ОГЛАВЛЕНИЕ

[ВВЕДЕНИЕ 2](#_Toc343855945)

[ИСТОРИЯ УСПЕХА ТЕХНОЛОГИИ WIFI 4](#_Toc343855946)

[СТАНДАРТЫ БЕСПРОВОДНЫХ СЕТЕЙ 5](#_Toc343855947)

[ПРИНЦИПЫ РАБОТЫ БЕСПРОВОДНОЙ СВЯЗИ WI-FI 9](#_Toc343855948)

[РАЗВИТИЕ ЗАЩИТЫ WI-FI 13](#_Toc343855949)

[ОБОРУДОВАНИЕ 18](#_Toc343855950)

[ПРЕИМУЩЕСТВА WI-FI 22](#_Toc343855951)

[НЕДОСТАТКИ WI-FI 22](#_Toc343855952)

[ЗАКЛЮЧЕНИЕ 25](#_Toc343855953)

[СПИСОК ИСТОЧНИКОВ 26](#_Toc343855954)

[ПРИЛОЖЕНИЕ 1 27](#_Toc343855955)

[ПРИЛОЖЕНИЕ 2 28](#_Toc343855956)

# ВВЕДЕНИЕ

В эпоху проходящей информатизации, данное явление приходит даже в самые отдаленные уголки нашей планеты. Мы часто слышим в СМИ о проведении новых проектов по информатизации общества. Как например, можно услышать от наших политиков, что происходит снабжение компьютерной техникой и услугами Интернет деревенских школ и школ малых городов. Но данный процесс проходит очень медленно. Гораздо быстрее происходит развитие компьютерных технологий.

В настоящее время существует безграничный по своей насыщенности источник знаний и различных данных. Это Интернет. С помощью него люди могут выполнять ряд нужных и полезных функций. Одно из этих функций является образование. И не только для школьников и студентов, но и для людей, занятых в разных отраслях производства, науки и общественной жизни страны. Так подсчитано, что для того, чтобы человеку ознакомиться со всеми нововведениями в его области труда необходимо затратить 75% рабочего времени. Но, к сожалению, данный ресурс не доступен для большинства населения страны. Это обусловлено многими причинами, о которых мы говорить не будем. Поговорим же непосредственно о том, как можно связаться с Интернет и вообще передать информацию.

В настоящее время данные можно передавать по проводным и беспроводным линиям телекоммуникаций. Каждый из данных способов имеет свои плюсы и минусы. В данной работе будет рассмотрена беспроводная технология. Она будет рассмотрена с разных аспектов. А именно мы поговорим о 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, КПК или ноутбуки. Очевидно, что 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. Тем не менее, до сих пор лишь немногие пользователи представляют себе, что же скрывается за загадочной аббревиатурой Wi-Fi.

# ИСТОРИЯ УСПЕХА ТЕХНОЛОГИИ WIFI

Интеграция вычислительной, коммуникационной и мобильной технологий стимулирует во всем мире спрос на беспроводные решения, позволяющие неизменно оставаться на связи — в любое время и в любом месте. По мере распространения беспроводных технологий конечные пользователи стремятся получить для работы и развлечений такие решения, которые бы соответствовали их мобильному стилю жизни. В Европе, США и других высокоразвитых странах применяется технология Wifi, причем использование данных технологий осуществляется в различных областях производственной сферы и сферы услуг. Это обусловлено прежде всего, заинтересованностью правительства государств и муниципальных органов в развитии данной области для улучшения процесса производства, науки, образования и других сфер жизни человека. В доказательство этим словам будет рассказано о истории внедрения технологии WiFi в различные области общественной жизни человека.

На Западе сейчас успешно функционирует множество коммерческих провайдеров Wi-Fi, а основой популярности этой беспроводной технологии является её активная поддержка мировыми производителями. Почти все современные модели ноутбуков, а также некоторые модели сотовых телефонов и КПК уже оснащаются Wi-Fi адаптерами, что не может не сказаться на росте числа публичных и корпоративных беспроводных сетей. По оценкам аналитиков к началу этого года в США насчитывалось около 29000 зон Wi-Fi, которые обслуживают по разным данным до 30 миллионов пользователей. В Западной Европе в начале года насчитывалось около 4 миллионов мобильных пользователей и 16000 точек доступа. Однако, эта статистика весьма приблизительна, поскольку каждые несколько секунд в мире появляется новый хот-спот. Известно, что в 2004 году общее число Wi-Fi зон во всем мире превысило 100 тысяч.

# СТАНДАРТЫ БЕСПРОВОДНЫХ СЕТЕЙ

WI-FI - это современная беспроводная технология передачи данных по радиоканалу (wireless, wlan wifi).

Любое оборудование, соответствующее стандарту IEEE 802.11, может быть протестировано в Wi-Fi Alliance и получить соответствующий сертификат и право нанесения логотипа Wi-Fi.

Строго говоря, фраза Wi-Fi, когда ее придумали, никак не расшифровывалась. Это гораздо позже придумали расшифровку ранее составленных букв: Wireless Fidelity, что в переводе с английского - беспроводная точность. Изначально же аббревиатура была придумана как что-то созвучное модному слову "ХАЙ ФАЙ". Стоит так же отметить, что есть и более длинное название термина: EEE 802.11b. Зародился Wi-Fi в 1985 году, в США, после того как была открыта частотная часть радиоканала для использования без специального разрешения.

Самым первым стандартом, получившим наибольшее распространение, стал стандарт IEEE 802.11b. Оборудование, соответствующее стандарту 802.11b, появилось ещё в 2001 году, и до сих пор большинство беспроводных сетей по-прежнему работает с использованием этого стандарта, а также выпускается множество беспроводных Wi-Fi устройств с поддержкой 802.11b.

Радиоволны, которые используются для Wi-Fi связи очень похожи на радиоволны используемые в рациях, приемниках, сотовых телефонах и других устройствах. Но Wi-Fi имеет несколько заметных отличий от других радиоприборов.

Связь ведется на частотах 2,4 - 5 ГГц. Эта частота намного выше, чем частоты, пригодные для мобильных телефонов, портативных радиостанций и телевидения. Чем выше частота сигнала, тем большее количество информации передается.

*Они используют сетевые стандарты, такие как 802.11:*

802.11. Скорость передачи Wi-Fi по нему равна 1-2 Мб/с.

802.11a работает с частотой в 5 ГГц и может иметь скорость до 54 Мбит в секунду. Он также использует мультиплексирование с ортогональным частотным разделением (OFDM), более развитый алгоритм кодирования. Это значительно снижает искажения.

802.11b является самым медленным и наименее дорогим стандартом. В свое время его стоимость сделали стандарт популярным, но теперь этот стандарт считается отсталым, так как быстрее стандарты становятся менее дорогими. 802.11b транслируется на частоте 2,4 ГГц. Он имеет возможность передавать до 11 мегабит. В алгоритме есть код для ускорения передачи данных.

802.11g транслируется с той же частотой в 2,4 ГГц, как 802.11b, но в несколько раз быстрее - он может передать более 54 мегабит информации в секунду. 802.11g скоростной, так как он использует тот же OFDM алгоритм кодирования, как и 802.11a.

802.11n является новейшим стандартом, который широко распространен. Этот стандарт существенно повышает скорость и дальность. Теоретически стандарт 802.11g передает 54 мегабит в секунду, хотя реально скоростью составляет около 24 мегабит в секунду из-за перегрузки сети.

Другие 802,11 стандарты созданы для конкретных беспроводных сетей, например для глобальных сетей (WAN) внутри транспортных средств.

В последнее время активно развивается еще одна группа стандартов для беспроводных сетей – 802.16 или Wi-MAX. Стандарты этой группы предназначены для построения сетей масштаба города. От стандартов 802.11 их отличает увеличенный радиус действия (2-6 км) и скорость передачи данных (от 1 до 134.4 Мбит/сек).

Выбор используемого стандарта и оборудования необходимо проводить с учетом действующего законодательства. Поскольку в разных странах требования к используемым частотам и мощности радиопередатчиков существенно различаются, производители оборудования выпускают различные версии одной и той же модели для разных регионов. В нашей стране нет радиочастот, открытых для свободного использования, поэтому для использования радиоканала необходимо получить соответствующее разрешение.

Как сообщает Cult of Mac , 29 июля 2011 года IEEE, Институт инженеров по электротехнике и электронике — IEEE выпустил официальную версию стандарта IEEE 802.22. Это есть Super Wi-Fi. Системы и устройства, поддерживающие этот стандарт, позволят передавать данные на скорости до 22 Мб/с в радиусе 100 км от ближайшего передатчика.

Сетевые протоколы используемые в Wi-Fi оборудовании:

DNS (англ. Domain Name System — система доменных имён) — компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты, обслуживающих узлах для протоколов в домене (SRV-запись).

NAT (от англ. Network Address Translation — «преобразование сетевых адресов») — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов.

Принимая пакет от локального компьютера, роутер смотрит на IP-адрес назначения. Если это локальный адрес, то пакет пересылается другому локальному компьютеру. Если нет, то пакет надо переслать наружу в интернет. Но ведь обратным адресом в пакете указан локальный адрес компьютера, который из интернета будет недоступен. Поэтому роутер «на лету» производит трансляцию IP-адреса и порта и запоминает эту трансляцию у себя во временной таблице. Через некоторое время после того, как клиент и сервер закончат обмениваться пакетами, роутер сотрет у себя в таблице запись о n-ом порте за сроком давности.

DHCP (англ. Dynamic Host Configuration Protocol — протокол динамической конфигурации узла) — это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.

L2TP (англ. Layer 2 Tunneling Protocol — протокол туннелирования второго уровня) — в компьютерных сетях туннельный протокол, использующийся для поддержки виртуальных частных сетей. Главное достоинство L2TP состоит в том, что этот протокол позволяет создавать туннель не только в сетях IP, но и в таких, как ATM, X.25 и Frame Relay.[1]

# ПРИНЦИПЫ РАБОТЫ БЕСПРОВОДНОЙ СВЯЗИ WI-FI

Беспроводная сеть использует радиоволны точно так же как радиоприемники, мобильные телефоны, телевизоры. На самом деле беспроводная связь Wi-Fi более похожа на двустороннюю радиосвязь. Вот что происходит:

Адаптер Wi-Fi преобразует поток данных в электрический радиосигнал и передает его через антенну.

Wi-Fi маршрутизатор получает радиосигнал и дешифрует его. Маршрутизатор Wi-fi отправляет данные с помощью физических, проводных соединений.

Фактически нам без проводов не обойтись. Но провода находятся только у провайдера. У нас же все красиво, и без лишних кабелей.

Это работает и в обратном направлении, маршрутизатор получает информацию из интернета и переводит его в радиосигнал, отправляя его потом беспроводным адаптером компьютера.

Wi-Fi радио может передаваться по любому из трех диапазонов рабочих частот. Или, они могут менять частоты на ходу. Смена частот помогает снизить помехи.

Для того чтобы работал Wi-Fi необходимо соответствующее оборудование для беспроводной связи, которое сейчас выпускают достаточное количество производителей. Все оборудование можно поделить, на:

*точку доступа, беспроводной роутер*

И у первого и у второго устройства, по сути, одинаковая начинка - приемопередающий модуль. Отличаются они между собой лишь режимами работы. Основное отличие одинаковых беспроводных устройств, выпускаемых разными производителями, это их программное обеспечение.

Беспроводное соединение устанавливается между двумя точками доступа (в качестве второй точки может быть роутер). Каждая беспроводная точка может соединиться только с одной точкой. Беспроводной роутер - это умная точка доступа. Это устройство позволяет обмениваться данными трем и более беспроводным точкам.

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. Стандарт Wi-Fi даёт клиенту полную свободу при выборе критериев для соединения.

По сути, точка доступа является приёмо-передатчиком радиосигнала и, как у любого такого устройства, у нее есть определенный радиус действия. Обычный WiFi-роутер позволяет передавать сигнал на расстояние до 90 м в зоне прямой видимости. В помещении же все зависит от многих факторов: планировка, толщина и материал стен, наличие других излучателей радиосигнала и др. Но, как правило, мощности передатчика простой точки доступа вполне достаточно для «покрытия» небольшого офиса из трех-четырех кабинетов или квартиры, площадью 150 м2. При необходимости зону покрытия можно увеличить, установив в местах слабого приема специальные точки доступа, работающие в режиме «повторителя». Они принимают сигнал от основной точки, усиливают, и передают дальше.

Типы и разновидности соединений

Соединение Ad-Hoc (точка-точка).

Все компьютеры оснащены беспроводными картами (клиентами) и соединяются напрямую друг с другом по радиоканалу работающему по стандарту 802.11b и обеспечивающих скорость обмена 11 Mбит/с, чего вполне достаточно для нормальной работы.

Инфраструктурное соединение

Данная модель используется, когда необходимо соединить больше двух компьютеров. Сервер с точкой доступа может выполнять роль роутера и самостоятельно распределять интернет-канал.

Точка доступа, с использованием роутера и модема

Точка доступа включается в роутер, роутер — в модем (эти устройства могут быть объединены в два или даже в одно). Теперь на каждом компьютере в зоне действия Wi-Fi , в котором есть адаптер Wi-Fi, будет работать интернет.

Клиентская точка

В этом режиме точка доступа работает как клиент и может соединятся с точкой доступа работающей в инфраструктурном режиме. Но к ней можно подключить только один МАС-адрес. Здесь задача состоит в том, чтобы объединить только два компьютера. Два Wi-Fi-адаптера могут работать друг с другом напрямую без центральных антенн.

Соединение мост

Компьютеры объединены в проводную сеть. К каждой группе сетей подключены точки доступа, которые соединяются друг с другом по радио каналу. Этот режим предназначен для объединения двух и более проводных сетей. Подключение беспроводных клиентов к точке доступа, работающей в режиме моста невозможно.

Оборудование, предназначенное для работы в стандарте 802.11, в основном делится на два класса - это клиенты и точки доступа (Access Point). Роль клиентов могут играть настольные компьютеры, ноутбуки, КПК, телефоны, принтеры, игровые приставки и прочая портативная и стационарная бытовая техника, оборудованная Wi-Fi-модулем. Если в ПК или КПК изначально отсутствует поддержка беспроводных сетей, то в большинстве случаев это можно с легкостью восполнить приобретением соответствующего адаптера, который может быть реализован в форме практически любой платы расширения. Точки доступа обычно выполнены в виде отдельного внешнего устройства, подключаемого непосредственно к кабелю проводной сети Ethernet или к любому другому совместимому источнику широкополосного доступа в Интернет. Иногда точки доступа комбинируют с каким-либо другим устройством, например, весьма распространены ADSL-модемы, совмещенные с точкой доступа Wi-Fi. На точку доступа возлагается львиная часть работы по обслуживанию беспроводной сети: она должна не только поддерживать радиопередачу со всеми клиентами и связывать сеть с внешним миром, но и регулировать трафик, обрабатывать данные и совершать массу других операций. Также в некоторых случаях может потребоваться и дополнительное оборудование: например, при недостаточном уровне сигнала нужны антенны, а при необходимости соединения между собой двух сетей - мосты.

# РАЗВИТИЕ ЗАЩИТЫ WI-FI

В 1997 году вышел первый стандарт IEEE 802.11, безопасность которого, как оказалось, далека от идеала. Простой пароль SSID (Server Set ID) для доступа в локальную сеть по современным меркам нельзя считать защитой, особенно, учитывая факт, что к Wi-Fi не нужно физически подключаться.

Главной же защитой долгое время являлось использование цифровых ключей шифрования потоков данных с помощью функции Wired Equivalent Privacy (WEP). Сами ключи представляют из себя обыкновенные пароли с длиной от 5 до 13 символов ASCII, что соответствует 40 или 104-разрядному шифрованию на статическом уровне. Как показало время, WEP оказалась не самой надёжной технологией защиты. И, кстати, все основные атаки хакеров пришлись как раз на эпоху внедрения WEP.

После 2001 года для проводных и беспроводных сетей был внедрён новый стандарт IEEE 802.1X, который использует вариант динамических 128-разрядных ключей шифрования, то есть периодически изменяющихся во времени. Таким образом, пользователи сети работают сеансами, по завершении которых им присылается новый ключ. Например, [Windows XP](http://technet.microsoft.com/ru-ru/windows/bb264763.aspx%22%20%5Ct%20%22_blank%22%20%5Co%20%22%D0%9F%D0%BE%D1%81%D0%B5%D1%82%D0%B8%D1%82%D0%B5%20%D1%82%D0%B5%D1%85%D1%86%D0%B5%D0%BD%D1%82%D1%80%20Windows%20XP) поддерживает данный стандарт, и по умолчанию время одного сеанса равно 30 минутам.

В конце 2003 года был внедрён стандарт Wi-Fi Protected Access (WPA), который совмещает преимущества динамического обновления ключей IEEE 802.1X с кодированием протокола интеграции временного ключа Temporal Key Integrity Protocol (TKIP), протоколом расширенной аутентификации Extensible Authentication Protocol (EAP) и технологией проверки целостности сообщений Message Integrity Check (MIC).

Помимо этого, параллельно развивается множество самостоятельных стандартов безопасности от различных разработчиков, в частности, в данном направлении преуспевают Intel и Cisco. В 2004 году появляется WPA2, или 802.11i, — максимально защищённый стандарт.

Технологии защиты

WEP

Эта технология была разработана специально для шифрования потока передаваемых данных в рамках локальной сети. Данные шифруются ключом с разрядностью от 40 до 104 бит. Но это не целый ключ, а только его статическая составляющая. Для усиления защиты применяется так называемый вектор инициализации Initialization Vector (IV), который предназначен для рандомизации дополнительной части ключа, что обеспечивает различные вариации шифра для разных пакетов данных. Данный вектор является 24-битным. Таким образом, в результате мы получаем общее шифрование с разрядностью от 64 (40+24) до 128 (104+24) бит. Идея очень хорошая, поскольку при шифровании мы оперируем и постоянными, и случайно подобранными символами.

Но, как оказалось, взломать такую защиту можно — соответствующие утилиты присутствуют в Интернете (например, AirSnort, WEPcrack). Основное её слабое место — это как раз вектор инициализации. Поскольку мы говорим о 24 битах, это подразумевает около 16 миллионов комбинаций (2 в 24 степени) — после использования этого количества ключ начинает повторяться. Хакеру необходимо [найти](http://www.outsidethebox.ms/x-files/windows-search/) эти повторы (от 15 минут до часа для ключа 40 бит) и за секунды взломать остальную часть ключа. После этого он может входить в сеть как обычный зарегистрированный пользователь.

802.1X

IEEE 802.1X — это новый стандарт, который оказался ключевым для развития индустрии беспроводных сетей в целом. На данный момент он поддерживается только со стороны ОС Windows [XP](http://technet.microsoft.com/ru-ru/windows/bb264763.aspx) и анонсирован для [Windows Server 2003](http://technet.microsoft.com/ru-ru/windowsserver/bb512919.aspx%22%20%5Ct%20%22_blank%22%20%5Co%20%22%D0%9F%D0%BE%D1%81%D0%B5%D1%82%D0%B8%D1%82%D0%B5%20%D1%82%D0%B5%D1%85%D1%86%D0%B5%D0%BD%D1%82%D1%80%20Windows%20Server%202003). За основу взято исправление недостатков технологий безопасности, применяемых в 802.11, в частности, возможность взлома WEP, зависимость от технологий производителя и т. п. 802.1X позволяет подключать в сеть даже PDA-устройства, что позволяет более выгодно использовать саму идею беспроводной связи. С другой стороны, 802.1X и 802.11 являются совместимыми стандартами. В 802.1X применяется тот же алгоритм, что и в WEP, а именно — RC4, но с некоторыми отличиями.

802.1X базируется на протоколе расширенной аутентификации Extensible Authentication Protocol (EAP), протоколе защиты транспортного уровня Transport Layer Security (TLS) и сервере доступа RADIUS (Remote Access Dial-in User Server). Плюс к этому стоит добавить новую организацию работы клиентов сети. После того, как пользователь прошёл этап аутентификации, ему высылается секретный ключ в зашифрованном виде на определённое незначительное время — время действующего на данный момент сеанса. По завершении этого сеанса генерируется новый ключ и опять высылается пользователю. Протокол защиты транспортного уровня TLS обеспечивает взаимную аутентификацию и целостность передачи данных. Все ключи являются 128-разрядными по умолчанию.

WPA

WPA — это временный стандарт, о котором договорились производители оборудования, пока не вступил в силу IEEE 802.11i. По сути, WPA = 802.1X + EAP + TKIP + MIC, где:

* WPA — технология защищённого доступа к беспроводным сетям (Wi-Fi Protected Access),
* EAP — протокол расширенной аутентификации (Extensible Authentication Protocol),
* TKIP — протокол интеграции временного ключа (Temporal Key Integrity Protocol),
* MIC — технология проверки целостности сообщений (Message Integrity Check).

Как видим, ключевыми здесь являются новые модули TKIP и MIC. Стандарт TKIP использует автоматически подобранные 128-битные ключи, которые создаются непредсказуемым способом и общее число вариаций которых достигает 500 миллиардов. Сложная иерархическая система алгоритма подбора ключей и динамическая их замена через каждые 10 Кбайт (10 тыс. передаваемых пакетов) делают систему максимально защищённой.

От внешнего проникновения и изменения информации также обороняет технология проверки целостности сообщений (Message Integrity Check). Достаточно сложный математический алгоритм позволяет сверять отправленные в одной точке и полученные в другой данные. Если замечены изменения и результат сравнения не сходится, такие данные считаются ложными и выбрасываются.

Правда, TKIP сейчас не является лучшим в реализации шифрования, поскольку в силу вступают новые алгоритмы, основанные на технологии Advanced Encryption Standard (AES), которая, кстати говоря, уже давно используется в VPN. Что касается WPA, поддержка AES уже реализована в Windows XP, пока только опционально.

VPN

Технология виртуальных частных сетей Virtual Private Network (VPN) была предложена компанией Intel для обеспечения безопасного соединения клиентских систем с серверами по общедоступным интернет-каналам. VPN очень хорошо себя зарекомендовали с точки зрения шифрования и надёжности аутентификации. Плюс технологии состоит и в том, что на протяжении более трёх лет практического использования в индустрии данный протокол не получил никаких нареканий со стороны пользователей. Информации о его взломах не было.

Технологий шифрования в VPN применяется несколько, наиболее популярные из них описаны протоколами PPTP, L2TP и IPSec с алгоритмами шифрования DES, Triple DES, AES и MD5. IP Security (IPSec) используется примерно в 65—70% случаев. С его помощью обеспечивается практически максимальная безопасность линии связи.

И хотя технология VPN не предназначалась изначально именно для Wi-Fi, она может использоваться для любого типа сетей, и идея защитить с её помощью беспроводные их варианты одна из лучших на сегодня.

Для VPN выпущено уже достаточно большое количество программного (ОС Windows NT/2000/XP, Sun Solaris, Linux) и аппаратного обеспечения. Для реализации VPN-защиты в рамках сети необходимо установить специальный VPN-шлюз (программный или аппаратный), в котором создаются туннели, по одному на каждого пользователя. Например, для беспроводных сетей шлюз следует установить непосредственно перед точкой доступа. А пользователям сети необходимо установить специальные клиентские программы, которые в свою очередь также работают за рамками беспроводной сети и расшифровка выносится за её пределы.

Хотя всё это достаточно громоздко, но очень надёжно, главный недостаток такого решения — необходимость в администрировании. Второй существенный минус — уменьшение пропускной способности канала на 30—40%.

# ОБОРУДОВАНИЕ

Для построения беспроводной ЛВС необходимо оборудование следующих типов:

Точки доступа (Access Point, AP), используются для подключения пользователей к ЛВС по радиоканалу;

Беспроводные мосты (Wireless Brigde), используются для объединения двух и более ЛВС по радиоканалу;

Внешние антенны, используются для усиления радиосигнала и/или для изменения направления распространения сигнала;

Сетевые радио-карты для клиентов (Wireless Netcard), используются для подключения компьютера клиента к АР;

Контроллеры беспроводной сети (Wireless LAN Controllers), используются для централизованного управления всей беспроводной сетью предприятия.

Точки доступа подразделяются на автономные (Autonomous) и упрощенные (Lightweight).

Отличие упрощенных точек доступа заключается в необходимости использования контроллера беспроводной сети. В этом случае весь интеллект сосредотачивается в контроллере, а точка доступа выступает только в роли радиоприемника/передатчика. Контроллер обеспечивает:

Автоматическое получение точками доступа текущей конфигурации;

Автоматический выбор канала и мощности каждого передатчика для обеспечения оптимальной зоны покрытия и предотвращения помех, вызванных перекрытием зон покрытия передатчиков с одинаковым радиоканалом;

Централизованное применение политик безопасности и качества обслуживания (QoS);

Обеспечение роуминга мобильных пользователей.

Применять упрощенные точки доступа целесообразно в сетях с большим количеством точек доступа и зоной охвата сложной геометрической формы.

Автономные точки доступа обычно применяются в случаях, когда их число невелико, например для организации радиоканала между зданиями или для беспроводных сетей с небольшой зоной покрытия, для обеспечения которой достаточно 1-2 точек.

В некоторых случаях устройства могу совмещать в себе функции AP и Wireless Bridge, например Cisco Aironet 1300, причем, при наличии двух радиопередатчиков, устройство может одновременно выполнять обе функции.

Типы антенн для Wi-Fi – устройств

В плане использования все антенны для Wi-Fi-устройств можно условно разделить на два больших класса: антенны для наружного (outdoor) и для внутреннего применения (indoor). Отличаются эти антенны прежде всего своими габаритами и коэффициентом усиления. Естественно, антенны для наружного использования больше по размерам и предусматривают форму крепления либо к стене дома, либо к вертикальному столбу.

Антенны для внутреннего использования меньше по размерам и обладают более низким коэффициентом усиления. Такие антенны либо устанавливаются на столе, либо крепятся к стене или непосредственно к точке доступа.

К самой точке доступа антенны могут подсоединяться либо напрямую, либо с помощью кабеля. При этом для подсоединения антенны или кабеля к точке доступа предназначен специальный миниатюрный SMA-разъем. На точках доступа применяется разъем типа Male, а на самой антенне или антенном кабеле — разъем типа Female

Штыревая антенна

Все точки доступа стандарта 802.11b/g комплектуются штатными миниатюрными штыревыми антеннами, которые могут быть как съемными, так и стационарными. Штыревая антенна представляет собой самый простой вариант антенны. Ее часто называют также несимметричным вибратором.

Если штыревую антенну расположить вертикально, то в горизонтальной плоскости она будет излучать энергию во все стороны равномерно, поэтому в горизонтальной плоскости такая антенна является всенаправленной и, естественно, говорить о преимущественном излучении в определенном направлении не приходится. В то же время в вертикальной плоскости такая антенна излучает неравномерно. В частности, излучение вдоль оси антенны вообще отсутствует. Именно поэтому даже в случае простейшей штыревой антенны можно выделить направления, соответствующие максимальному усилению. Для штыревых антенн максимальное усиление достигается в плоскости, перпендикулярной антенне и проходящей через ее середину.

Отметим, что в силу изотропного характера излучения штыревой антенны, в горизонтальной плоскости точку доступа с такой антенной оптимально устанавливать в центре офиса или квартиры, чтобы максимально охватить беспроводной сетью все пространство квартиры или офиса.

Штыревая антенна c перпендикулярным рефлектором

Конструкцию штыревой антенны можно несколько улучшить, использовав перпендикулярный к антенне рефлектор — металлическую поверхность (экран), выполняющую функцию идеальной заземляющей поверхности. Подобные антенны не производятся промышленностью (во всяком случае, в продаже их нет), однако такую антенну несложно изготовить самостоятельно.

Как и в случае обычной штыревой антенны, штыревую антенну с перпендикулярным рефлектором наиболее целесообразно устанавливать в центре помещения (квартиры или офиса).

Штыревая антенна с параллельным рефлектором

Еще один способ модифицирования штыревой антенны заключается в том, чтобы использовать не перпендикулярный, а параллельный антенне рефлектор. В этом случае существенно меняется ее диаграмма направленности и в горизонтальной плоскости такая антенна перестает быть изотропной.

Такую антенну целесообразно располагать возле стены.

Итак, все направленные антенны устроены примерно одинаково и очень просто. Если антенна относится к панельному типу, то ее конструкция включает экран и излучатель, выполненный в форме прямоугольника и установленный на некотором расстоянии от экрана. Различия между антеннами заключаются лишь в размерах излучателя и экрана, а также в расстоянии между ними. В антеннах, предназначенных для использования внутри помещений, имеется один излучатель, а антенны, предназначенные для применения вне помещений, могут содержать несколько излучателей.

# ПРЕИМУЩЕСТВА WI-FI

* Позволяет развернуть сеть без прокладки кабеля, что может уменьшить стоимость развёртывания и/или расширения сети. Места, где нельзя проложить кабель, например, вне помещений и в зданиях, имеющих историческую ценность, могут обслуживаться беспроводными сетями.
* Позволяет иметь доступ к сети мобильным устройствам. Wi-Fi-устройства широко распространены на рынке. А устройства разных производителей могут взаимодействовать на базовом уровне сервисов.
* 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 сетей Wi-Fi, работающих вне помещений, или требуют регистрации Wi-Fi-оператора.
* Высокое по сравнению с другими стандартами потребление энергии, что уменьшает время жизни батарей и повышает температуру устройства.
* Самый популярный стандарт шифрования WEP может быть относительно легко взломан даже при правильной конфигурации (из-за слабой стойкости алгоритма). Несмотря на то, что новые устройства поддерживают более совершенный протокол шифрования данных WPA и WPA2, который проверяет пользователей сети через сервер и задействует 128-битные ключи шифрования и динамические ключи сессии для обеспечения защиты беспроводной сети, многие старые точки доступа не поддерживают его и требуют замены.
* Wi-Fi имеют ограниченный радиус действия. Типичный домашний маршрутизатор Wi-Fi стандарта 802.11b или 802.11g имеет радиус действия 45 м в помещении и 90 м снаружи. Микроволновая печь или зеркало, расположенные между устройствами Wi-Fi, ослабляют уровень сигнала. Расстояние зависит также от частоты.
* 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.
* Уменьшение производительности сети во время дождя.
* Перегрузка оборудования при передаче небольших пакетов данных из-за присоединения большого количества служебной информации.
* Малая пригодность для работы приложений, использующих медиа-потоки в реальном времени (например, протокол RTP, применяемый в IP-телефонии): качество медийного потока непредсказуемо из-за возможных высоких потерь при передаче данных, обусловленных целым рядом неконтролируемых пользователем факторов (атмосферные помехи, ландшафт и иное, в частности перечисленное выше). Несмотря на данный недостаток, выпускается масса VoIP оборудования на базе устройств 802.11b/g, которое ориентировано в том числе и на корпоративный сегмент: однако в большинстве случаев документация к подобным устройствам содержит оговорку, гласящую, что качество связи определяется устойчивостью и качеством радиоканала.

# ЗАКЛЮЧЕНИЕ

В данной работе было рассказано о беспроводной технологии Wi-Fi. конечно все аспекты, касающиеся данной темы нельзя описать в рамках одного реферата, на это может уйти очень много времени и составлять более фундаментальный труд, который будет полезен многим будущим пользователям Wi-Fi.

Нельзя не сказать, что технология Wi-Fi преследует в будущем несколько нереальные для нас пока цели. Т.е. для нашего понимания трудно представить, что когда-нибудь возможно будет, просто гуляя по городу, воспользоваться беспроводным выходом в Интернет. Не стоит также забывать о том, что беспроводная технология и технологии спутниковой передачи информации и мобильной связи это разные вещи. Также очень важно понимать, что к тому моменту, когда мы сможем в полной мере ощутить все достоинства данной технологии, в нее может быть внедрено еще много нового и полезного.

Несомненно, за технологией Wi-Fi будущее, но в нашей стране она пока не находит серьезной поддержки у широких масс. Ведь по проникновению Интернета и оснащенности пользователей разнообразными мобильными устройствами с поддержкой беспроводного доступа россияне отнюдь не в списке мировых лидеров. А потому в ближайшее время новые точки доступа будут появляться в первую очередь в местах скопления наиболее платежеспособных клиентов в бизнес-центрах, выставочных комплексах, отелях, ресторанах и аэропортах, то есть там, где их использование будет экономически оправданно. Интересующиеся дополнительной информацией по этому вопросу могут посетить сайт wifi.mail.ru, где размещен наиболее полный список известных на сегодняшний день как коммерческих, так и бесплатных точек доступа Wi-Fi в российских городах.

# СПИСОК ИСТОЧНИКОВ

1. Сергей Пахомов. История успеха Wi-Fi./ КомпьютерПресс №5. – 2003 ;
2. Wifi card, Основы Wi-Fi, http://www.wificard.ru/wi\_fi.php;
3. Понятие о Wi-Fi, http://wi-fi.na.by;
4. Информационный портал о Wi-Fi, http://www.wifi-connect.ru/3comlan.htm;
5. Компьютер Пресс, Антенны для Wi-Fi-устройств, http://www.compress.ru/article.aspx?id=17784&iid=822;
6. Wi-Fi сети, http://wificenter.ru;
7. Broadband – высокоскоростной Интернет, принципы Wi-Fi, http://www.broadband.org.ua/content/view/1694/284/;
8. Безопасность Wi-Fi-сетей - http://www.oszone.net/1398/;

# ПРИЛОЖЕНИЕ 1



Рисунок 1



Рисунок 2

# ПРИЛОЖЕНИЕ 2

Сравнительна таблица:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Критерии | Wi-Fi роутер NETGEAR WNR1000-100RUS | Wi-Fi роутер ASUS WL-520GC | Wi-Fi роутер NETGEAR JWNR2000-100RUS | Роутер NETGEAR WNR612-100RUS | Wi-Fi роутер NETGEAR WNR3500L-100RUS |
| Цена | 1 299 руб. | 2 099 руб. | 1 799 руб. | 1 499 руб. | 3 599 руб. |
| Сетевые протоколы | Сетевые протоколыDNS, NAT, DHCP, L2TP | DHCP, L2TP, IPSec | DHCP, L2TP | L2TP | DHCP, L2TP |
| Multiple SSID | 802.11b, 802.11g, 802.11n | 802.11b, 802.11g | 802.11b, 802.11g, 802.11n | 802.11b, 802.11g, 802.11n | 802.11b, 802.11g, 802.11n |
| WEP-шифрование | 64 бит, 128 бит | 64 бит, 128 бит | 64 бит, 128 бит | 64 бит, 128 бит | 64 бит, 128 бит |
| Индикаторы | Power, Internet, Status, LAN | Power, Internet, WLAN, LAN | Power, Internet, Status, LAN | Power, Internet, WLAN, LAN | Power, Internet, Status, LAN |
| Firewall | Есть |  | Есть | Есть | Есть |
| Статическая маршрутизация | Есть |  | Есть | Есть | Есть |
| Dynamic DNS |  |  |  | Есть |  |
| Высота | 2.8 см | 3 см | 17.3 см | 14.5 см | 17.5 см |
| Глубина | 11.8 см | 16.5 см | 11.6 см | 9.4 см | 13 см |
| Ширина | 17.5 см | 22 см | 3.3 см | 3 см | 3.5 см |
| Вес | 0.280 кг | 0.22 кг | 0.216 кг | 0.14 кг | 0.33 кг |