Request).
6. Точка радиодоступа посылает в ответ фрейм подтверждения ассоциации (Association Response).
7. Абонент может теперь осуществлять обмен пользовательским трафиком с точкой радиодоступа и проводной сетью.

Существует несколько типов аутентификации:

* *Открытая аутентификация* (англ. Open Authentication).

По умолчанию аутентификация беспроводных устройств отсутствует. Всем устройствам разрешено устанавливать соединения независимо от их типа. Открытая аутентификация должна использоваться только в общедоступных беспроводных сетях, например, в школах и интернет-кафе (ресторанах).

* *Предварительно согласованный ключ* (PSK- англ. Pre Shared Key).

При использовании режима **PSK** точка доступа и клиент должны использовать общий ключ или кодовое слово. Точка доступа отправляет клиенту случайную строку байтов. Клиент принимает эту строку, шифрует ее, используя ключ, и отправляет ее обратно в точку доступа. Точка доступа получает зашифрованную строку и для ее расшифровки использует свой ключ. Если расшифрованная строка, принятая от клиента, совпадает с исходной строкой, то клиенту дается разрешение установить соединение.

* *Расширяемый протокол аутентификации (EAP-*[англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) Extensible Authentication Protocol).

**EAP** обеспечивает взаимную или двухстороннюю аутентификацию, а также аутентификацию пользователя. При применении EAP пользователь, а не только узел, должен предъявить имя и пароль, которые затем проверяются по базе данных сервера RADIUS. Если предъявленные учетные данные являются допустимыми, пользователь рассматривается как прошедший аутентификацию.

Хорошей новостью, является то, что большинство перечисленных рисков могут быть минимизированы или вообще сведены к нулю, если обезопасить сеть надлежащим образом.

 1Статья "MAC-адрес" интернет - энциклопедии «Википедия». [https://ru.wikipedia.org/wiki/MAC-адрес](https://ru.wikipedia.org/wiki/MAC-%D0%B0%D0%B4%D1%80%D0%B5%D1%81%20) Ссылка действительна на 28.03.2015
2Статья "Защита в сетях Wi-Fi" интернет - энциклопедии «Википедия». [https://ru.wikipedia.org/wiki/Защита\_в\_сетях\_Wi-Fi](https://ru.wikipedia.org/wiki/%D0%97%D0%B0%D1%89%D0%B8%D1%82%D0%B0_%D0%B2_%D1%81%D0%B5%D1%82%D1%8F%D1%85_Wi-Fi%20) Ссылка действительна на 28.03.2015

**Заключение**

Итак, *беспроводные компьютерные сети* (Wireless Area Network) — это технология, позволяющая создавать вычислительные сети, полностью соответствующие стандартам для обычных проводных сетей, без использования кабельной проводки. Она используется для работы в замкнутом пространстве, так как при беспроводном подключении пользователи могут использовать интернет-соединение, находясь в удобном для них месте (в пределах радиуса действия точки доступа). Так же, беспроводные сети используют для соединения удаленных локальных сетей или удаленных сегментов локальной сети. Существует 4 основных вида беспроводных компьютерных сетей, которые созданы для решения различных задач и проблем:

* WPAN (Беспроводная персональная сеть)
* WLAN (Беспроводная локальная сеть)
* WiMAX (Беспроводная сеть масштаба города)
* WWAN (Беспроводная глобальная сеть)

Многие считают, что беспроводные сети намного лучше проводного подключения к сети Ethernet, но не все знают, что у них есть достаточно большое количество недостатков:

* Различие информационной и полезной скоростей
* Воздействие различных препятствий (потолки, мебель, металлические двери и т.д.) на работу беспроводного подключения
* Воздействие другой техники, работающей на одной волне с точкой доступа Wi-Fi
* Проблема скрытого узла
* Несанкционированное подключение к устройствам и сетям
* Перехват и модификация трафика
* Нарушение доступности

Большинство из перечисленных минусов, связанных с безопасностью, можно устранить, если сохранять желательные меры предосторожности при работе в среде беспроводной сети. В конечном итоге, плюсы использования беспроводного подключения "перевешивают" минусы, что делает такие сети широко распространенными в наше время.

**Список литературы**

1)Гусева А.И., Киреев В.С. Вычислительные системы, сети и телекоммуникации: учебник для студенческих учреждений высшего профессионального образования. - М.: Издательский центр "Академия", 2014.

2)Джим Гейер Беспроводные сети. Первый шаг : Пер. с англ. — М. : Издательский дом "Вильяме", 2005.

# 3)Статья "Беспроводные компьютерные сети" интернет ресурса «Диком». [http://dicom.spb.ru/articles/network-and-servers/wireless-computer-networks/](http://dicom.spb.ru/articles/network-and-servers/wireless-computer-networks/%20) Ссылка действительна на 15.03.2015

4)Статья "Беспроводные сети" интернет ресурса для IT-специалистов «Хабрахабр». <http://habrahabr.ru/sandbox/21711/> Ссылка действительна на 15.03.2015.

# 5)Статья "Защита в сетях Wi-Fi" интернет - энциклопедии «Википедия». [https://ru.wikipedia.org/wiki/Защита\_в\_сетях\_Wi-Fi](https://ru.wikipedia.org/wiki/%D0%97%D0%B0%D1%89%D0%B8%D1%82%D0%B0_%D0%B2_%D1%81%D0%B5%D1%82%D1%8F%D1%85_Wi-Fi%20) Ссылка действительна на 28.03.2015

6)Статья "Проблема скрытого узла" интернет ресурса о сетевых технологиях «Ирне». <http://irne.ru/articles/wireless/hidden-node-problem.html> Ссылка действительна на 15.03.2015.

# 7)Статья "Реальная скорость соединения, используемая в технологии Wi-Fi компании «ZyXEL»". <http://zyxel.ru/kb/2306> Ссылка действительна на 28.03.2015

# 8) Статья "Что влияет на работу беспроводных сетей Wi-Fi? Что может являться источником помех и каковы их возможные причины?". <http://zyxel.ru/kb/2082> Ссылка действительна на 28.03.20159)Статья "CSMA/CA" интернет - энциклопедии «Википедия». [https://ru.wikipedia.org/wiki/CSMA/CA](https://ru.wikipedia.org/wiki/CSMA/CA%20) Ссылка действительна на 28.03.2015

10)Статья "MAC-адрес" интернет - энциклопедии «Википедия». [https://ru.wikipedia.org/wiki/MAC-адрес](https://ru.wikipedia.org/wiki/MAC-%D0%B0%D0%B4%D1%80%D0%B5%D1%81%20) Ссылка действительна на 28.03.2015