БЕСПРОВОДНЫЕ ТЕХНОЛОГИИ СВЯЗИ В ИНФОКОММУНИКАЦИОННЫХ СЕТЯХ И СИСТЕМАХ

БЕСПРОВОДНАЯ СВЯЗЬ

В 90-х годах XIX века – первые эксперименты по передаче телеграфных сообщений с помощью радиосигналов.

С 20-х годов XX века началось применение радио для передачи голоса.

Сегодня существует большое число беспроводных телекоммуникационных систем:

- широковещательных, таких как радио или телевидение
- линий для передачи дискретной информации

Для создания протяженных линий связи используются радиорелейные и спутниковые системы

Применяются беспроводные системы доступа к сетям операторов связи и беспроводные локальные сети.

ОСОБЕННОСТИ БЕСПРОВОДНОЙ СВЯЗИ

Беспроводная среда передачи данных отличается **высоким уровнем помех**, которые создают внешние источники излучения, а также многократно отраженные сигналы.

В беспроводных системах связи применяют различные **средства для снижения влияния помех**.

- К числу таких средств входят **коды прямой коррекции ошибок** и **протоколы с подтверждением доставки информации**.
- Средством борьбы с помехами является использование **технологии расширенного спектра**, разработанной специально для беспроводных систем.

ПРЕИМУЩЕСТВА БЕСПРОВОДНЫХ КОММУНИКАЦИЙ

Основное преимущество беспроводных линий связи – возможность передавать информацию от абонента к абоненту без проводов, привязывающих абонентов к определенной точке пространства.

С развитием технологий системы беспроводной связи приобрели две необходимые составляющие успеха — **удобство использования** и **низкую стоимость**.

БЕСПРОВОДНАЯ ЛИНИЯ СВЯЗИ

- Беспроводная линия связи строится в соответствии с достаточно простой схемой:
  - Каждый узел оснащается антенной, которая одновременно является передатчиком и приемником электромагнитных волн.
- Электромагнитные волны распространяются в атмосфере или вакууме со скоростью $3x10^8$ м/с во всех направлениях или же в пределах определенного сектора.

РАЗДЕЛЯЕМАЯ СРЕДА

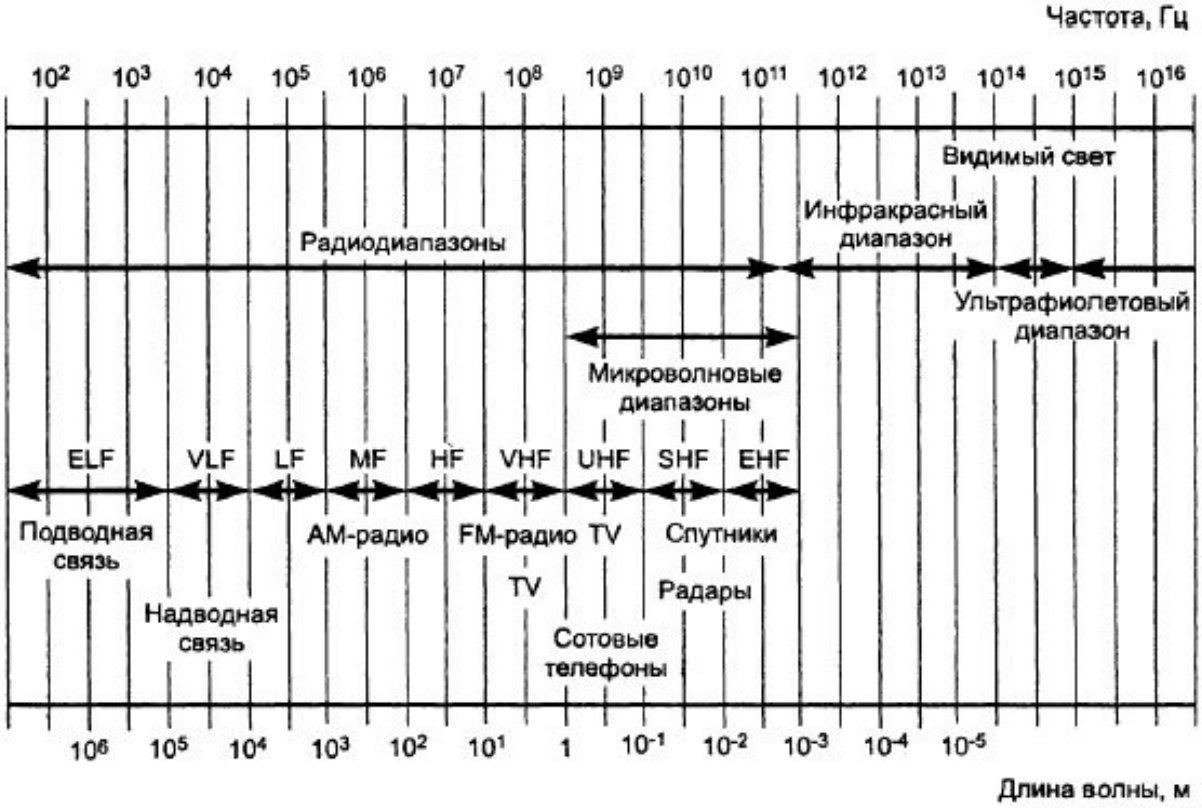
При ненаправленном распространении электромагнитные волны заполняют все пространство (в пределах определенного радиуса, определяемого затуханием мощности сигнала), то это пространство является *разделяемой средой*.

- Разделение среды передачи для беспроводных систем приводит к тому, что пространство в отличие от кабельной системы является **общедоступным**, а не принадлежит одной организации.

Кроме того, проводная среда строго определяет направление распространения сигнала в пространстве, а *беспроводная среда является ненаправленной*.

ДИАПАЗОНЫ ЭЛЕКТРОМАГНИТНОГО СПЕКТРА

- Характеристики беспроводной линии связи — расстояние между узлами, территория охвата, скорость передачи информации и т. п. — во многом зависят от частоты используемого электромагнитного спектра.



ДИАПАЗОНЫ ЭЛЕКТРОМАГНИТНОГО СПЕКТРА

- Диапазон до 300 ГГц имеет общее стандартное название — **радиодиапазон.**
- Союз ITU разделил его на несколько поддиапазонов, начиная от сверхнизких частот (Extremely Low Frequency, ELF) и заканчивая сверхвысокими (Extra High Frequency, EHF).
- Радиостанции работают в диапазоне от 20 кГц до 300 МГц, и для этих диапазонов существует не определенное в стандартах, но часто используемое название **широковещательное радио.**
  - Сюда попадают низкоскоростные системы AM- и FM-диапазонов, предназначенные для передачи данных со скоростями от нескольких десятков до сотен килобит в секунду.
  - Передача данных - радиомодемы, которые соединяют два сегмента локальной сети на скоростях 2400, 9600 или 19200 Кбит/с.

ДИАПАЗОНЫ ЭЛЕКТРОМАГНИТНОГО СПЕКТРА

- **Микроволновые системы (**диапазон от 300 МГц до 3000 ГГц) представляют наиболее широкий класс систем, объединяющий радиорелейные линии связи, спутниковые каналы, беспроводные локальные сети и системы фиксированного беспроводного доступа, называемые также системами беспроводных абонентских окончаний (Wireless Local Loop, WLL).
- Выше микроволновых диапазонов располагается инфракрасный диапазон. Инфракрасное излучение не может проникать через стены, то **системы инфракрасных волн** используются для образования небольших сегментов локальных сетей в пределах одного помещения.
- **Системы видимого света** используются как высокоскоростная альтернатива микроволновым двухточечным каналам для организации доступа на небольших расстояниях.

ДИАПАЗОНЫ ЛОКАЛЬНЫХ БЕСПРОВОДНЫХ СЕТЕЙ

- Для обеспечения работы локальных беспроводных сетей используются следующие диапазоны:
  - **Микроволновый – 2,4 ГГц, 5 ГГц**
  - **Инфракрасного диапазона – 900 нм**

ОСНОВНЫЕ ОБЛАСТИ ПРИМЕНЕНИЯ БЕСПРОВОДНЫХ ЛОКАЛЬНЫХ СЕТЕЙ

- *Резидентный доступ альтернативных операторов связи,* у которых нет проводного доступа к клиентам, проживающим в многоквартирных домах.
- *Доступ* в аэропортах, железнодорожных вокзалах и т. п.
- Организация локальных сетей в зданиях, где нет возможности установить современную кабельную систему, например, *в исторических зданиях* с оригинальным интерьером.
- Организация *временных локальных сетей,* например, при проведении конференций.
- *Расширения локальных сетей.* Небольшое число рабочих мест в таком здании делает крайне невыгодным прокладку к нему отдельного кабеля, поэтому беспроводная связь оказывается более рациональным вариантом.
- *Мобильные локальные сети.* Пользователь получает возможность пользоваться услугами сети, перемещаясь из помещения в помещение или из здания в здание.

НЕРАВНОМЕРНОСТЬ ИНТЕНСИВНОСТИ СИГНАЛА

Неравномерное распределение интенсивности сигнала приводит:

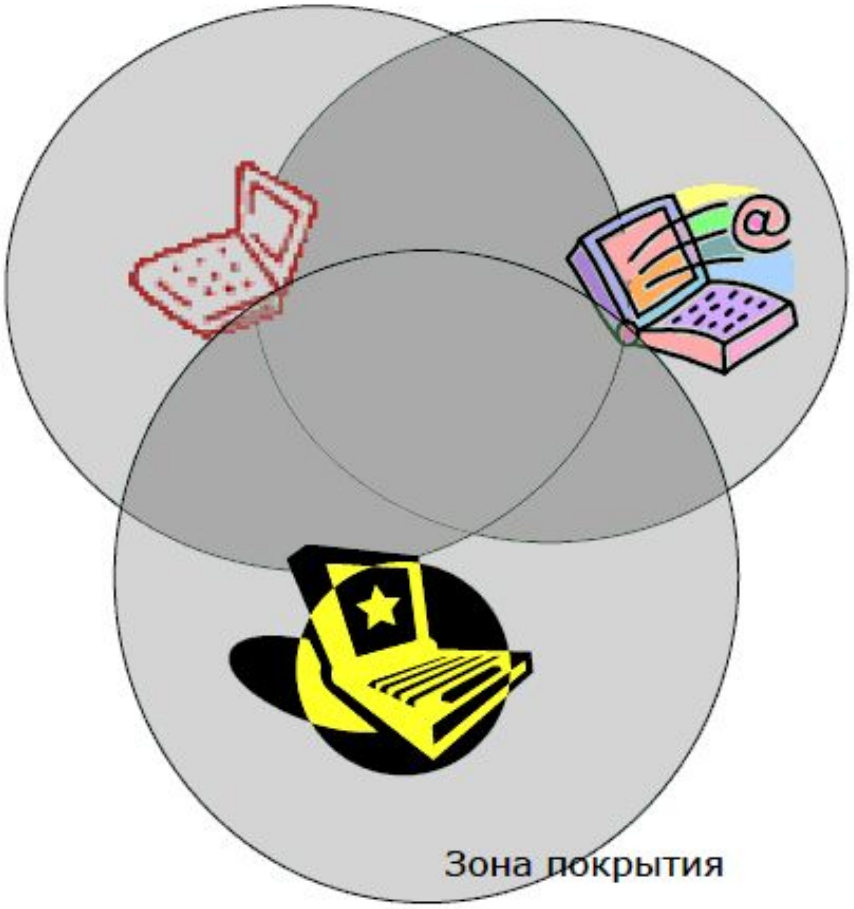
- к *битовым ошибкам* передаваемой информации;
- к *неопределенности зоны покрытия* беспроводной локальной сети.

В проводных локальных сетях только те устройства, которые подключены к кабельной системе получают сигналы и участвуют в работе ЛВС.

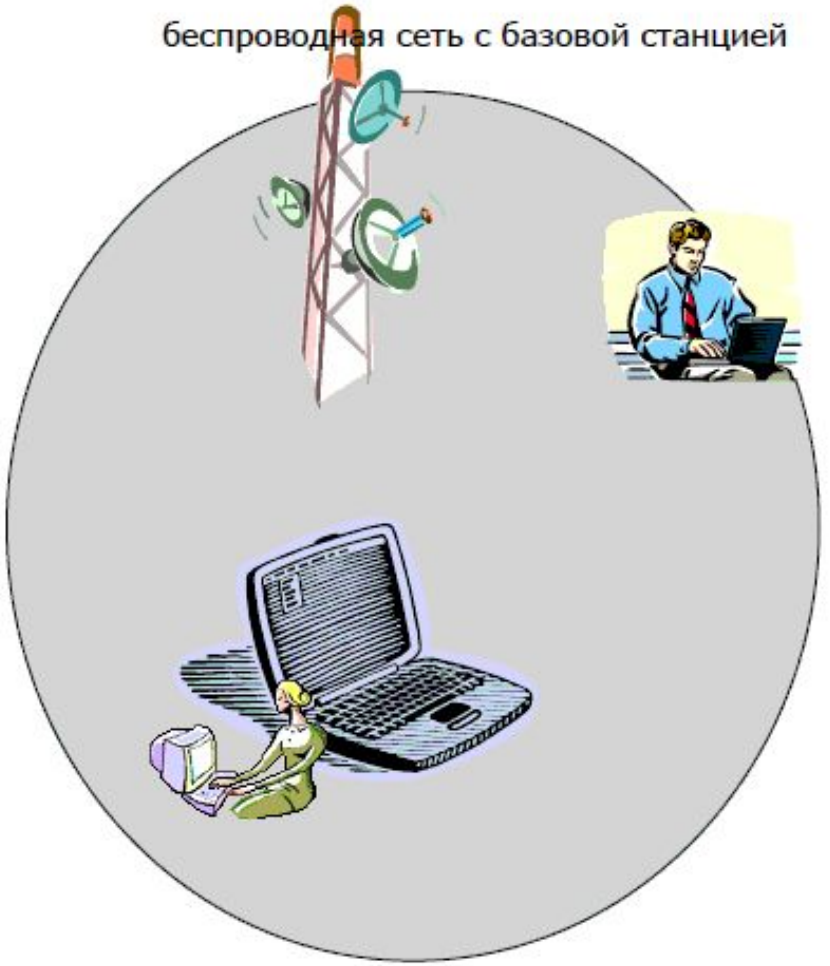
Беспроводная локальная сеть не имеет точной области покрытия.

ОБЕСПЕЧЕНИЕ СВЯЗНОСТИ БЕСПРОВОДНОЙ ЛОКАЛЬНОЙ СЕТИ

специализированная беспроводная сеть



беспроводная сеть с базовой станцией



ПРОБЛЕМА НЕПОЛНОСВЯЗНОСТИ

- Неполносвязность беспроводной сети порождает проблему доступа к разделяемой среде, известную под названием **скрытого терминала.**
  - Проблема возникает в том случае, когда два узла находятся вне зон досягаемости друг друга (узлы A и C), но существует третий узел B, который принимает сигналы как от A, так и от C.
- Если в радиосети используется традиционный метод доступа, основанный на прослушивании несущей, например CSMA/CD. Коллизии будут возникать значительно чаще, чем в проводных сетях.
  - Пусть, например, узел B занят обменом с узлом A. Узлу C сложно определить, что среда занята, он может посчитать ее свободной и начать передавать свой кадр.
  - В результате сигналы в районе узла B будут искажены, то есть произойдет коллизия, вероятность возникновения которой в проводной сети была бы неизмеримо ниже.
- Применение базовой станции может улучшить связность сети.
  - Базовая станция обычно обладает большей мощностью, а ее антенна устанавливается так, чтобы более равномерно и беспрепятственно покрывать нужную территорию.

ТЕХНОЛОГИЯ ШИРОКОПОЛОСНОГО СИГНАЛА

- **Технология расширенного спектра** разработана специально для беспроводной передачи.
  - Она позволяет улучшить помехоустойчивость кода для сигналов малой мощности.
- Технология расширенного спектра — не единственная техника кодирования, которая применяется для беспроводных линий связи микроволнового диапазона.
  - Также применяются частотная (FSK) и фазовая (PSK) манипуляции сигнала. Амплитудная манипуляция (ASK) не используется по той причине, что каналы микроволнового диапазона имеют широкую полосу пропускания, а усилители, которые обеспечивают одинаковый коэффициент усиления для широкого диапазона частот, очень дороги.

ОРТОГОНАЛЬНОЕ ЧАСТОТНОЕ МУЛЬТИПЛЕКСИРОВАНИЕ

- Использование широкой полосы пропускания позволяет применять модуляцию с несколькими несущими, когда полоса делится на несколько подканалов, каждый из которых использует свою несущую частоту.
- Битовый поток делится на несколько подпотоков, текущих с более низкой скоростью. Затем каждый подпоток модулируется с помощью определенной несущей частоты, которая кратна основной несущей частоте, то есть f_0, $2 f_0$, $3 f_0$ и т. д.
- Модуляция отдельных потоков выполняется с помощью обычных методов FSK или PSK.
- Такая техника называется **ортогональным частотным мультиплексированием** (Orthogonal Frequency Division Multiplexing, OFDM).

ПРОЦЕДУРА ОРТОГОНАЛЬНОГО ЧАСТОТНОГО МУЛЬТИПЛЕКСИРОВАНИЯ

- Перед передачей все несущие потоки сворачиваются в общий сигнал путем быстрого преобразования Фурье.
  - Спектр такого сигнала примерно равен спектру сигнала, кодируемого одной несущей.
- После передачи из общего сигнала путем обратного преобразования Фурье выделяются несущие подканалы, а затем из каждого канала выделяется битовый поток.
  - Выигрыш в разделении исходного высокоскоростного битового потока на несколько низкоскоростных подпотоков проявляется в том, что увеличивается интервал между отдельными символами кода.
- Это означает, что снижается эффект межсимвольной интерференции, вызванный многолучевого распространения электромагнитных волн.

РАСШИРЕНИЕ СПЕКТРА СКАЧКООБРАЗНОЙ ПЕРЕСТРОЙКОЙ ЧАСТОТЫ

- Метод **расширения спектра скачкообразной перестройкой частоты** (Frequency Hopping Spread Spectrum, FHSS):
  - На каждой несущей частоте для передачи дискретной информации применяются стандартные методы модуляции, такие как FSK или PSK.
  - Для синхронизации, для обозначения начала каждого периода передачи в течение некоторого времени передаются синхробиты.
  - Полезная скорость этого метода кодирования оказывается меньше из-за постоянных накладных расходов на синхронизацию.

Хеди Ламмар

В августе 1942 года Ламарр и Антейл получили патент под номером 2 292 387 «Секретная система связи (Secret Communication System)». Патент описывает секретные системы связи, включающие передачу ложных каналов на разных частотах. Однако американский флот отверг проект из-за сложности в реализации. Но спустя полвека этот патент стал основой для связи с расширенным спектром, которая сегодня используется повсюду, от мобильных телефонов до Wi-Fi.

РАСШИРЕНИЕ СПЕКТРА СКАЧКООБРАЗНОЙ ПЕРЕСТРОЙКОЙ ЧАСТОТЫ (ПРОДОЛЖЕНИЕ)

- Несущая частота меняется в соответствии с номерами частотных подканалов, вырабатываемых алгоритмом псевдослучайных чисел.
  - Псевдослучайная последовательность зависит от некоторого параметра, который называют **начальным числом.**
- Если приемнику и передатчику известны алгоритм и значение начального числа, то они меняют частоты в одинаковой последовательности, называемой **последовательностью псевдослучайной перестройки частоты.**

ПРЯМОЕ ПОСЛЕДОВАТЕЛЬНОЕ РАСШИРЕНИЕ СПЕКТРА

- В методе **прямого последовательного расширения спектра** (Direct Sequence Spread Spectrum, DSSS) также используется весь частотный диапазон, выделенный для одной беспроводной линии связи.
- В отличие от метода FHSS весь частотный диапазон занимается не за счет постоянных переключений с частоты на частоту, а за счет того, что каждый бит информации заменяется N битами, так что тактовая скорость передачи сигналов увеличивается в N раз.
  - Такой подход означает, что спектр сигнала также расширяется в N раз. Достаточно соответствующим образом выбрать скорость передачи данных и значение N, чтобы спектр сигнала заполнил весь диапазон.
- Цель кодирования методом DSSS та же, что методом FHSS — повышение устойчивости к помехам.
- Узкополосная помеха будет искажать только определенные частоты спектра сигнала, так что приемник с большой степенью вероятности сможет правильно распознать передаваемую информацию.

РАСШИРЕНИЕ СПЕКТРА

- Код, которым заменяется двоичная единица исходной информации, называется **расширяющей последовательностью**, а каждый бит такой последовательности — **чипом.**
  - Скорость передачи результирующего кода называют **чиповой скоростью**.
- Двоичный нуль кодируется инверсным значением расширяющей последовательности.
  - Приемники должны знать расширяющую последовательность, которую использует передатчик, чтобы понять передаваемую информацию.
- Количество битов в расширяющей последовательности определяет **коэффициент расширения** исходного кода.
  - Для кодирования битов результирующего кода может использоваться любой вид модуляции.
  - Чем больше коэффициент расширения, тем шире спектр результирующего сигнала и тем больше степень подавления помех.
  - При этом растет занимаемый каналом диапазон спектра. Обычно коэффициент расширения имеет значения от 10 до 100.

СТЕК ПРОТОКОЛОВ IEEE 802.11

- Стек протоколов стандарта IEEE 802.11 соответствует общей структуре стандартов комитета 802, включает в себя физический уровня и уровеbнь MAC, над которыми работает уровень LLC.
- Технология 802.11 определяется нижними двумя уровнями, то есть физическим уровнем и уровнем MAC, а уровень LLC выполняет свои стандартные общие для всех технологий LAN функции.
- На физическом уровне существует несколько вариантов спецификаций, которые отличаются используемым частотным диапазоном, методом кодирования и как следствие — скоростью передачи данных.
- Все варианты физического уровня работают с одним и тем же алгоритмом уровня MAC, но некоторые временные параметры уровня MAC зависят от используемого физического уровня.

ВАРИАНТЫ ФИЗИЧЕСКОГО УРОВНЯ 802.11

В 1997 году комитетом **802.11** был принят стандарт, который определял функции уровня MAC вместе с *тремя вариантами физического уровня*, которые обеспечивают передачу данных со скоростями 1 и 2 Мбит/с:

- В первом варианте средой являются *инфракрасные волны* диапазона 850 нм, которые генерируются либо полупроводниковым лазерным диодом, либо светодиодом (LED).
- Во втором варианте в качестве передающей среды используется *микроволновый диапазон* 2,4 ГГц, который в соответствии с рекомендациями ITU в большинстве стран не лицензируется. Этот вариант основан на методе FHSS. Количество каналов и частота переключения между каналами настраиваются, так что при развертывании беспроводной локальной сети можно учитывать особенности регулирования спектра частот конкретной страны. Так, в США в диапазоне 2,4 ГГц может быть до 79 каналов, причем максимальное время нахождения на каждом канале не должно превышать 400 мс.
- Третий вариант, в котором используется тот же *микроволновый диапазон*, основан на методе DSSS, где в качестве последовательности чипов применяется 11-битный код 10110111000. Каждый бит кодируется путем двоичной фазовой (1 Мбит/с) или квадратурной фазовой (2 Мбит/с) манипуляции.

РАЗВИТИЕ СТАНДАРТА IEEE 802.11

В 1999 году были приняты еще два варианта физического уровня: **802.11a** и **802.11b.**

- *Спецификация 802.11a* обеспечивает повышение скорости за счет более высокого диапазона частот (5 ГГц). Для этого задействуются 300 МГц из этого диапазона, ортогональное частотное мультиплексирование (OFDM) и прямая коррекция ошибок (FEC). Скорости передачи данных составляют 6, 9, 12, 18, 24, 36, 48 и 54 Мбит/с. Однако его использование связано с двумя проблемами. Во-первых, оборудование для этих частот пока еще слишком дорогое, во-вторых, в некоторых странах частоты этого диапазона подлежат лицензированию.
- В *спецификации 802.11b института IEEE* по-прежнему используется диапазон 2,4 ГГц, что позволяет задействовать более дешевое оборудование. Для повышения скорости до 11 Мбит/с, которая сопоставима со скоростью классического стандарта Ethernet, здесь применяется более эффективный метод DSSS, использующий технику Complementary Code Keying (CCK).

Еще один стандарт для физического уровня разработан группой **802.11g** института IEEE летом 2003 года.

- В нем задействован диапазон 2,4 ГГц, но со скоростью передачи данных до 54 Мбит/с. В этой спецификации используется ортогональное частотное мультиплексирование (OFDM).

СТАНДАРТЫ IEEE

В стандарте IEEE 802.11b благодаря высокой скорости передачи данных (до 11 Мбит/с), практически эквивалентной пропускной способности обычных проводных локальных сетей Ethernet, а также ориентации на диапазон 2,4 ГГц, этот стандарт завоевал наибольшую популярность у производителей оборудования для беспроводных сетей.

- Оборудование, работающее на максимальной скорости 11 Мбит/с, имеет меньший радиус действия, чем на более низких скоростях, стандартом 802.11b предусмотрено автоматическое снижение скорости при ухудшении качества сигнала.

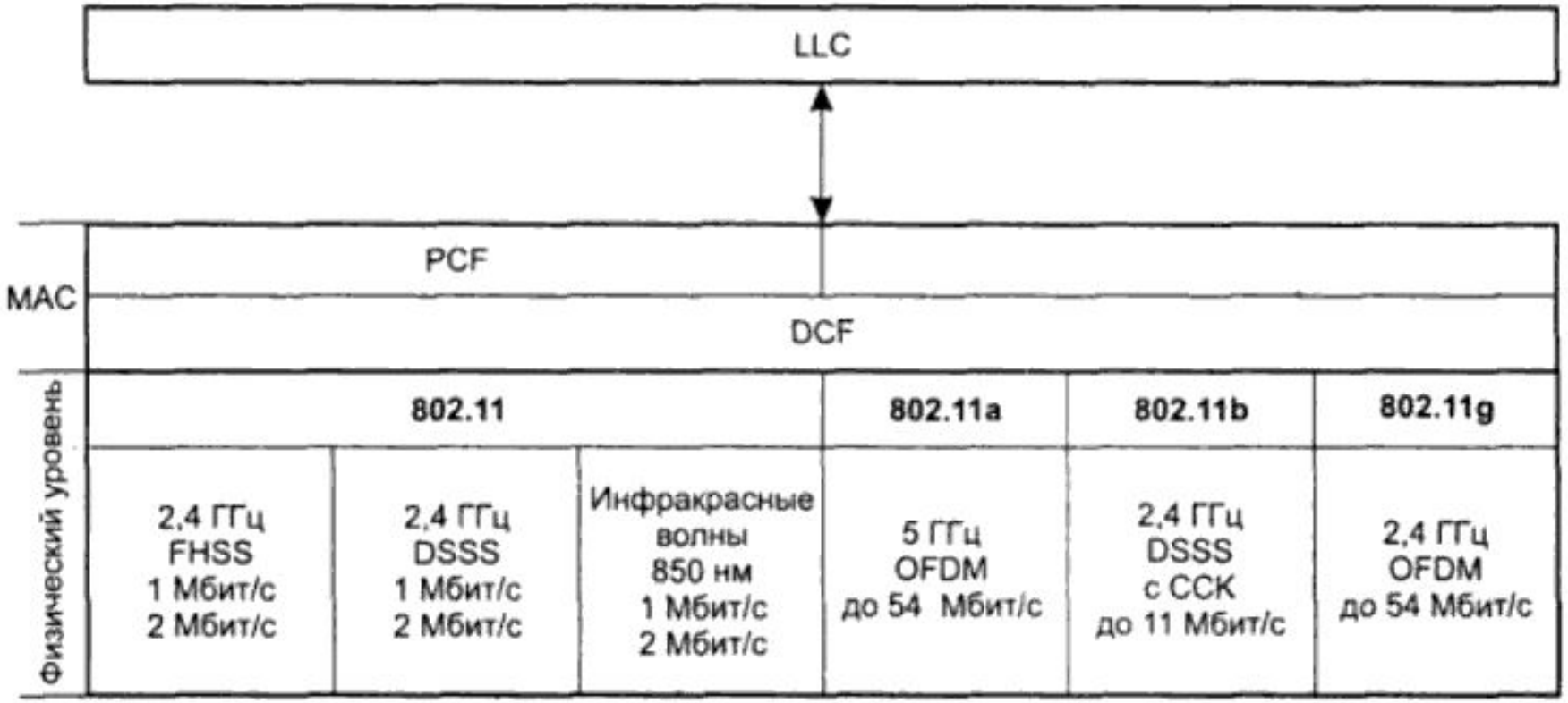
Стандарт IEEE 802.11a имеет большую ширину полосы из семейства стандартов 802.11 при скорости передачи данных до 54 Мбит/с.

- В отличие от базового стандарта, ориентированного на область частот 2,4 ГГц, спецификациями 802.11a предусмотрена работа в диапазоне **5 ГГц**. В качестве метода модуляции сигнала выбрано ортогональное частотное мультиплексирование (OFDM).
- К недостаткам 802.11a относятся более высокая потребляемая мощность радиопередатчиков для частот 5 ГГц, а также меньший радиус действия.

Стандарт IEEE 802.11g является логическим развитием 802.11b и предполагает передачу данных в том же частотном диапазоне. Кроме того, стандарт 802.11g полностью совместим с 802.11b, то есть любое устройство 802.11g должно поддерживать работу с устройствами 802.11b. Максимальная скорость передачи в стандарте 802.11g составляет 54 Мбит/с, поэтому на сегодня это наиболее перспективный стандарт беспроводной связи.

- При разработке стандарта 802.11g рассматривались две отчасти конкурирующие технологии: метод ортогонального частотного разделения OFDM и метод двоичного пакетного сверточного кодирования PBCC, опционально реализованный в стандарте 802.11b. В результате стандарт 802.11g содержит компромиссное решение: в качестве базовых применяются технологии OFDM и CCK, а опционально предусмотрено использование технологии PBCC.

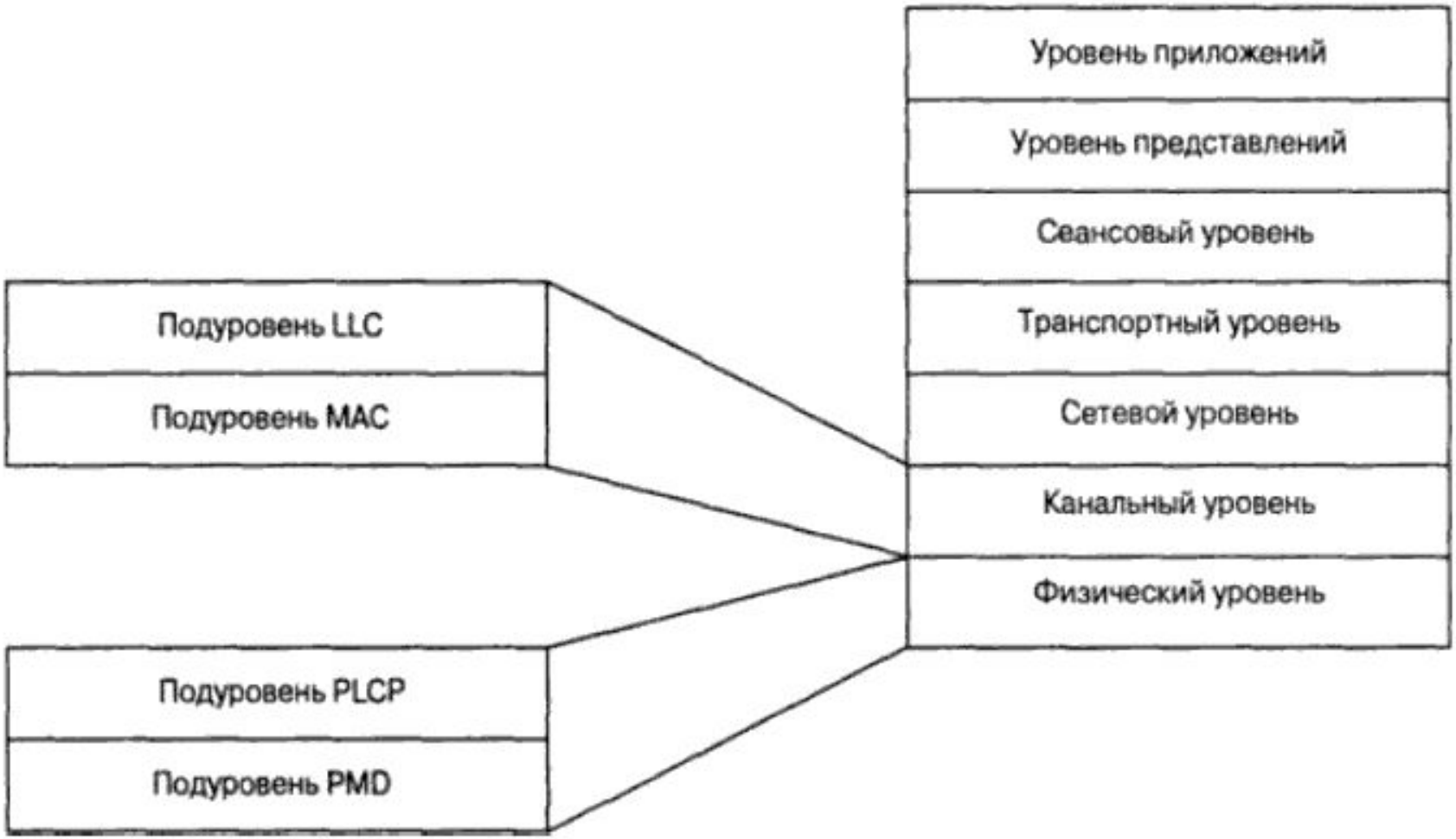
СТЕК ПРОТОКОЛОВ IEEE 802.11



ФИЗИЧЕСКИЙ УРОВЕНЬ

- Основное назначение физических уровней стандарта 802.11 - обеспечить механизмы беспроводной передачи для подуровня MAC, а также поддерживать выполнение вторичных функций, таких как оценка состояния беспроводной среды и сообщение о нем подуровню MAC.
- Уровни MAC и PHY разрабатывались так, чтобы они были независимыми. Независимость между MAC и подуровнем PHY и позволила использовать дополнительные высокоскоростные физические уровни, описанные в стандартах 802.11b, 802.11a и 802.11g.
- Каждый из физических уровней стандарта 802.11 имеет два подуровня:
  - Physical Layer Convergence Procedure (PLCP). Процедура определения состояния физического уровня.
  - Physical Medium Dependent (PMD). Подуровень физического уровня, зависящий от среды передачи.

ПОДУРОВНИ УРОВНЯ PHY



ФИЗИЧЕСКИЙ УРОВЕНЬ

- Подуровень PLCP является уровнем обеспечения взаимодействия, на котором осуществляется перемещение элементов данных протокола MAC (MAC Protocol Data Units - MPDU) между MAC-станциями с использованием подуровня PMD, на котором реализуется тот или иной метод передачи и приема данных через беспроводную среду.
- Подуровни PLCP и PMD отличаются для разных вариантов стандарта 802.11.

УРОВЕНЬ MAC

- Уровень MAC выполняет в беспроводных сетях больше функций, чем в проводных сетях.
- Функции уровня MAC в стандарте 802.11 включают:
  - доступ к разделяемой среде;
  - обеспечение мобильности станций при наличии нескольких базовых станций;
  - обеспечение безопасности, эквивалентной безопасности проводных локальных сетей.

ТОПОЛОГИИ ЛОКАЛЬНЫХ СЕТЕЙ СТАНДАРТА 802.11

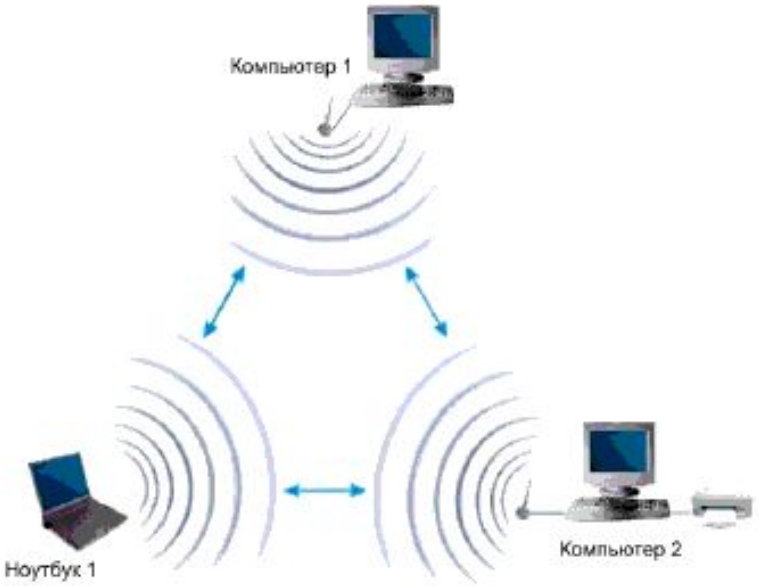
- Сеть с базовым набором услуг (Basic Service Set, BSS) образуется отдельными станциями, узлы взаимодействуют друг с другом непосредственно без базовой станции.
- Станции могут использовать разделяемую среду для того, чтобы передавать данные:
  - непосредственно друг другу в пределах одной BSS-сети;
  - в пределах одной BSS-сети транзитом через точку доступа;
  - между разными BSS-сетями через две точки доступа и распределенную систему;
  - между BSS-сетью и проводной локальной сетью через точку доступа, распределенную систему и портал.

ТОПОЛОГИИ ЛОКАЛЬНЫХ СЕТЕЙ СТАНДАРТА 802.11

- BSS-сети не являются традиционными сотами в отношении зон покрытия, они могут находиться друг от друга на значительном расстоянии, а могут частично или полностью перекрываться — стандарт 802.11 оставляет здесь свободу для проектировщика сети.
- В сетях, обладающих инфраструктурой, некоторые станции сети являются базовыми, или, в терминологии 802.11, **точками доступа** (Access Point, AP).
- Станция, которая выполняет функции AP, является членом какой-нибудь BSS-сети.
- Все базовые станции сети связаны между собой с помощью распределенной системы (Distribution System, DS), в качестве которой может использоваться та же среда (то есть радио- или инфракрасные волны), что и для взаимодействия между станциями, или же отличная от нее, например проводная.
- Точки доступа вместе с распределенной системой поддерживают **службу распределенной системы** (Distribution System Service, DSS). Задача DSS - передача пакетов между станциями, которые не могут взаимодействовать между собой непосредственно.

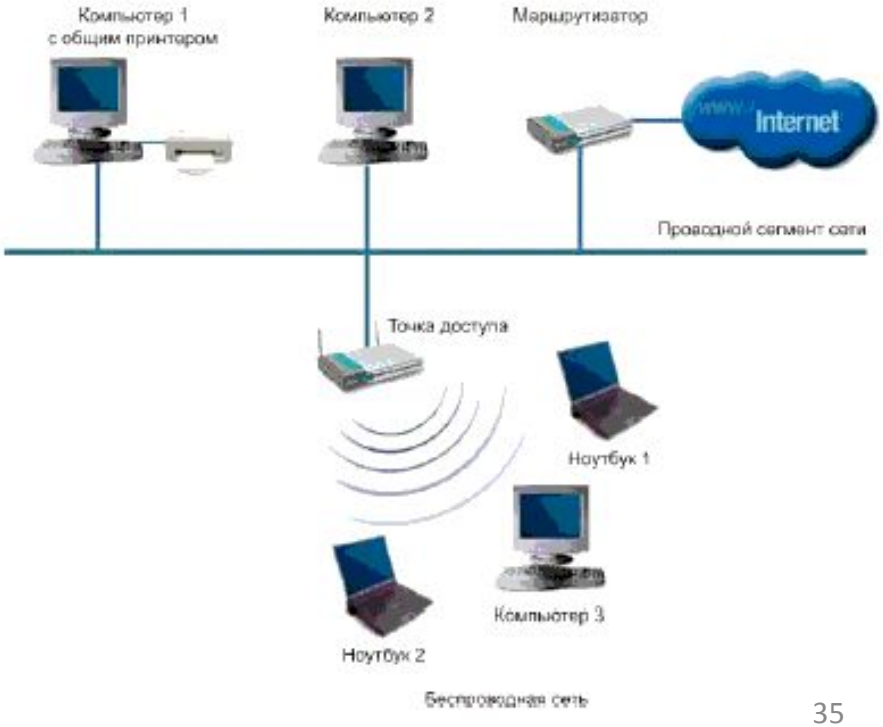
РЕЖИМ РАБОТЫ AD HOC

- В режиме Ad Hoc клиенты устанавливают связь непосредственно друг с другом. Устанавливается одноранговое взаимодействие по типу "точка-точка", и компьютеры взаимодействуют напрямую без применения точек доступа.
- Режим Ad Hoc позволяет устанавливать соединение на скорости не более 11 Мбит/с, независимо от используемого оборудования. Реальная скорость обмена данными будет ниже и составит не более 11/N Мбит/с, где N - число устройств в сети.



ИНФРАСТРУКТУРНЫЙ РЕЖИМ

- В инфраструктурном режиме точки доступа обеспечивают связь клиентских компьютеров, являясь функционально, как беспроводной коммутатор.
- Клиентские станции не связываются непосредственно одна с другой, а связываются с точкой доступа, и она уже направляет пакеты адресатам



РАСПРЕДЕЛЕННЫЙ РЕЖИМ ДОСТУПА DCF

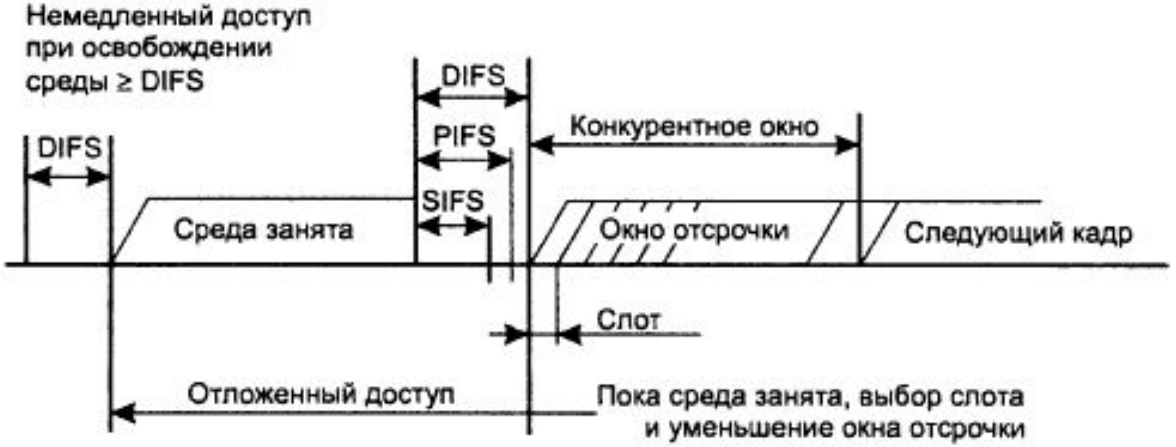
- В сетях 802.11 уровень MAC обеспечивает два режима доступа к разделяемой среде:
  - **распределенный режим DCF** (Distributed Coordination Function);
  - **централизованный режим PCF** (Point Coordination Function).
- В беспроводных сетях прямого распознавания используется косвенное выявление коллизий.
- Для этого каждый переданный кадр должен подтверждаться кадром положительной квитанции, посылаемым станцией назначения.
- Если по истечении оговоренного тайм-аута квитанция не поступает, станция-отправитель считает, что произошла коллизия.
- Режим доступа DCF требует синхронизации станций. В спецификации 802.11 эта проблема решается следующим образом — временные интервалы начинают отсчитываться от момента окончания передачи очередного кадра.
- Это не требует передачи каких-либо специальных синхронизирующих сигналов и не ограничивает размер пакета размером слота, так как слоты принимаются во внимание только при принятии решения о начале передачи кадра.

ЦЕНТРАЛИЗОВАННЫЙ РЕЖИМ ДОСТУПА PCF

- В том случае, когда в BSS-сети имеется станция, выполняющая функции точки доступа, может применяться также централизованный режим доступа PCF, обеспечивающий приоритетное обслуживание трафика.
- В этом случае точка доступа играет роль арбитра среды.
- Режим доступа PCF в сетях 802.11 сосуществует с режимом DCF. Оба режима координируются с помощью трех типов межкадровых интервалов.
- После освобождения среды каждая станция отсчитывает время простоя среды, сравнивая его с тремя значениями:
  - короткий межкадровый интервал (Short IFS, **SIFS);**
  - межкадровый интервал режима PCF **(PIFS);**
  - межкадровый интервал режима DCF **(DIFS).**

СОВМЕСТНАЯ РАБОТА РЕЖИМОВ PCF И DCF

- Захват среды с помощью распределенной процедуры DCF возможен только в том случае, когда среда свободна в течение времени, равного или большего, чем DIFS. То есть в качестве IFS в режиме DCF нужно использовать интервал DIFS — самый длительный период из трех возможных, что дает этому режиму самый низкий приоритет.
- Межкадровый интервал SIFS имеет наименьшее значение, он служит для первоочередного захвата среды ответными CTS-кадрами или квитанциями, которые продолжают или завершают уже начавшуюся передачу кадра.
- Значение межкадрового интервала PIFS больше, чем SIFS, но меньше, чем DIFS. Промежутком времени между завершением PIFS и DIFS пользуется арбитр среды. В этом промежутке он может передать специальный кадр, который говорит всем станциям, что начинается **контролируемый период**. Получив этот кадр, станции, которые хотели бы воспользоваться алгоритмом DCF для захвата среды, уже не могут этого сделать, они должны дожидаться окончания контролируемого периода.



УПРАВЛЯЕМЫЙ ПЕРИОД

- На управляемом интервале реализуется *централизованный метод* доступа PCF.
  - Арбитр выполняет процедуру опроса, чтобы по очереди предоставить каждой такой станции право на использование среды, направляя ей специальный кадр.
- Станция, получив такой кадр, может ответить другим кадром, который подтверждает прием специального кадра и одновременно передает данные (либо по адресу арбитра для транзитной передачи, либо непосредственно станции).
- Для того чтобы какая-то доля среды всегда доставалась асинхронному трафику, длительность контролируемого периода ограничена.
- После его окончания арбитр передает соответствующий кадр и начинается неконтролируемый период.
- Каждая станция может работать в режиме PCF, для этого она должна подписаться на эту услугу при присоединении к сети.

БЕЗОПАСНОСТЬ

- В стандарте 802.11 предусмотрены средства безопасности, которые повышают защищенность беспроводной локальной сети до уровня обычной проводной локальной сети.
- Основной протокол защиты данных в сетях 802.11 называется — **WEP** (Wired Equivalent Privacy — секретность, эквивалентная проводной).
- Протокол использует **шифрование данных**, передаваемых через беспроводную среду, и тем самым обеспечивает их конфиденциальность.
- Технология 802.11 предлагает механизм безопасности — **механизм аутентификации** — доказательство легальности пользователя, подключающегося к сети.

МЕХАНИЗМ ШИФРОВАНИЯ WEP

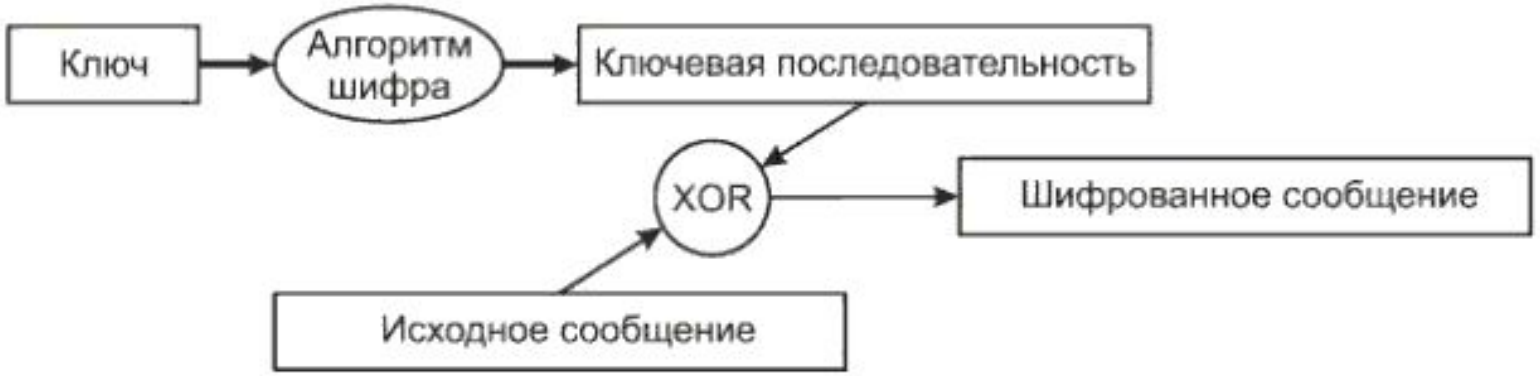
- Шифрование WEP основано на алгоритме RC4 (код Ривеста), который представляет собой симметричное потоковое шифрование.
- Ядро алгоритма состоит из функции генерации ключевого потока.
  - Эта функция генерирует последовательность битов, которая затем объединяется с открытым текстом посредством суммирования по модулю два.
  - Дешифрование состоит из регенерации этого ключевого потока и суммирования его с шифрограммой по модулю два для восстановления исходного текста.
  - Другая главная часть алгоритма - функция инициализации, которая использует ключ переменной длины для создания начального состояния генератора ключевого потока.

ОСОБЕННОСТИ WEP-ПРОТОКОЛА

- Достаточно устойчив к атакам, связанным с простым перебором ключей шифрования, что обеспечивается необходимой длиной ключа и частотой смены ключей и инициализирующего вектора;
- Самосинхронизация для каждого сообщения. Это свойство является ключевым для протоколов уровня доступа к среде передачи, где велико число искаженных и потерянных пакетов;
- Эффективность и простота реализации;
- Открытость;
- Использование WEP-шифрования не является обязательным в сетях стандарта IEEE 802.11.

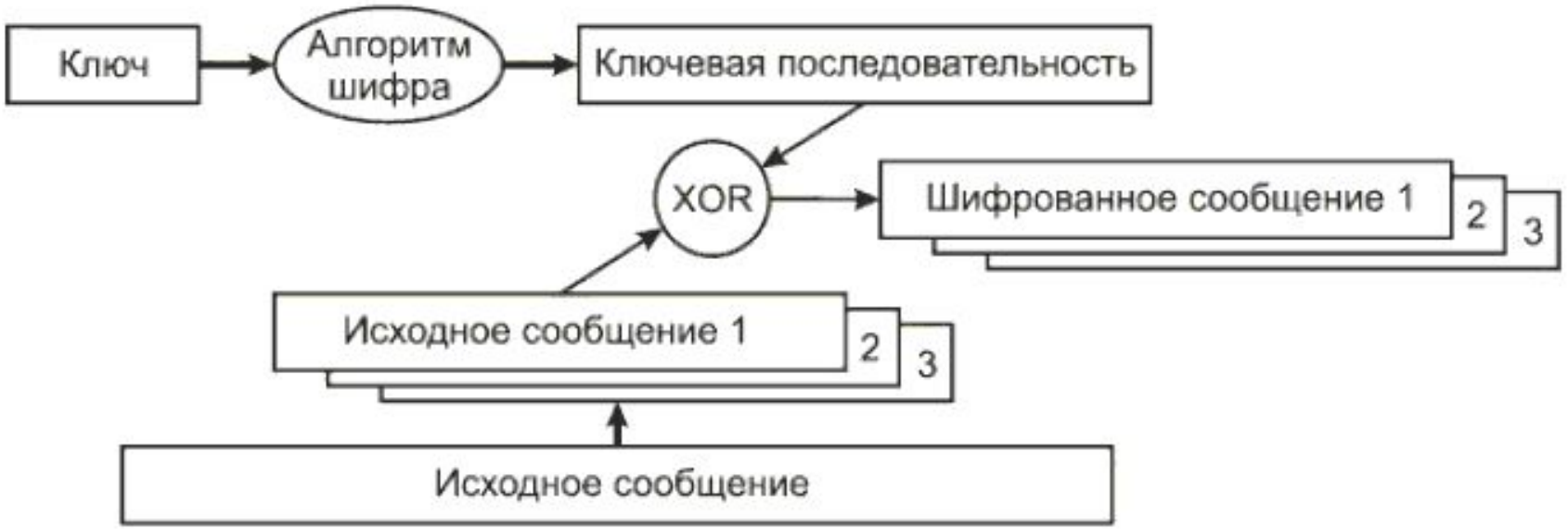
ПОТОКОВОЕ ШИФРОВАНИЕ

- При потоковом шифровании выполняется побитовое сложение по модулю 2 (функция "исключающее ИЛИ", XOR) ключевой последовательности, генерируемой алгоритмом шифрования на основе заранее заданного ключа, и исходного сообщения.
- Ключевая последовательность имеет длину, соответствующую длине исходного сообщения, подлежащего шифрованию



БЛОЧНОЕ ШИФРОВАНИЕ

- Блочное шифрование работает с блоками заранее определенной длины, не меняющимися в процессе шифрования.
- Исходное сообщение фрагментируется на блоки, и функция XOR вычисляется над ключевой последовательностью и каждым блоком.
- Размер блока фиксирован, а последний фрагмент исходного сообщения дополняется пустыми символами до длины нормального блока

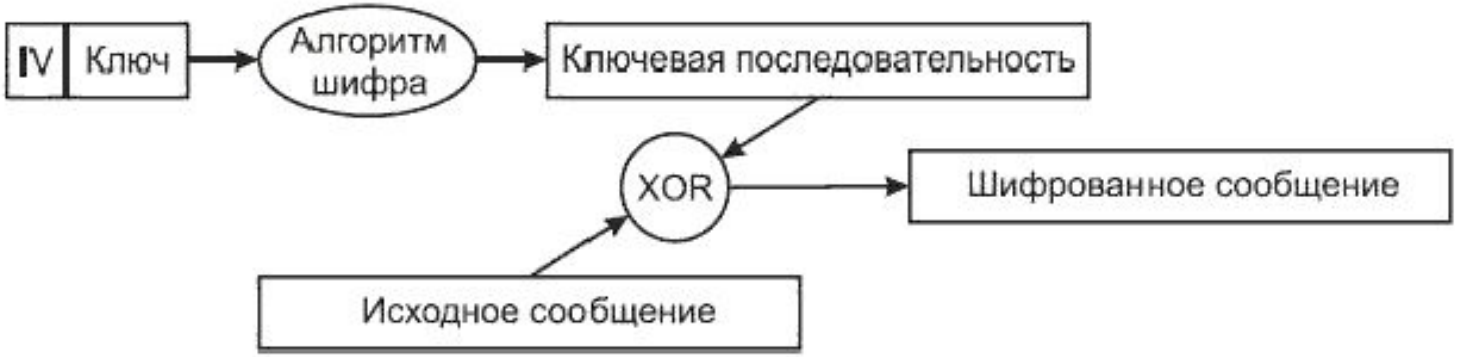


НЕДОСТАТКИ МЕТОДА

- Потоковое шифрование и блочное шифрование используют метод электронной кодовой книги (ECB).
- Метод ECB характеризуется тем, что одно и то же исходное сообщение на входе всегда порождает одно и то же зашифрованное сообщение на выходе.
- Это потенциальная брешь в системе безопасности.
- Для устранения указанной проблемы используют:
  - **Векторы инициализации** (Initialization Vectors - IVs).
  - **Обратную связь** (feedback modes).
- До начала процесса шифрования 40- или 104-битный секретный ключ распределяется между всеми станциями, входящими в беспроводную сеть.
- К секретному ключу добавляется вектор инициализации (IV).

ВЕКТОР ИНИЦИАЛИЗАЦИИ (IV)

- Вектор инициализации используется для модификации ключевой последовательности.
- При использовании вектора инициализации ключевая последовательность генерируется алгоритмом шифрования, на вход которого подается секретный ключ, совмещенный с IV.
- При изменении вектора инициализации ключевая последовательность также меняется.



АЛГОРИТМ ШИФРОВАНИЯ WEP

- Вектор инициализации имеет длину 24 бита и совмещается с 40- или 104-битовым базовым ключом шифрования WEP таким образом, что на вход алгоритма шифрования подается 64- или 128-битовый ключ.
- Вектор инициализации присутствует в нешифрованном виде в заголовке фрейма в радиоканале, с тем чтобы принимающая сторона могла успешно декодировать этот фрейм.
- Несмотря на то, что обычно говорят об использовании шифрования WEP с ключами длиной 64 или 128 битов, эффективная длина ключа составляет лишь 40 или 104 бита по причине передачи вектора инициализации в нешифрованном виде.
  - При настройках шифрования в оборудовании при 40-битном эффективном ключе вводятся 5 байтовых ASCII-символов или 10 шестнадцатеричных чисел, и при 104-битном эффективном ключе вводятся 13 байтовых ASCII-символов или 26 шестнадцатеричных чисел.

ПОВЫШЕННАЯ БЕЗОПАСНОСТЬ

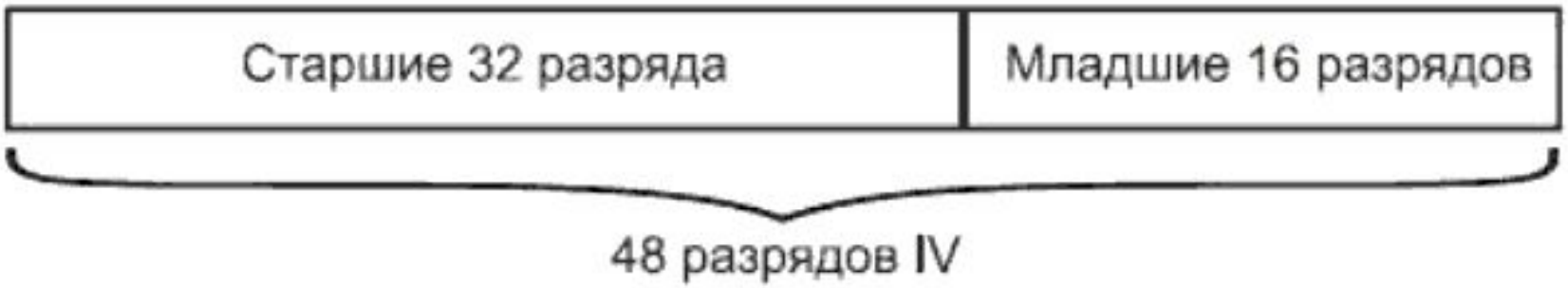
- **Стандарт сети 802.11i с повышенной безопасностью (WPA2)**
  - Стандарт WPA основан на алгоритме шифрования RC4 и протоколе TKIP.
  - В июне 2004 г. IEEE ратифицировал давно ожидаемый стандарт обеспечения безопасности в беспроводных локальных сетях - 802.11i.
  - Стандарт 802.11i, также известный как WPA2 и выпущенный Wi-Fi Alliance.
  - Стандарт 802.11i использует концепцию повышенной безопасности (Robust Security Network - RSN), предусматривающую, что беспроводные устройства должны обеспечивать дополнительные возможности.
  - Это потребует изменений в аппаратной части и программном обеспечении, т.е. сеть, полностью соответствующая RSN, станет несовместимой с существующим оборудованием WEP.

СПЕЦИФИКАЦИЯ WPA

- Стандарт безопасности WPA обеспечивает уровень безопасности более, чем может предложить WEP.
- IEEE предложила временный протокол целостности ключа(Temporal Key Integrity Protocol, TKIP).
- Основные усовершенствования, внесенные протоколом TKIP:
  - Пофреймовое изменение ключей шифрования. WEP-ключ быстро изменяется, и для каждого фрейма он другой;
  - Контроль целостности сообщения. Обеспечивается эффективный контроль целостности фреймов данных с целью предотвращения скрытых манипуляций с фреймами и воспроизведения фреймов;
  - Усовершенствованный механизм управления ключами.

ПОФРЕЙМОВОЕ ИЗМЕНЕНИЕ КЛЮЧЕЙ ШИФРОВАНИЯ

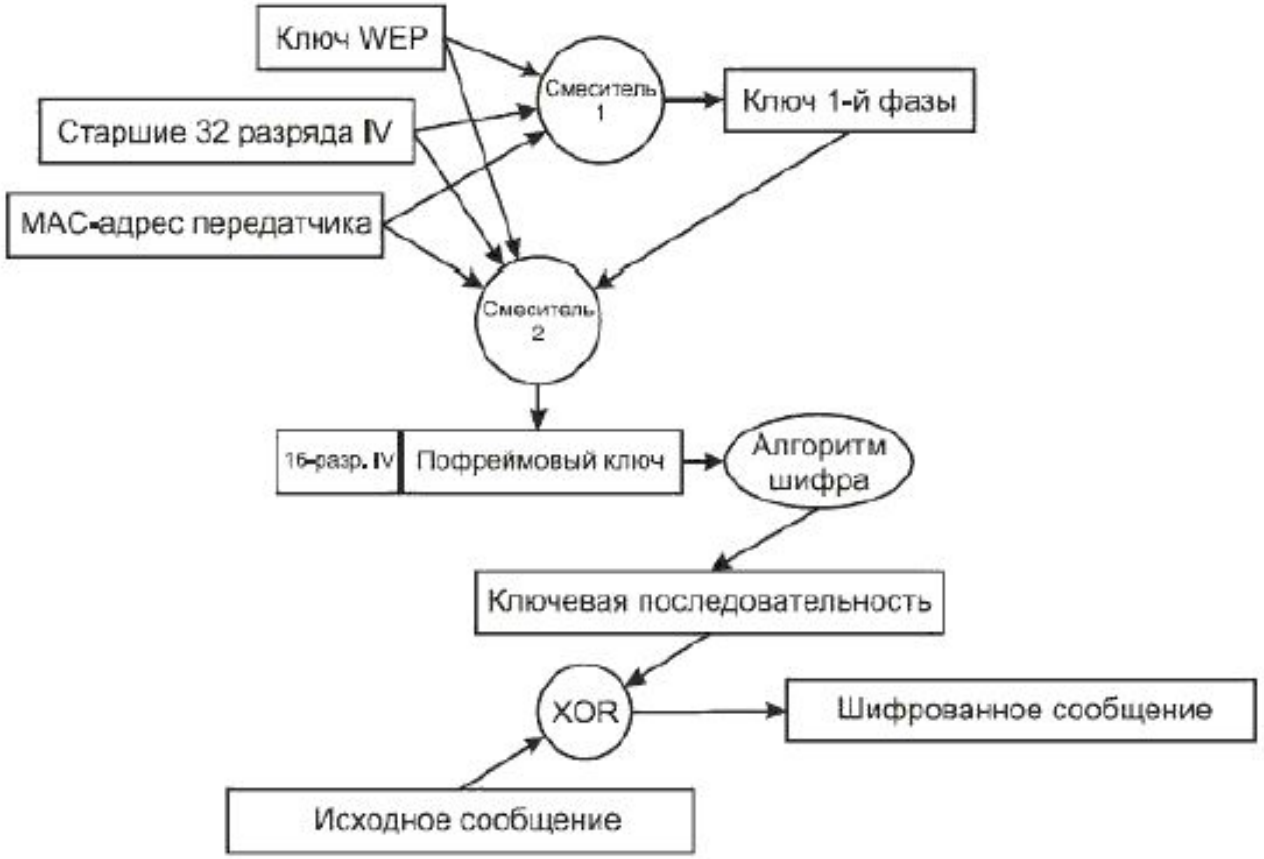
- Основной принцип, на котором основано пофреймовое изменение ключа, состоит в том, что IV, MAC-адрес передатчика и WEP-ключ обрабатываются вместе с помощью двухступенчатой функции перемешивания.
- Результат применения этой функции соответствует стандартному 104-разрядному WEP-ключу и 24-разрядному IV.
- IEEE предложила также увеличить 24-разрядный вектор инициализации до 48-разрядного IV.



ПРОЦЕСС ПОФРЕЙМОВОГО ИЗМЕНЕНИЯ КЛЮЧА

- Процесс пофреймового изменения ключа можно разбить на следующие этапы:
  - Базовый WEP-ключ перемешивается со старшими 32 разрядами 48-разрядного IV (32-разрядные числа могут принимать значения 0-4 294 967 295) и MAC-адресом передатчика. Результат этого действия называется **ключ 1-й фазы**. Этот процесс позволяет занести ключ 1-й фазы в кэш и также напрямую поместить в ключ.
  - Ключ 1-й фазы снова перемешивается с IV и MAC-адресом передатчика для выработки значения пофреймового ключа.
  - Вектор инициализации (IV), используемый для передачи фрейма, имеет размер только 16 бит (16-разрядные числа могут принимать значения 0-65 535). Оставшиеся 8 бит (в стандартном 24-битовом IV) представляют собой фиксированное значение, используемое как заполнитель.
  - Пофреймовый ключ применяется для WEP-шифрования фрейма данных.
  - Когда 16-битовое пространство IV оказывается исчерпанным, ключ 1-й фазы отбрасывается и 32 старших разряда увеличиваются на 1.
  - Значение пофреймового ключа вычисляется заново, как на этапе 2.

ПРОЦЕСС СОЗДАНИЯ ШИФРОВАННОГО СООБЩЕНИЯ В WPA



КОНТРОЛЬ ЦЕЛОСТНОСТИ СООБЩЕНИЯ

- Для усиления малоэффективного механизма, основанного на использовании контрольного признака целостности (ICV) стандарта 802.11, применяется контроль целостности сообщения (MIC).
- MIC имеет уникальный ключ, который отличается от ключа, используемого для шифрования фреймов данных.
- Этот уникальный ключ перемешивается с назначенным MAC-адресом и исходным MAC-адресом фрейма, а также со всей незашифрованной частью фрейма.

МЕХАНИЗМ ШИФРОВАНИЯ TKIP

- С помощью алгоритма пофреймового назначения ключей генерируется пофреймовый ключ.
- Алгоритм MIC генерирует MIC для фрейма в целом.
- Фрейм фрагментируется в соответствии с установками MAC относительно фрагментации.
- Фрагменты фрейма шифруются с помощью пофреймового ключа.
- Осуществляется передача зашифрованных фрагментов.

ПЕРСОНАЛЬНЫЕ СЕТИ И ТЕХНОЛОГИЯ BLUETOOTH

- Персональные сети должны обеспечивать как фиксированный доступ, так и мобильный.
- Персональные сети во многом похожи на локальные, но у них есть и свои особенности:
  - Многие из устройств, которые могут входить в персональную сеть, *гораздо проще*, чем традиционный узел LAN — компьютер. Кроме того, такие устройства обычно имеют небольшие габариты и стоимость.
  - *Область покрытия PAN меньше области покрытия LAN*, для взаимодействия узлов PAN часто достаточно нескольких метров.
  - *Высокие требования к безопасности.* Протоколы PAN должны обеспечивать разнообразные методы аутентификации устройств и шифрования данных в мобильной обстановке.
  - Персональные сети в гораздо большей степени *тяготеют к беспроводным решениям*, чем локальные.
  - Если человек носит PAN-устройство постоянно с собой и на себе, то оно не должно причинять вред его здоровью. Поэтому такое устройство должно *излучать сигналы небольшой мощности*, желательно не более 100 мВт (обычный сотовый телефон излучает сигналы мощностью от 600 мВт до 3 Вт).
- Сегодня самой популярной технологией PAN является **Bluetooth**, которая обеспечивает взаимодействие 8 устройств в разделяемой среде диапазона 2,4 ГГц со скоростью передачи данных до 723 Кбит/с.

АРХИТЕКТУРА BLUETOOTH

- Стандарт Bluetooth разработан группой Bluetooth SIG (Bluetooth Special Interest Group), которая была организована по инициативе компании Ericsson.
  - Стандарт Bluetooth также адаптирован рабочей группой IEEE 802.15.1 в соответствии с общей структурой стандартов IEEE 802.
- В технологии Bluetooth используется концепция **пикосети.** Название подчеркивает небольшую область покрытия, от 10 до 100 м, в зависимости от мощности излучения передатчика устройства.
  - В пикосеть может входить до 255 устройств, но только 8 из них могут в каждый момент времени быть активными и обмениваться данными. Одно из устройств в пикосети является **главным**, остальные — **подчиненными**.
  - Активное подчиненное устройство может обмениваться данными только с главным устройством, прямой обмен между подчиненными устройствами невозможен. Все подчиненные устройства данной пикосети, кроме семи активных, должны находится в режиме пониженного энергопотребления, в котором они только периодически прослушивают команду главного устройства для перехода в активное состояние.

АРХИТЕКТУРА BLUETOOTH (ПРОДОЛЖЕНИЕ)

- Главное устройство отвечает за доступ к *разделяемой среде пикосети*, которая представляет собой нелицензируемые частоты диапазона 2,4 ГГц.
- Разделяемая среда передает данные со скоростью 1 Мбит/с, но из-за накладных расходов на заголовки пакетов и смену частот полезная скорость передачи данных в среде не превышает 777 Кбит/с.
  - Пропускная способность среды делится главным устройством между семью подчиненными устройствами на основе техники TDM.
- Такая архитектура позволяет применять более простые протоколы в устройствах, выполняющих функции подчиненных (например, в радионаушниках), и отдает более сложные функции управления пикосетью компьютеру, который, скорее всего, будет главным устройством этой сети.

АУТЕНТИФИКАЦИЯ В СЕТИ BLUETOOTH

- Присоединение к пикосети происходит динамически.
  - Главное устройство пикосети, используя процедуру опроса, собирает информацию об устройствах, которые попадают в зону его пикосети.
  - После обнаружения нового устройства главное устройство проводит с ним переговоры.
  - Если желание подчиненного устройства присоединиться к пикосети совпадает с решением главного устройства (подчиненное устройство прошло проверку аутентичности и оказалось в списке разрешенных устройств), то новое подчиненное устройство присоединяется к сети.
- Безопасность сетей Bluetooth обеспечинается за счет аутентификации устройств и шифрования передаваемого трафика.
- Протоколы Bluetooth обеспечивают более высокий уровень защиты, чем протокол WEP стандарта IEEE 802.11.

ОБЕСПЕЧЕНИЕ ПОМЕХОЗАЩИЩЕННОСТИ

Для того чтобы сигналы разных пикосетей не интерферировали, каждое главное устройство использует *собственную* последовательность **псевдослучайной перестройки частоты**.

Использование отличающихся последовательностей псевдослучайной перестройки частоты затрудняет общение пикосетей между собой. Для преодоления этой проблемы устройство, играющее роль моста, должно при подключении к каждой из пикосетей соответствующим образом менять частоту.

Коллизии, хотя и с очень небольшой вероятностью, все же могут происходить, когда два или более устройства из разных пикосетей выберут для работы один и тот же частотный канал.

Рассредоточенная сеть реализует метод доступа CDMA на основе техники FHSS. Для надежной передачи данных в технологии Bluetooth может выполняться прямая коррекция ошибок FEC, а получение кадра подтверждается с помощью квитанций.

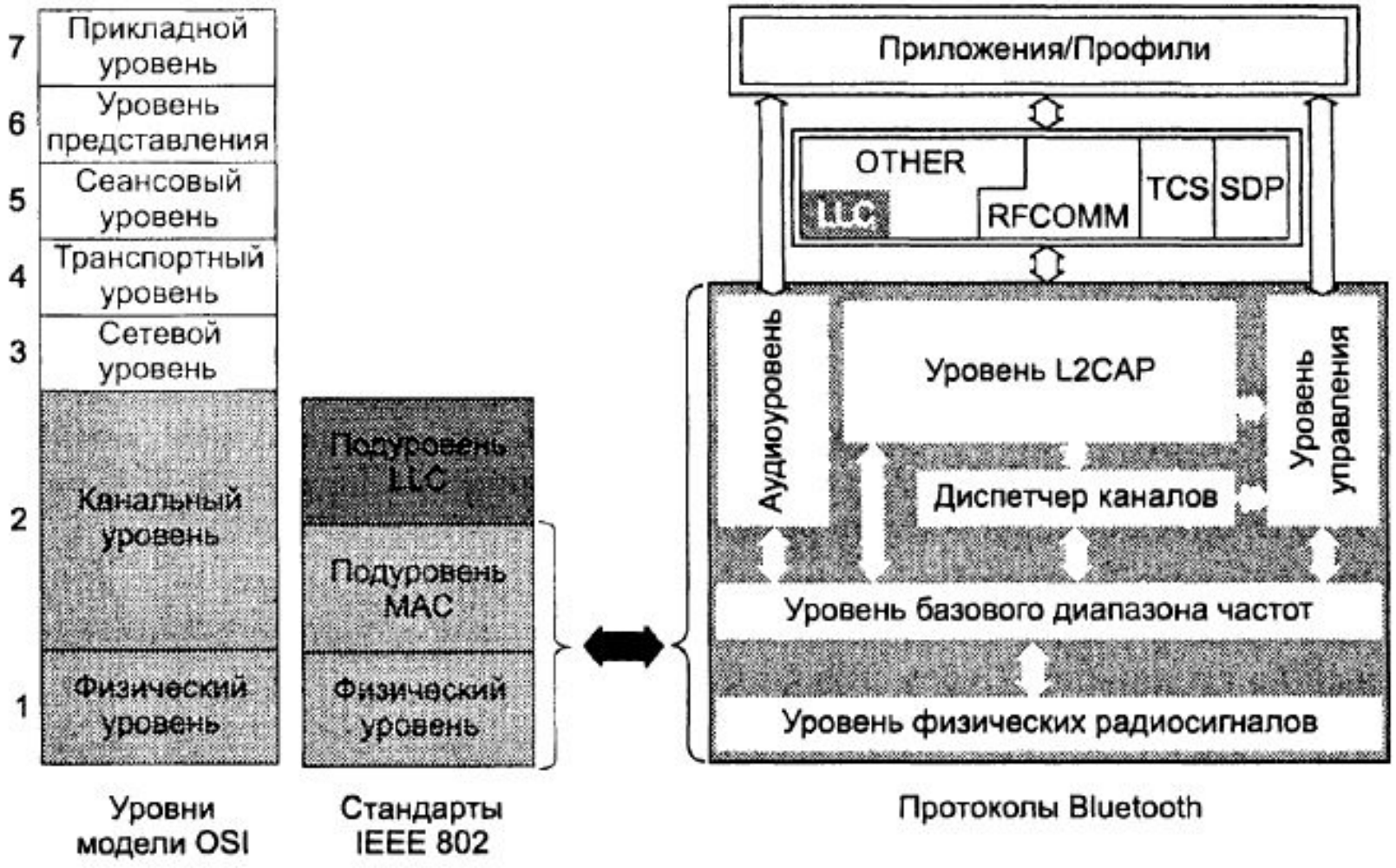
МЕТОДЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

- Сети Bluetooth используют разные методы для передачи информации двух типов.
  - Для *чувствительного к задержкам трафика* (например, голоса) сеть поддерживает **синхронный канал, ориентированный на соединение** (Synchronous Connection-Oriented link, SCO), работающий со скоростью 64 Кбит/с, Для канала SCO пропускная способность резервируется на все время соединения.
  - Для *эластичного трафика* (например, компьютерных данных) используется работающий с переменной скоростью **асинхронный канал, не ориентированный на соединение** (Asynchronous Connection-Less link, ACL). Для канала ACL пропускная способность выделяется по запросу подчиненного устройства или по потребности главного устройства.

СТЕК ПРОТОКОЛОВ BLUETOOTH

- Bluetooth является законченной оригинальной технологией, рассчитанной на самостоятельное применение в электронных персональных устройствах.
- Данная технология поддерживает полный стек протоколов, включая собственные прикладные протоколы.
  - При приведении стандартов Bluetooth в соответствие к архитектуре стандартов IEEE 802 рабочая группа 802.15.1 ограничилась только так называемыми протоколами *ядра Bluetooth*, которые соответствуют функциям физического уровня и уровня MAC.

СООТВЕТСТВИЕ ПРОТОКОЛОВ BLUETOOTH МОДЕЛИ OSI И СТАНДАРТАМ IEEE 802



УРОВНИ ПРОТОКОЛОВ ЯДРА BLUETOOTH

- **Уровень физических радиосигналов** описывает частоты и мощности сигналов, используемых для передачи информации.
- **Уровень базового диапазона частот** отвечает за организацию каналов передачи данных в радиосреде. В его обязанности входят выбор последовательности псевдослучайной перестройку частоты, синхронизация устройств в пико-сети, формирование и передача кадров по установленным каналам SCO и ACL. Кадр Bluetooth имеет переменную длину, поле данных может содержать от 0 до 2744 бит (343 байт). Для передачи голоса используются кадры фиксированного размера с полем данных 240 бит (30 байт).
- **Диспетчер каналов** отвечает за аутентификацию устройств и шифрование трафика, а также управляет статусом устройств, то есть может сделать подчиненное устройство главным, и наоборот.

УРОВНИ ПРОТОКОЛОВ ЯДРА BLUETOOTH (ПРОДОЛЖЕНИЕ)

- **Уровень протокола адаптации для управления логическим каналом** (Logical Link Control Adaptation Layer, L2CAP) является верхним уровнем протоколов ядра Bluetooth.
  - Этот протокол используется только в тех случаях, когда устройство передает данные, голосовой трафик обходит этот протокол и обращается непосредственно к уровню базового диапазона частот.
  - Уровень L2CAP принимает от протоколов верхнего уровня сегменты данных размером до 64 Кбайт и делит их на небольшие кадры для уровня базового диапазона частот.
  - При приеме уровень L2CAP собирает кадры в исходный сегмент и передает протоколу верхнего уровня.
- **Аудиоуровень** обеспечивает передачу голоса по каналам SCO.
  - На этом уровне применяется импульсно-кодовая модуляция (PCM), что определяет скорость голосового канала в 64 Кбит/с.
- **Уровень управления** передает внешнему блоку информацию о состоянии соединений и принимает от внешнего блока команды, изменяющие конфигурацию и состояние соединений.

КАДРЫ BLUETOOTH

- Разделяемая среда представляет собой последовательность частотных каналов технологии FHSS в диапазоне 2,4 ГГц. Каждый частотный канал имеет ширину 1 МГц, количество каналов равно 79 (в США и большинстве других стран мира) или 23 (в Испании, Франции, Японии).
- Чиповая скорость равна 1600 Гц, поэтому период чипа составляет 625 мкс. Главное устройство разделяет общую среду на основе временного мультиплексирования (TDM), используя в качестве тайм-слота время пребывания системы на одном частотном канале, то есть 625 мкс.
- Информация кодируется с тактовой частотой 1 МГц путем двоичной частотной манипуляции (BFSK), в результате битовая скорость составляет 1 Мбит/с. В течение одного тайм-слота пикосеть Bluetooth передает 625 бит, но не все они используются для передачи полезной информации. При смене частоты устройствам сети требуется некоторое время для синхронизации, поэтому из 625 бит только 366 передают кадр данных.
- Кадр данных может занимать 1, 3 или 5 слотов. В том случае, когда кадр занимает больше одного слота, частота канала остается неизменной в течение всего времени передачи кадра. В этом случае накладные расходы на синхронизацию меньше, так что размер кадра, состоящего, например, из 5 последовательных слотов, равен 2870 бит (с полем данных до 2744 бит).

ФОРМАТ КАДРА BLUETOOTH

- Рассмотрим формат кадра, состоящего из одного слота — 366 бит:
  - **Поле данных** занимает 240 бит.
  - **Код доступа** (72 бита) используется для идентификации пикосети.
    - Каждое Bluetooth-устройство имеет глобально уникальный 6-байтовый адрес, поэтому для идентификации пикосети используется три младших байта уникального адреса главного устройства. Каждое устройство при формировании кадра помещает эти байты в поле кода доступа, дополняя их битами 1/3 для прямой коррекции ошибок (сокращение 1/3 говорит о том, что 1 бит информации преобразуется в 3 бита кода). Если главное или подчиненное устройство получает кадр, содержащий неверный код доступа, то оно отбрасывает этот кадр, считая, что он, скорее всего, получен из другой пикосети.
  - **Заголовок кадра** (54 бита) содержит MAC-адрес, однобитовой признак подтверждения приема кадра, тип кадра, а также ряд признаков. MAC-адрес состоит из трех битов, это временный адрес одного их семи подчиненных устройств, при этом адрес 000 является широковещательным. Информация заголовка также передается с помощью битов 1/3 алгоритма FEC.