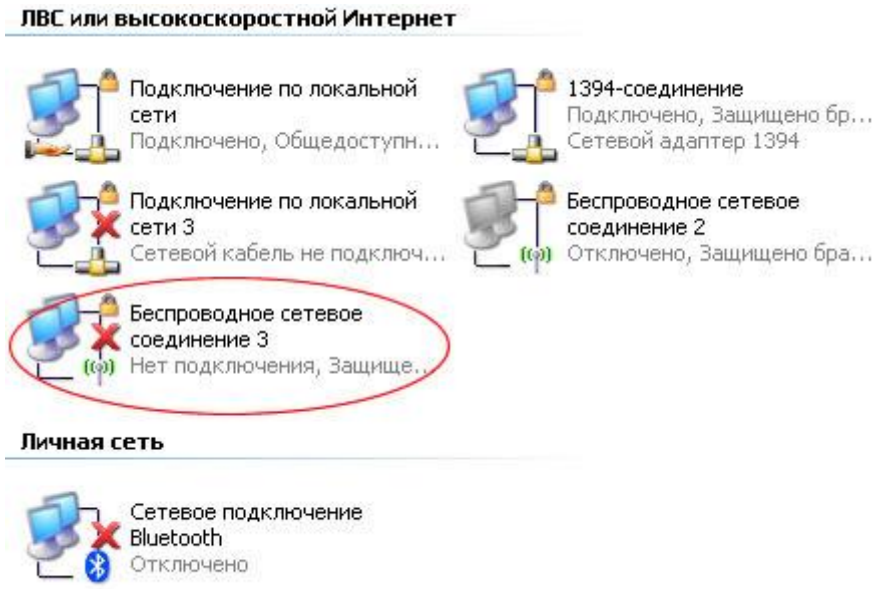
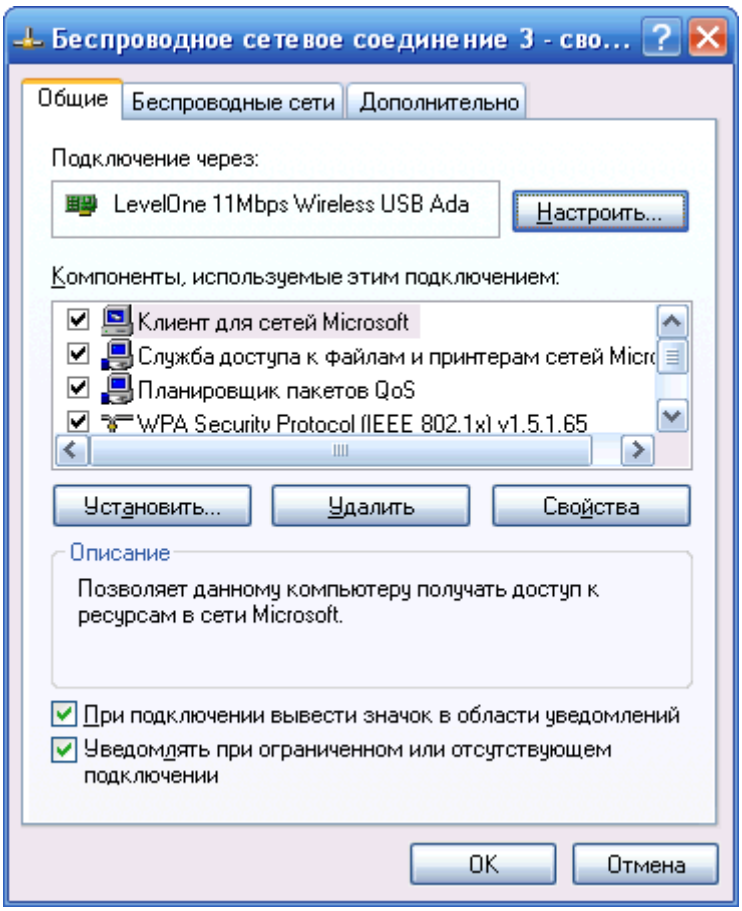
Соединение по Wi Fi технологии в домашних условиях.

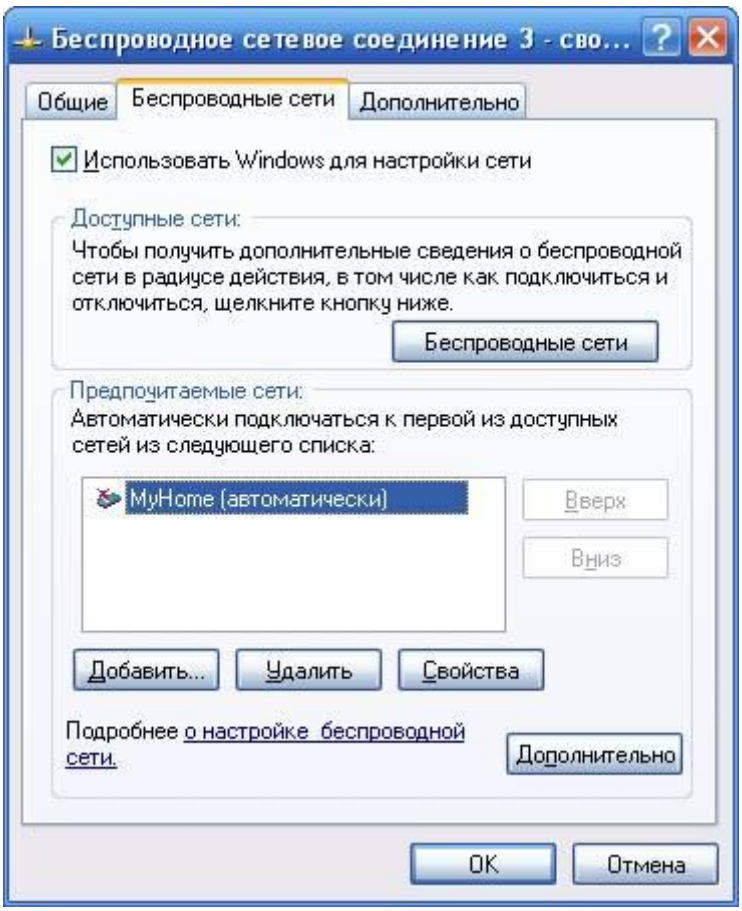
Для примера монтажа Wi Fi сети имеется стационарный компьютер с постоянным подключением к Интернет, и ноутбук, который мы хотели бы соединить в **локальную сеть**, а также обеспечить совместный выход в Интернет. На сегодняшний день существует несколько решений этой задачи, однако не все из них можно назвать простыми и доступными. На наш взгляд, самым простым и доступным способом является использование двух Wi Fi адаптеров (соединение Ad-Hoc), работающих по стандарту 802.11b и обеспечивающих скорость обмена 11 Mbit / s, чего вполне достаточно для нормальной работы.
Для наших экспериментов использовался USB контроллер LevelOne WNC -0101 USB и встроенный в ноутбук MaxSelect Mission Hammer Wide, Mini - PCI контроллер Realtek RTL 8180 Wireless LAN.
Прежде всего, для правильной работы необходимо установить драйвер и утилиту для настройки параметров и мониторинга соединения, и только потом подключать USB Wi Fi контроллер LevelOne WNC -0101 USB.
Далее приступаем к **настройке сети**. Для этого имеется два способа: через утилиту IEEE 802.11b WPC Utility(USB) или через использование стандартных средств Windows XP.



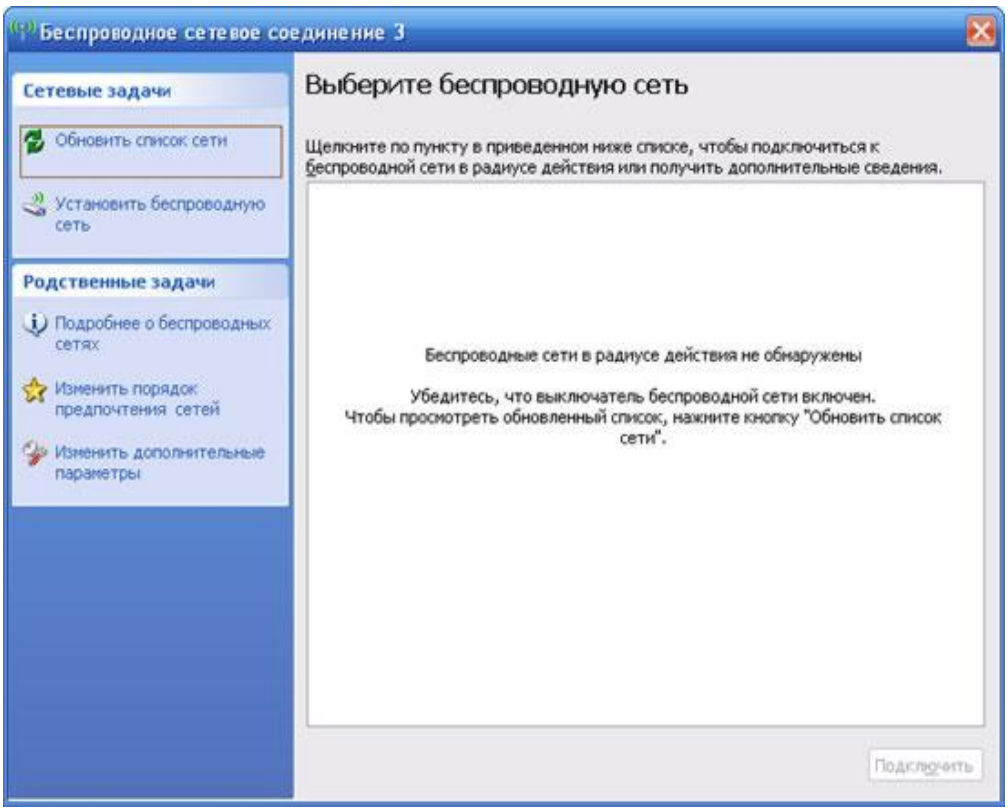
Открываем свойства сетевого окружения, где отображаются все, имеющиеся на нашем компьютере сетевые соединения. Теперь открываем "свойства беспроводное соединения 3" этого соединения, где нас интересует вторая закладка «Беспроводные **сети**». Именно здесь будут проводиться все настройки беспроводной **сети.**



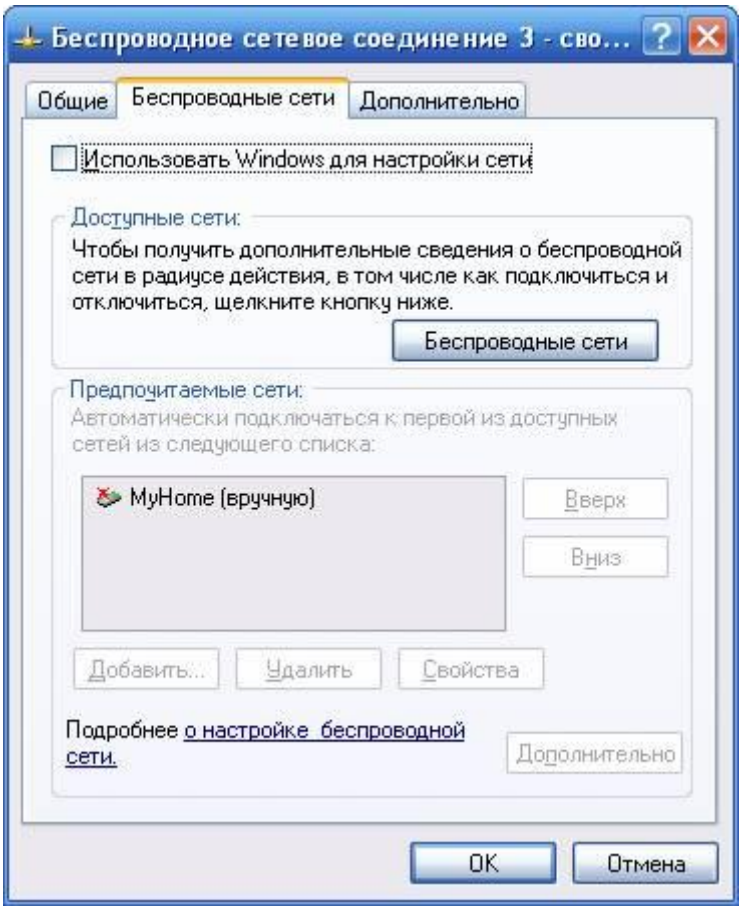
Опция «Использовать Windows для **настройки сети**» позволяет выбрать, какими инструментами будет производиться настройка.
На следующем этапе создаем беспроводное соединение путем нажатия кнопки «добавить» в разделе «Предпочитаемые сети», где необходимо ввести имя сети, а также установить некоторые специальные параметры, обеспечивающие определенный уровень безопасности.



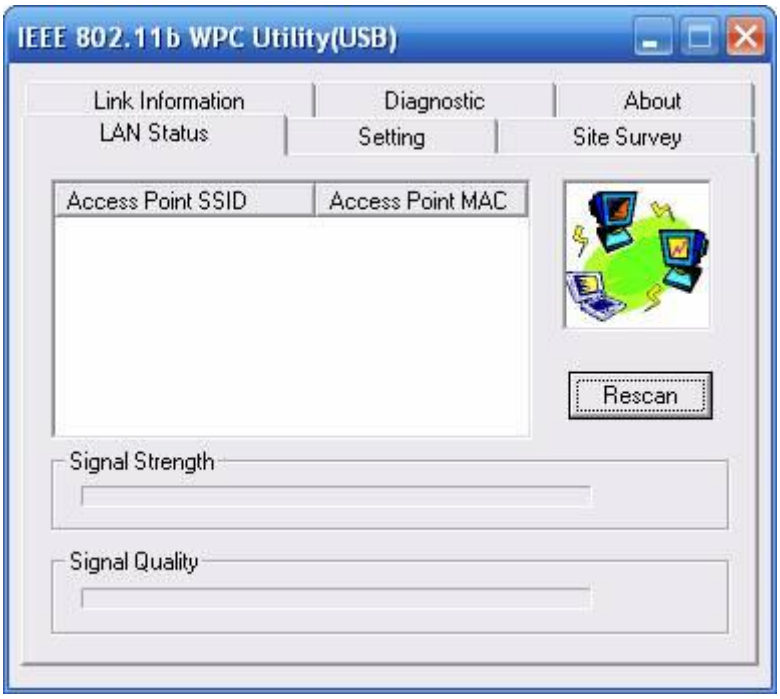
Средства Windows XP позволяют создать беспроводную сеть с помощью специального мастера, доступного в разделе «Доступные сети». Для этого необходимо нажать кнопочку «Беспроводные сети» и в открывшемся менеджере беспроводных сетей нажать кнопку «**Установить беспроводную сеть**». Главным отличием этого мастера является возможность сохранения настроек беспроводной сети на Flash диске, что заметно упрощает перенос конфигурации сети на другие компьютеры, однако для ситуации, когда необходимо соединить два компьютера, эта особенность не актуальна.



Рассмотрим второй способ настройки с помощью утилиты поставляемой в комплекте с контроллером LevelOne WNC -0101 USB. Для того, чтобы разрешить использование фирменной утилиты необходимо убрать галочку «Использовать Windows для **настройки сети**» в закладке «Беспроводные сети».



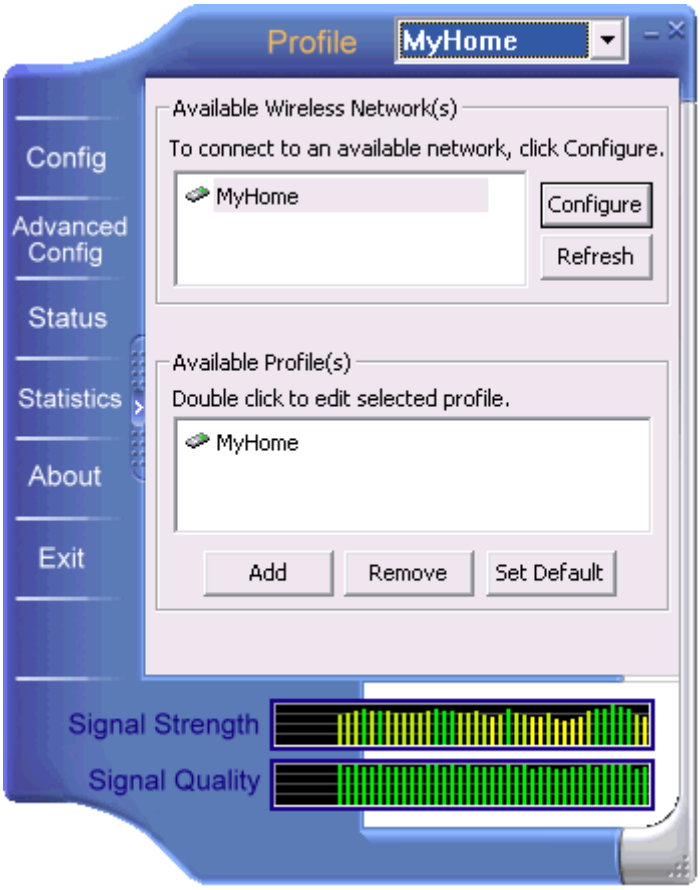
Утилита включает несколько больший набор особенностей, чем средства Windows. Здесь имеется шесть закладок. Первая закладка «LAN Status» отображает все, найденные вокруг, беспроводные сети, а также показывает мощность и качество сигнала.



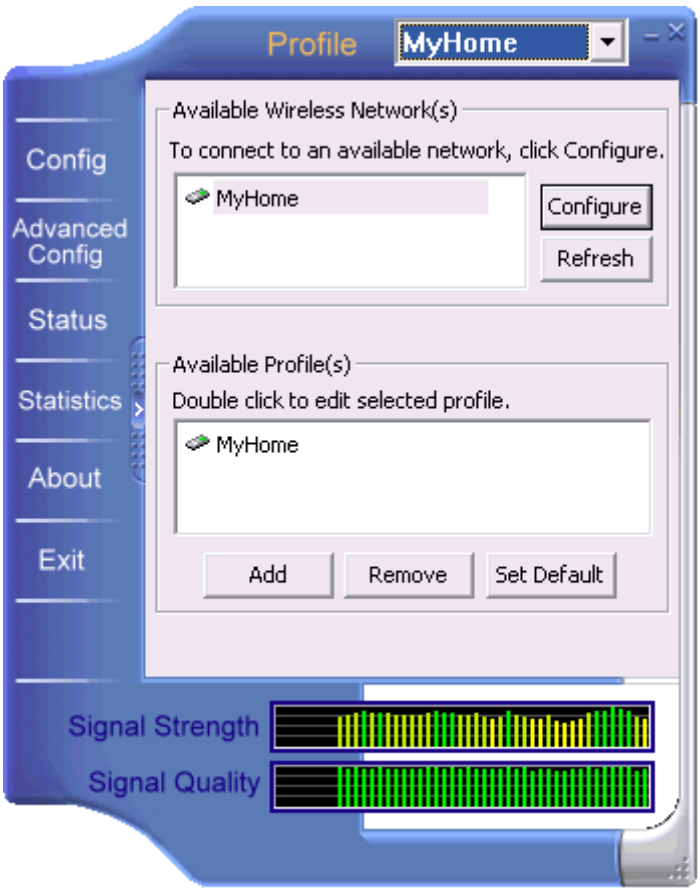
Создать новую сеть можно, открыв закладку «Setting».

Данная утилита имеет ряд особенностей, здесь можно создать до пяти профилей, позволяющих быстро менять параметры соединения. Создаем первый профиль, первоначально нужно указать имя сети (SSID), тип сети (AD - Hoc). Используемый канал связи и страну можно оставить без изменений. Дополнительные свойства соединения доступны в окне «Advance». Здесь пользователь может выбрать скорость

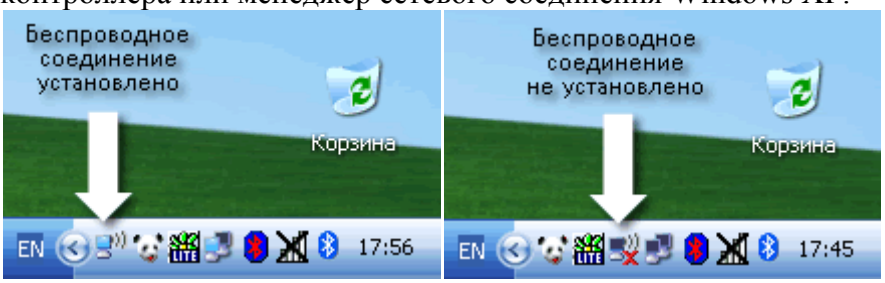
передачи, режим сохранения энергии (важно для ноутбуков), а также режим шифрования. На этом первый этап настройки настольного компьютера завершен и теперь необходимо **настроить беспроводную сеть** на ноутбуке.



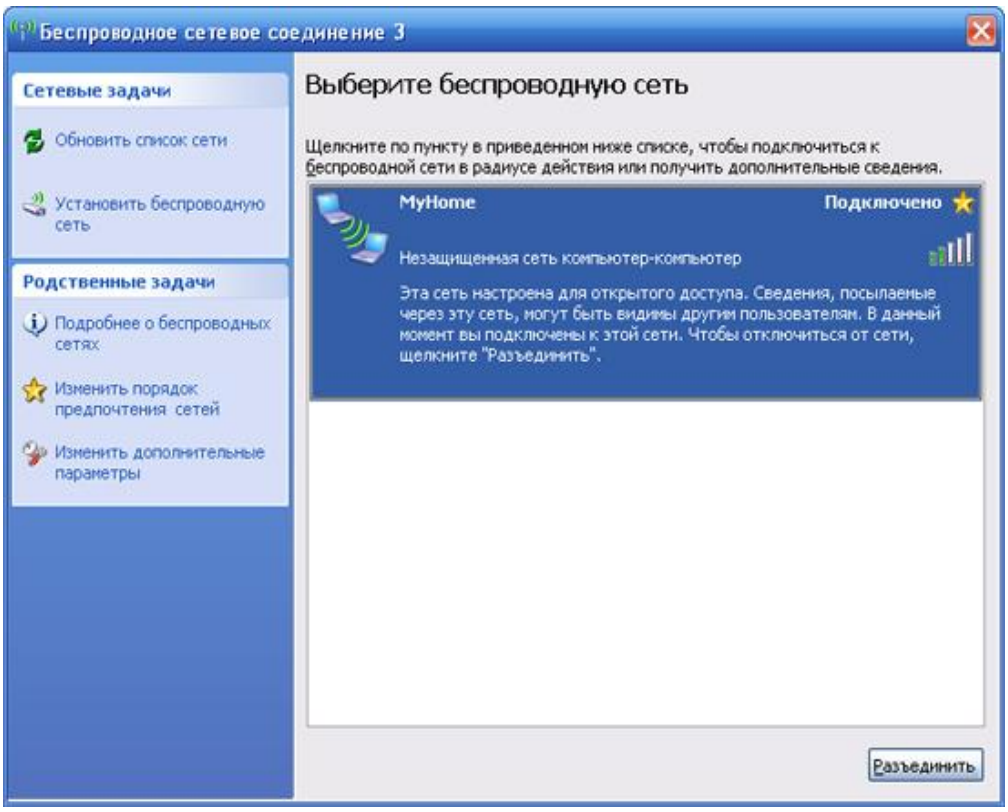
Данный процесс полностью идентичен настройке настольного компьютера, которую мы рассмотрели выше, за исключением Wi Fi контроллера и специализированной программы для его настройки.
Устанавливаем соединение между двумя компьютерами. Для этого используется как фирменная утилита, так и менеджер сетевого соединения Windows XP. Необходимо выполнить перезагрузку обоих компьютеров, что позволит установить автоматическое соединение, о чем будет свидетельствать иконка в системной области рабочего стола.



В случае если соединения не произошло, нужно открыть утилиту **настройки Wi Fi** контроллера или менеджер сетевого соединения Windows XP.



В основном окне менеджера отображается список обнаруженных сетей.



Теперь приступим к настройки IP соединения, настройки шлюза и совместного доступа к файлам и принтерам.
Для решения этой задачи необходимо зайти в свойства сетевого окружения, установить необходимые протоколы, путем нажатия кнопки добавить, а так же установить необходимые службы (служба доступа к файлам и папкам сетей Микрософт и клиент для сетей Микрософт). Так же необходимо правильно сконфигурировать ip адрес, таким образом чтобы он не был задействован во внутренней сети, что вызовет конфликт адресов в результате которого не удастся настроить шлюз. Далее нужно настроить файрвол.
Запускаем мастер **настройки** сети имя компьютера и описание (необязательно), а также имя рабочей группы.

Заключение.
Беспроводные локальные сети (WLAN – wireless LAN) могут использоваться в офисе для подключения мобильных сотрудников (ноутбуки, носимые терминалы) в местах скопления пользователей - аэропортах, бизнес-центрах, гостиницах и т. д.
Мобильный Интернет и мобильные **локальные сети** открывают корпоративным и домашним пользователям новые сферы применения карманных ПК, ноутбуков.
Одновременно с этим постоянно снижаются цены на беспроводное оборудование Wi Fi и расширяется его ассортимент. Wi Fi также подходит для людей, которым по долгу необходимо перемещаться по помещению, к примеру, на складе или в магазине. В этом случае для учета (отгрузки, приема и т. п.) товаров используются носимые терминалы, которые постоянно соединены с корпоративной сетью по протоколу Wi Fi, и все изменения сразу отражаются в центральной базе данных. WLAN применим и в организации временных сетей, когда долго и нерентабельно прокладывать провода, а потом их демонтировать.
Еще один вариант использования – в исторических постройках, где прокладка проводов невозможна или запрещена. Иногда не хочется портить внешний вид помещения

проводами или коробами для их прокладки. Кроме того, Wi Fi-протокол подходит и для бытового применения, где тем более неудобно прогладывать провода.
Что касается мобильных компьютеров, 12 марта 2003 года корпорация Intel представила технологию Intel Centrino для мобильных ПК — основу для мобильных компьютеров нового поколения со встроенными функциями беспроводной связи, которые предоставят корпоративным и домашним пользователям большую свободу и новые возможности подключения к компьютерным сетям. Технология, которую представляет торговая марка Intel Centrino для мобильных ПК, включает в себя процессор Intel Pentium M, семейство наборов микросхем Intel 855 и сетевой интерфейс Intel Pro/Wireless 2100. Все компоненты технологии оптимизированы, проверены и протестированы для совместной работы в мобильных системах.
Сетевой интерфейс Intel PRO/Wireless 2100 разработан и проверен на полную совместимость с узлами доступа 802.11b, сертифицированными по стандарту Wi Fi. Он оснащен мощными встроенными средствами безопасности для беспроводных **локальных сетей**, включая технологии 802.11x, WEP и VPN, с возможностью программного обновления до поддержки WPA.
Wi Fi технологии становятся все более совершенными и качество их соединения и безопасность стремительно приближается к возможностям обычного, широко используемого, проводного соединения.

Архитектура, компоненты сети и стандарты
Стандарт RadioEthernet IEEE 802.11 - это стандарт организации беспроводных коммуникаций на ограниченной территории в режиме локальной сети, т.е. когда несколько абонентов имеют равноправный доступ к общему каналу передач. 802.11 - первый промышленный стандарт для беспроводных **локальных сетей** (Wireless Local Area Networks), или WLAN. Стандарт был разработан Institute of Electrical and Electronics Engineers (IEEE), 802.11 может быть сравнен со стандартом 802.3 для обычных проводных Ethernet сетей.
Стандарт RadioEthernet IEEE 802.11 определяет порядок организации беспроводных сетей на уровне управления доступом к среде (MAC-уровне) и физическом (PHY) уровне. В стандарте определен один вариант MAC (Medium Access Control) уровня и три типа физических каналов.
Подобно проводному Ethernet, IEEE 802.11 определяет протокол использования единой среды передачи, получивший название carrier sense multiple access collision avoidance (CSMA/CA). Вероятность коллизий беспроводных узлов минимизируется путем предварительной посылки короткого сообщения, называемого ready to send (RTS), оно информирует другие узлы о продолжительности предстоящей передачи и адресате. Это позволяет другим узлам задержать передачу на время, равное объявленной длительности сообщения. Приемная станция должна ответить на RTS посылкой clear to send (CTS). Это позволяет передающему узлу узнать, свободна ли среда и готов ли приемный узел к приему. После получения пакета данных приемный узел должен передать подтверждение (ACK) факта безошибочного приема. Если ACK не получено, попытка передачи пакета данных будет повторена.
В стандарте предусмотрено обеспечение безопасности данных, которое включает аутентификацию для проверки того, что узел, входящий в сеть, авторизован в ней, а также шифрование для защиты от подслушивания.
На физическом уровне стандарт предусматривает два типа радиоканалов и один инфракрасного диапазона.
В основу стандарта 802.11 положена сотовая архитектура. Сеть может состоять из одной или нескольких ячеек (сот). Каждая сота управляется базовой станцией, называемой

точкой доступа (Access Point, AP). Точка доступа и находящиеся в пределах радиуса ее действия рабочие станции образуют базовую зону обслуживания (Basic Service Set, BSS). Точки доступа многосотовой сети взаимодействуют между собой через распределительную систему (Distribution System, DS), представляющую собой эквивалент магистрального сегмента кабельных ЛС. Вся инфраструктура, включающая точки доступа и распределительную систему, образует расширенную зону обслуживания (Extended Service Set). Стандартом предусмотрен также односотовый вариант беспроводной сети, который может быть реализован и без точки доступа, при этом часть ее функций выполняется непосредственно рабочими станциями.

В настоящее время существует множество стандартов семейства IEEE 802.11:

1. 802.11 - первоначальный основополагающий стандарт. Поддерживает передачу данных по радиоканалу со скоростями 1 и 2 (опционально) Мбит/с.
2. 802.11a - высокоскоростной стандарт WLAN. Поддерживает передачу данных со скоростями до 54 Мбит/с по радиоканалу в диапазоне около 5 ГГц.
3. 802.11b - самый распространенный стандарт. Поддерживает передачу данных со скоростями до 11 Мбит/с по радиоканалу в диапазоне около 2,4 ГГц.
4. 802.11c - Стандарт, регламентирующий работу беспроводных мостов. Данная спецификация используется производителями беспроводных устройств при разработке точек доступа.
5. 802.11d - Стандарт определял требования к физическим параметрам каналов (мощность излучения и диапазоны частот) и устройств беспроводных сетей с целью обеспечения их соответствия законодательным нормам различных стран.
6. 802.11e - Создание данного стандарта связано с использованием средств мультимедиа. Он определяет механизм назначения приоритетов разным видам трафика - таким, как аудио- и видеоприложения. Требование качества запроса, необходимое для всех радио интерфейсов IEEE WLAN.
7. 802.11f - Данный стандарт, связанный с аутентификацией, определяет механизм взаимодействия точек связи между собой при перемещении клиента между сегментами сети. Другое название стандарта - Inter Access Point Protocol. Стандарт, описывающий порядок связи между равнозначными точками доступа.
8. 802.11g - устанавливает дополнительную технику модуляции для частоты 2,4 ГГц. Предназначен, для обеспечения скоростей передачи данных до 54 Мбит/с по радиоканалу в диапазоне около 2,4 ГГц.
9. 802.11h – Разработка данного стандарта связана с проблемами при использовании 802.11a в Европе, где в диапазоне 5 ГГц работают некоторые системы спутниковой связи. Для предотвращения взаимных помех стандарт 802.11h имеет механизм "квазиинтеллектуального" управления мощностью излучения и выбором несущей частоты передачи. Стандарт, описывающий управление спектром частоты 5 ГГц для использования в Европе и Азии.
10. 802.11i (WPA2) – Целью создания данной спецификации является повышение уровня безопасности беспроводных сетей. В ней реализован набор защитных функций при обмене информацией через беспроводные сети - в частности, технология AES (Advanced Encryption Standard) - алгоритм шифрования, поддерживающий ключи длиной 128, 192 и 256 бит. Предусматривается совместимость всех используемых в данное время устройств - в частности, Intel Centrino - с 802.11i-сетями. Затрагивает протоколы 802.1X, TKIP и AES.
11. 802.11j - Спецификация предназначена для Японии и расширяет стандарт 802.11a добавочным каналом 4,9 ГГц.
12. 802.11n - Перспективный стандарт, находящийся на сегодняшний день в разработке, который позволит поднять пропускную способность сетей до 100 Мбит/сек.
13. 802.11r - Данный стандарт предусматривает создание универсальной и совместимой

системы роуминга для возможности перехода пользователя из зоны действия одной сети в зону действия другой.

Из всех существующих стандартов беспроводной передачи данных IEEE 802.11, на практике наиболее часто используются всего три, определенных Инженерным институтом электротехники и радиоэлектроники (IEEE), это: 802.11b, 802.11g и 802.11a.

Сравнение стандартов беспроводной передачи данных:
Стандарт 802.11b 802.11g 802.11a
Количество используемых радиоканалов 3 не перекрывающихся 3 не перекрывающихся 8 не перекрывающихся
Частотный диапазон 2.4 ГГц 2.4 ГГц 5 ГГц
Макс. скорость передачи данных 11 Мб/с 54 Мб/с 54 Мб/с
Примерная дальность действия 30 м при 11 Мб/с
100 м при 1 Мб/с 15 м при 54 Мб/с
50 м при 11 Мб/с 12 м при 54 Мб/с
100 м при 6 Мб/с

802.11b. В окончательной редакции широко распространенный стандарт 802.11b был принят в 1999 г. и благодаря ориентации на свободный от лицензирования диапазон 2,4 ГГц завоевал наибольшую популярность у производителей оборудования. Пропускная способность (теоретическая 11 Мбит/с, реальная — от 1 до 6 Мбит/с) отвечает требованиям большинства приложений. Поскольку оборудование 802.11b, работающее на максимальной скорости 11 Мбит/с, имеет меньший радиус действия, чем на более низких скоростях, то стандартом 802.11b предусмотрено автоматическое понижение скорости при ухудшении качества сигнала.
К началу 2004 года в эксплуатации находилось около 15 млн. радиоустройств 802.11b.
В конце 2001-го появился - стандарт беспроводных локальных сетей 802.11a, функционирующих в частотном диапазоне 5 ГГц (диапазон ISM). Беспроводные ЛВС стандарта IEEE 802.11a обеспечивают скорость передачи данных до 54 Мбит/с, т. е. примерно в пять раз быстрее сетей 802.11b, и позволяют передавать большие объемы данных, чем сети IEEE 802.11b.
К недостаткам 802.11a относятся большая потребляемая мощность радиопередатчиков для частот 5 ГГц, а также меньший радиус действия (оборудование для 2,4 ГГц может работать на расстоянии до 300 м, а для 5 ГГц — около 100 м). Кроме того, устройства для 802.11a дороже, но со временем ценовой разрыв между продуктами 802.11b и 802.11a будет уменьшаться.
802.11g является новым стандартом, регламентирующим метод построения WLAN, функционирующих в нелицензируемом частотном диапазоне 2,4 ГГц. Максимальная скорость передачи данных в беспроводных сетях IEEE 802.11g составляет 54 Мбит/с. Стандарт 802.11g представляет собой развитие 802.11b и обратно совместим с 802.11b. Соответственно ноутбук с картой 802.11g сможет подключаться и к уже действующим точкам доступа 802.11b, и ко вновь создаваемым 802.11g. Теоретически 802.11g обладает достоинствами двух своих предшественников. В числе преимуществ 802.11g надо отметить низкую потребляемую мощность, большую дальность действия и высокую проникающую способность сигнала. Можно надеяться и на разумную стоимость оборудования, поскольку низкочастотные устройства проще в изготовлении.

1.2. Организация сети

Стандарт IEEE 802.11 работает на двух нижних уровнях модели ISO/OSI: физическом и канальном. Другими словами, использовать оборудование Wi Fi так же просто, как и Ethernet: протокол TCP/IP накладывается поверх протокола, описывающего передачу информации по каналу связи. Расширение IEEE 802.11b не затрагивает канальный уровень и вносит изменения в IEEE 802.11 только на физическом уровне.

В беспроводной локальной сети есть два типа оборудования: клиент (обычно это компьютер, укомплектованный беспроводной сетевой картой, но может быть и иное устройство) и точка доступа, которая выполняет роль моста между беспроводной и проводной сетями. Точка доступа содержит приемопередатчик, интерфейс проводной сети, а также встроенный микрокомпьютер и программное обеспечение для обработки данных.

1.2.1. Физический уровень IEEE 802.11

Стандарт IEEE 802.11 предусматривает передачу сигнала одним из двух методов - прямой последовательности (Direct Sequence Spread Spectrum, DSSS) и частотных скачков (Frequency Hopping Spread Spectrum, FHSS) различающиеся способом модуляции, но использующие одну и ту же технологию расширения спектра. Основной принцип технологии расширения спектра (Spread Spectrum, SS) заключается в том, чтобы от узкополосного спектра сигнала, возникающего при обычном потенциальном кодировании, перейти к широкополосному спектру, что позволяет значительно повысить помехоустойчивость передаваемых данных

Метод FHSS предусматривает изменение несущей частоты сигнала при передаче информации. Для повышения помехоустойчивости нужно увеличить спектр передаваемого сигнала, для чего несущая частота меняется по псевдослучайному закону, и каждый пакет данных передается на своей несущей частоте. При использовании FHSS конструкция приемопередатчика получается очень простой, но этот метод применим, только если пропускная способность не превышает 2 Мбит/с, так что в дополнении IEEE 802.11b остался один DSSS. Из этого следует, что совместно с устройствами IEEE 802.11b может применяться только то оборудование стандарта IEEE 802.11, которое поддерживает DSSS, при этом скорость передачи не превысит максимальной скорости в "узком месте" (2 Мбит/с), коим является оборудование, использующее старый стандарт без расширения.

В основе метода DSSS лежит принцип фазовой манипуляции (т.е. передачи информации скачкообразным изменением начальной фазы сигнала). Для расширения спектра передаваемого сигнала применяется преобразование передаваемой информации в так называемый код Баркера, являющийся псевдослучайной последовательностью. На каждый передаваемый бит приходится 11 бит в последовательности Баркера. Различают прямую и инверсную последовательности Баркера. Из-за большой избыточности при кодировании вероятность того, что действие помехи превратит прямую последовательность Баркера в инверсную, близка к нулю. Единичные биты передаются прямым кодом Баркера, а нулевые - инверсным.

Под беспроводные компьютерные сети в диапазоне 2,4 ГГц отведен довольно узкий "коридор" шириной 83 МГц, разделенный на 14 каналов. Для исключения взаимных помех между каналами необходимо, чтобы их полосы отстояли друг от друга на 25 МГц.

Несложный подсчет показывает, что в одной зоне одновременно могут использоваться только три канала. В таких условиях невозможно решить проблему отстройки от помех автоматическим изменением частоты, вот почему в беспроводных локальных сетях используется кодирование с высокой избыточностью. В ситуации, когда и эта мера не позволяет обеспечить заданную достоверность передачи, скорость с максимального значения 11 Мбит/с последовательно снижается до одного из следующих фиксированных значений: 5,5; 2; 1 Мбит/с. Снижение скорости происходит не только при высоком уровне помех, но и если расстояние между элементами беспроводной сети достаточно велико.

1.2.2. Канальный уровень IEEE 802.11

Подобно проводной сети Ethernet, в беспроводных компьютерных сетях Wi Fi канальный уровень включает в себя подуровни управления логическим соединением (Logical Link Control, LLC) и управления доступом к среде передачи (Media Access Control, MAC). У Ethernet и IEEE 802.11 один и тот же LLC, что значительно упрощает объединение проводных и беспроводных сетей. MAC у обоих стандартов имеет много общего, однако есть некоторые тонкие различия, принципиальные для сравнения проводных и беспроводных сетей.

В Ethernet для обеспечения возможности множественного доступа к общей среде передачи (в данном случае кабелю) используется протокол CSMA/CD, обеспечивающий выявление и обработку коллизий (в терминологии компьютерных сетей так называются ситуации, когда несколько устройств пытаются начать передачу одновременно).

В сетях IEEE 802.11 используется полудуплексный режим передачи, т.е. в каждый момент времени станция может либо принимать, либо передавать информацию, поэтому обнаружить коллизию в процессе передачи невозможно. Для IEEE 802.11 был разработан модифицированный вариант протокола CSMA/CD, получивший название CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Работает он следующим образом. Станция, которая собирается передавать информацию, сначала "слушает эфир". Если не обнаружено активности на рабочей частоте, станция сначала ожидает в течение некоторого случайного промежутка времени, потом снова "слушает эфир" и, если среда передачи данных все еще свободна, осуществляет передачу. Наличие случайной задержки необходимо для того, чтобы сеть не зависла, если несколько станций одновременно захотят получить доступ к частоте. Если информационный пакет приходит без искажений, принимающая станция посылает обратно подтверждение. Целостность пакета проверяется методом контрольной суммы. Получив подтверждение, передающая станция считает процесс передачи данного информационного пакета завершенным. Если подтверждение не получено, станция считает, что произошла коллизия, и пакет передается снова через случайный промежуток времени.

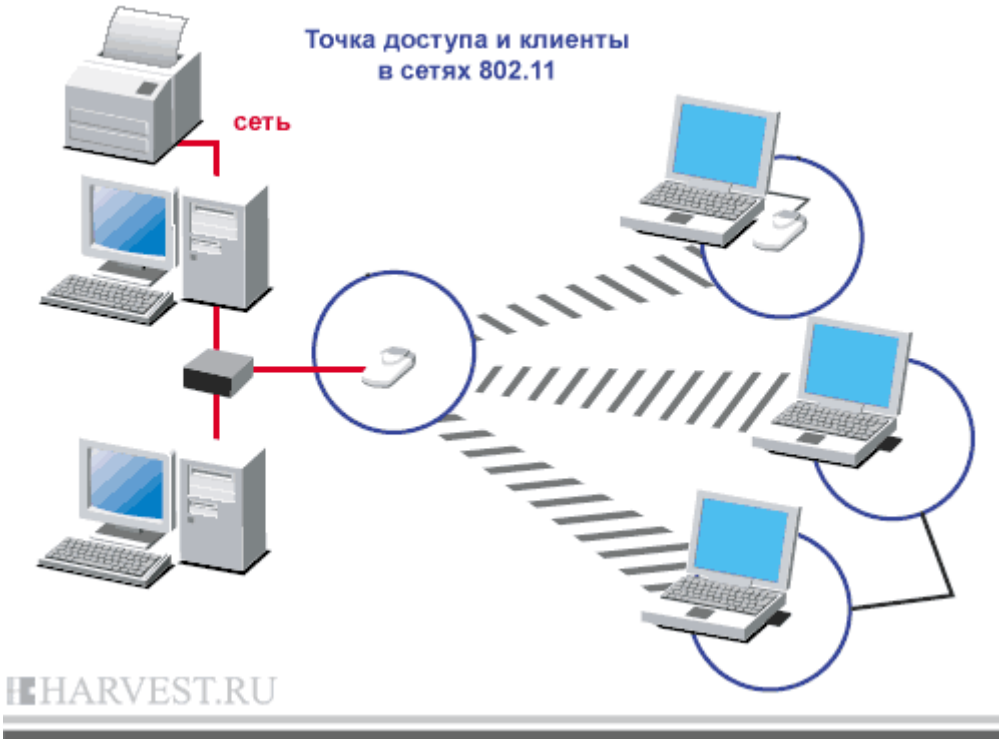
Еще одна специфичная для беспроводных сетей проблема - две клиентские станции имеют плохую связь друг с другом, но при этом качество связи каждой из них с точкой доступа хорошее. В таком случае передающая клиентская станция может послать на точку доступа запрос на очистку эфира. Тогда по команде с точки доступа другие клиентские станции прекращают передачу на время "общения" двух точек с плохой связью. Режим принудительной очистки эфира (протокол Request to Send/Clear to Send - RTS/CTS) реализован далеко не во всех моделях оборудования IEEE 802.11 и, если он есть, то включается лишь в крайних случаях.

В Ethernet при передаче потоковых данных используется управление доступом к каналу связи, распределенное между всеми станциями. Напротив, в IEEE 802.11 в таких случаях применяется централизованное управление с точки доступа. Клиентские станции

последовательно опрашиваются на предмет передачи потоковых данных. Если какая-нибудь из станций сообщает, что она будет передавать потоковые данные, точка доступа выделяет ей промежуток времени, в который из всех станций сети будет передавать только она.
Следует отметить, что принудительная очистка эфира снижает эффективность работы беспроводной сети, поскольку связана с передачей дополнительной служебной информации и кратковременными перерывами связи. Кроме этого, в проводных сетях Ethernet при необходимости можно реализовать не только полудуплексный, но и дуплексный вариант передачи, когда коллизия обнаруживается в процессе передачи (это повышает реальную пропускную способность сети). Поэтому, увы, при прочих равных условиях реальная пропускная способность беспроводной сети IEEE 802.11b будет ниже, чем у проводного Ethernet. Таким образом, если сетям Ethernet 10 Мбит/с и IEEE 802.11b (максимальная скорость передачи информации 11 Мбит/с) с одинаковым числом пользователей давать одинаковую нагрузку, постепенно увеличивая ее, то, начиная с некоторого порога, сеть IEEE 802.11b начнет "тормозить", а Ethernet все еще будет функционировать нормально.
Поскольку клиентские станции могут быть мобильными устройствами с автономным питанием, в стандарте IEEE 802.11 большое внимание уделено вопросам управления питанием. В частности, предусмотрен режим, когда клиентская станция через определенные промежутки времени "просыпается", чтобы принять сигнал включения, который, возможно, передает точка доступа. Если этот сигнал принят, клиентское устройство включается, в противном случае оно снова "засыпает" до следующего цикла приема информации.

1.3.Типы и разновидности соединений
1. 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 Мбит/с, чего вполне достаточно для нормальной работы.

2. Инфраструктурное соединение.
Все компьютеры оснащены беспроводными картами и подключаются к точке доступа. Которая, в свою очередь, имеет возможность подключения к проводной сети.



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

3. 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.

4. 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 MAC-адрес. Здесь задача состоит в том, чтобы объединить только два компьютера. Два WiFi-адаптера могут работать друг с другом напрямую без центральных антенн.

5. 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.

6. Репитер.
Точка доступа просто расширяет радиус действия другой точки доступа, работающей в инфраструктурном режиме.

1.4. Безопасность WiFi сетей
Как и любая компьютерная сеть, WiFi – является источником повышенного риска несанкционированного доступа. Кроме того, проникнуть в беспроводную сеть значительно проще, чем в обычную, — не нужно подключаться к проводам, достаточно оказаться в зоне приема сигнала.
Беспроводные сети отличаются от кабельных только на первых двух - физическом (Phy) и отчасти канальном (MAC) - уровнях семиуровневой модели взаимодействия открытых систем. Более высокие уровни реализуются как в проводных сетях, а реальная безопасность сетей обеспечивается именно на этих уровнях. Поэтому разница в безопасности тех и других сетей сводится к разнице в безопасности физического и MAC-уровней.
Хотя сегодня в защите WiFi-сетей применяются сложные алгоритмические математические модели аутентификации, шифрования данных и контроля целостности их передачи, тем не менее, вероятность доступа к информации посторонних лиц является весьма существенной. И если **настройке сети** не уделить должного внимания злоумышленник может:
• заполучить доступ к ресурсам и дискам пользователей WiFi-сети, а через неё и к ресурсам LAN;
• подслушивать трафик, извлекать из него конфиденциальную информацию;
• искажать проходящую в сети информацию;

• воспользоваться интернет-траффиком;
• атаковать ПК пользователей и серверы сети
• внедрять поддельные точки доступа;
• рассылать спам, и совершать другие противоправные действия от имени вашей сети.
Для защиты сетей 802.11 предусмотрен комплекс мер безопасности передачи данных.
На раннем этапе использования WiFi сетей таковым являлся пароль SSID (Server Set ID) для доступа в локальную сеть, но со временем оказалось, что данная технология не может обеспечить надежную защиту.
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. 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, в результате 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 вектор инициализации. Поскольку мы говорим о 24 битах, это подразумевает около 16 миллионов комбинаций, после использования этого количества, ключ начинает повторяться. Хакеру необходимо найти 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.
Как показало время, WEP тоже оказалась не самой надёжной технологией защиты. 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 поддерживает данный стандарт, и по умолчанию время одного сеанса равно 30 минутам. IEEE 802.1X — это новый стандарт, который оказался ключевым для развития индустрии беспроводных сетей в целом. 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 (EAP), протоколе защиты транспортного уровня (TLS) и сервере доступа Remote Access Dial-in User Server. Протокол защиты транспортного уровня TLS обеспечивает взаимную аутентификацию и целостность передачи данных. Все ключи являются 128-разрядными по умолчанию.
В конце 2003 года был внедрён стандарт WiFi Protected Access (WPA), который совмещает преимущества динамического обновления ключей IEEE 802.1X с кодированием протокола интеграции временного ключа TKIP, протоколом расширенной аутентификации (EAP) и технологией проверки целостности сообщений MIC. 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
• EAP — протокол расширенной аутентификации (Extensible Authentication Protocol)

• TKIP — протокол интеграции временного ключа (Temporal Key Integrity Protocol)
• MIC — технология проверки целостности сообщений (Message Integrity Check).
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, уже давно используется в VPN. Что касается WPA, поддержка AES уже реализована в Windows XP, пока только опционально.
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, который, в настоящее время является максимально защищённым.
Таким образом, на сегодняшний день у обычных пользователей и администраторов сетей имеются все необходимые средства для надёжной защиты WiFi, и при отсутствии явных ошибок (пресловутый человеческий фактор) всегда можно обеспечить уровень безопасности, соответствующий ценности информации, находящейся в такой сети.
Сегодня беспроводную сеть считают защищенной, если в ней функционируют три основных составляющих системы безопасности: аутентификация пользователя, конфиденциальность и целостность передачи данных. Для получения достаточного уровня безопасности необходимо воспользоваться рядом правил при организации и **настройке частной WiFi-сети**:
• Шифровать данные путем использования различных систем. Максимальный уровень безопасности обеспечит применение VPN;
• использовать протокол 802.1X;
• запретить доступ к **настройкам точки доступа** с помощью беспроводного подключения;
• управлять доступом клиентов по MAC-адресам;
• запретить трансляцию в эфир идентификатора SSID;
• располагать антенны как можно дальше от окон, внешних стен здания, а также ограничивать мощность радиоизлучения;
• использовать максимально длинные ключи;
• изменять статические ключи и пароли;
• использовать метод WEP-аутентификации “Shared Key" так как клиенту для входа в сеть необходимо будет знать WEP-ключ;
• пользоваться сложным паролем для доступа к **настройкам точки доступа;**
• по возможности не использовать в беспроводных сетях протокол TCP/IP для организации папок, файлов и принтеров общего доступа. Организация разделяемых ресурсов средствами NetBEUI в данном случае безопаснее;
• не разрешать гостевой доступ к ресурсам общего доступа, использовать длинные сложные пароли;
• не использовать в беспроводной сети DHCP. Вручную распределить статические IP-адреса между легитимными клиентами безопаснее;
• на всех ПК внутри беспроводной сети установить файерволлы, не устанавливать точку доступа вне брандмауэра, использовать минимум протоколов внутри WLAN (например,

только HTTP и SMTP);
• регулярно исследовать уязвимости сети с помощью специализированных сканеров безопасности (например NetStumbler)
• использовать специализированные сетевые операционные системы такие как, Windows Nt, Windows 2003, Windows Xp.
Так же угрозу сетевой безопасности могут представлять природные явления и технические устройства, однако только люди (недовольные уволенные служащие, хакеры, конкуренты) внедряются в сеть для намеренного получения или уничтожения информации и именно они представляют наибольшую угрозу.