Раздел 4. Лекция 4.

Последовательные интерфейсы RS-232, USB, IEEE 1394, IrDA, Bluetooth, WiFi, Thunderbolt. Часть 3

Основные вопросы лекции

1. Беспроводной интерфейс WiFi. Архитектура, принцип действия, характеристики. Стек протоколов. Перспективы развития.
2. Беспроводной интерфейс Bluetooth. Архитектура, принцип действия, характеристики. Стек протоколов. Перспективы развития.

1. Основные технологии беспроводной передачи данных

Способы беспроводной передачи информации между мобильными устройствами:

- инфракрасное соединение;
- соединение посредством радиоволн;
- соединение с помощью микроволновых (СВЧ) технологий.

Классификация **по дальности**:

1. Сектор локальных интерфейсов (короткодействующие технологии беспроводной передачи данных (*Bluetooth, WirelessUSB*).
2. Сектор локальных домашних и офисных сетей (среднедействующие технологии беспроводной передачи данных (*WiFi*).
3. Сектор региональных городских сетей (среднедействующие технологии беспроводной передачи данных (*WiMAX, Worldwide Interoperability for Microwave Access , IEEE 802.16, Mobile Broadband Wireless Access, MBWA, IEEE 802.20*)).
4. Сектор глобальных сетей (дальнедействующие технологии беспроводной передачи данных на базе радиорелейных, сотовых и спутниковых технологий).

1. Основные разновидности беспроводной передачи данных

- Персональные (wireless personal-area network, PAN);
- Временно создаваемые сети произвольной структуры;
  - ❑ локальные сети беспроводного доступа (wireless local-area network, LAN);
- Беспроводные наземные радиорелейные магистрали, беспроводная городская сеть (wireless metropolitan-area network, MAN);
  - ❑ сотовая сеть;
  - ❑ глобальная спутниковая сеть (wireless wide-area network, WAN).
- Гибридные гетерогенные сети разной конфигурации.

1. Тип. Сфера действия. Стандарты. Область применения

Персональная

- в непосредственной близости от пользователя;
- Bluetooth, IEEE 802.15, IRDA2;
- замена кабелей периферийных устройств.

Локальные

- в пределах зданий;
- IEEE 802.15, Wi-Fi, HiperLAN;
- мобильные расширения проводных сетей.

Региональные

- в пределах города;
- патентованные, IEEE 802.16, WIMAX;
- беспроводная связь между зданиями и предприятиями и Internet сети.

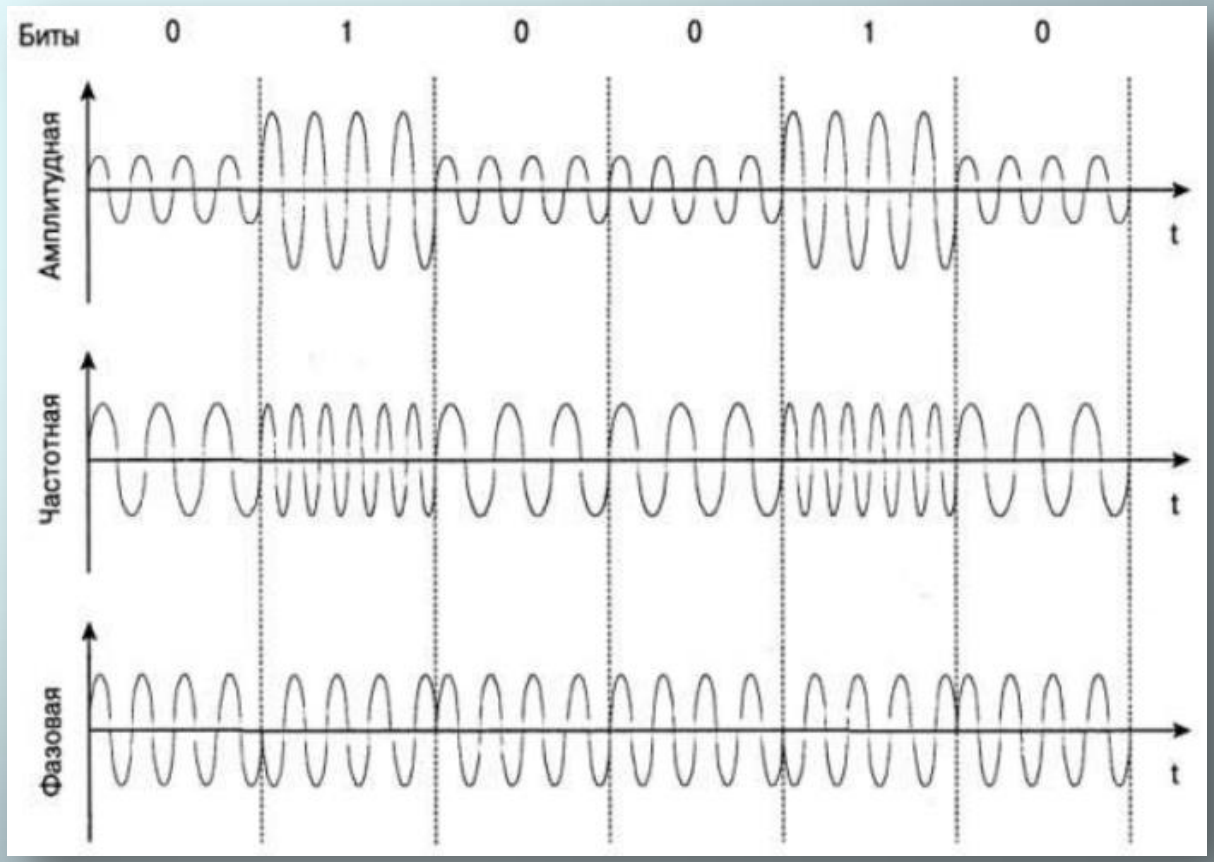
Глобальные

- по всему миру;
- стандарт CDPD (Cellular Digital Packet Data) цифровой пакетной передачи данных по сети сотовой связи и сотовые системы связи поколений 2, 2,5, 3, ...;
- мобильный доступ к Internet.

1. Сигналы для передачи информации

Аналоговые и цифровые:

- амплитудная модуляция (Amplitude-Shift Keying - ASK);
- частотная модуляция (Frequency-Shift Keying - FSK);
- фазовая модуляция (Phase-Shift Keying - PSK).



1. Методы доступа к среде в беспроводных сетях

Одна из основных проблем построения беспроводных систем – это решение задачи доступа многих пользователей к ограниченному ресурсу среды передачи. Существует несколько базовых методов доступа (их еще называют **методами уплотнения или мультиплексирования**), основанных **на разделении между станциями таких параметров, как пространство, время, частота и код**.

Задача уплотнения: выделить каждому каналу связи пространство, время, частоту и/или код с минимумом взаимных помех и максимальным использованием характеристик передающей среды.

1. Уплотнение с пространственным разделением

Основано на разделении сигналов в пространстве, когда передатчик посылает сигнал, используя код c, время t и частоту f области s_i. То есть **каждое беспроводное устройство может вести передачу данных только в границах определенной территории, на которой любому другому устройству запрещено передавать свои сообщения**.

К примеру, если радиостанция вещает на строго определенной частоте на закрепленной за ней территории, а какая-либо другая станция в этой же местности также начнет вещать на той же частоте, слушатели радиопередач не смогут получить «чистый» сигнал ни от одной из этих станций. Другое дело, если радиостанции работают на одной частоте в разных городах. Искажений сигналов каждой радиостанции не будет в связи с ограниченной дальностью распространения сигналов этих станций, что исключает их наложение друг на друга.

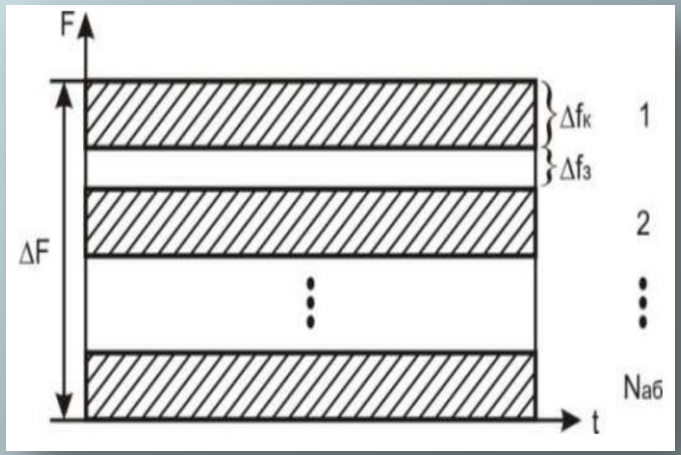
Характерный пример - системы сотовой телефонной связи.

1. Уплотнение с частотным разделением (Frequency Division Multiplexing - FDM)

Каждое устройство работает на определенной частоте, благодаря чему несколько устройств могут вести передачу данных на одной территории. Это один из наиболее известных методов, так или иначе используемый в самых современных системах беспроводной связи.

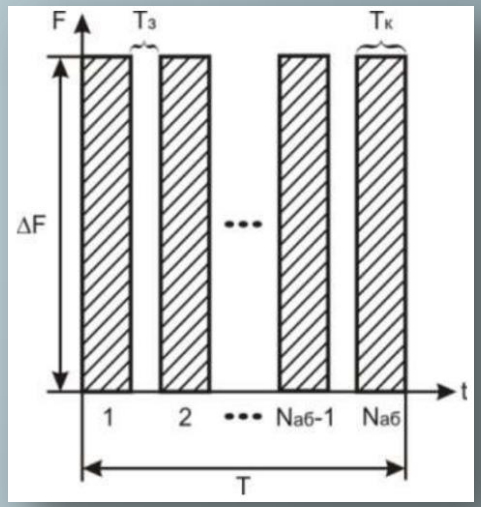
Пример схемы частотного уплотнения - функционирование в одном городе нескольких радиостанций, работающих на разных частотах. Для надежной отстройки друг от друга их рабочие частоты должны быть разделены защитным частотным интервалом, который позволяет исключить взаимные помехи.

Эта схема, хотя и позволяет использовать множество устройств на определенной территории, сама по себе приводит к неоправданному расточительству обычно скудных частотных ресурсов, поскольку требует выделения своей частоты для каждого беспроводного устройства.



1. Уплотнение с временным разделением (Time Division Multiplexing - TDM)

В данной схеме **распределение каналов идет по времени**, т. е. каждый передатчик транслирует сигнал на одной и той же частоте области s, но в различные промежутки времени (как правило, циклически повторяющиеся) при строгих требованиях к синхронизации процесса передачи.



Подобная схема достаточно удобна, так как временные интервалы могут динамично перераспределяться между устройствами сети. Устройствам с большим трафиком назначаются более длительные интервалы, чем устройствам с меньшим объемом трафика.

Основной недостаток систем с временным уплотнением – это мгновенная потеря информации при срыве синхронизации в канале, например из-за сильных помех, случайных или преднамеренных. Однако успешный опыт эксплуатации таких знаменитых TDM-систем, как сотовые телефонные сети стандарта GSM, свидетельствует о достаточной надежности механизма временного уплотнения.

1. Механизм мультиплексирования посредством ортогональных несущих частот (Orthogonal Frequency Division Multiplexing - OFDM)

Суть этого механизма:

- весь доступный частотный диапазон разбивается на достаточно много поднесущих (от нескольких сот до тысяч);
- одному каналу связи (приемнику и передатчику) назначают для передачи несколько таких несущих, выбранных из множества по определенному закону;
- передача ведется одновременно по всем поднесущим, т. е. в каждом передатчике исходящий поток данных разбивается на N субпотоков, где N - число поднесущих, назначенных данному передатчику.

Распределение поднесущих в ходе работы может динамически изменяться, что делает данный механизм не менее гибким, чем метод временного уплотнения.

1. Преимущества OFDM

Схема OFDM имеет несколько преимуществ.

- Во-первых, селективному замиранию будут подвержены только некоторые подканалы, а не весь сигнал. Если поток данных защищен кодом прямого исправления ошибок, то с этим замиранием легко бороться.
- Во-вторых, что более важно, OFDM позволяет подавить межсимвольную интерференцию.

  Межсимвольная интерференция оказывает значительное влияние при высоких скоростях передачи данных, так как расстояние между битами (или символами) мало.

  В схеме OFDM скорость передачи данных уменьшается в N раз, что позволяет увеличить время передачи символа в N раз. Таким образом, если время передачи символа для исходного потока составляет Ts , то период сигнала OFDM будет равен NTs. Это позволяет существенно снизить влияние межсимвольных помех. При проектировании системы N выбирается таким образом, чтобы величина NTs значительно превышала среднеквадратичный разброс задержек канала.

1. Технология расширенного спектра

Изначально метод расширенного спектра создавался для разведывательных и военных целей. Основная идея метода состоит в том, чтобы распределить информационный сигнал по широкой полосе радиодиапазона, что в итоге позволит значительно усложнить подавление или перехват сигнала.

Первая разработанная схема расширенного спектра известна как **метод перестройки частоты**.

Более современной схемой расширенного спектра является **метод прямого последовательного расширения**. Оба метода используются в различных стандартах и продуктах беспроводной связи.

1. Расширение спектра скачкообразной перестройкой частоты (Frequency Hopping Spread Spectrum - FHSS)

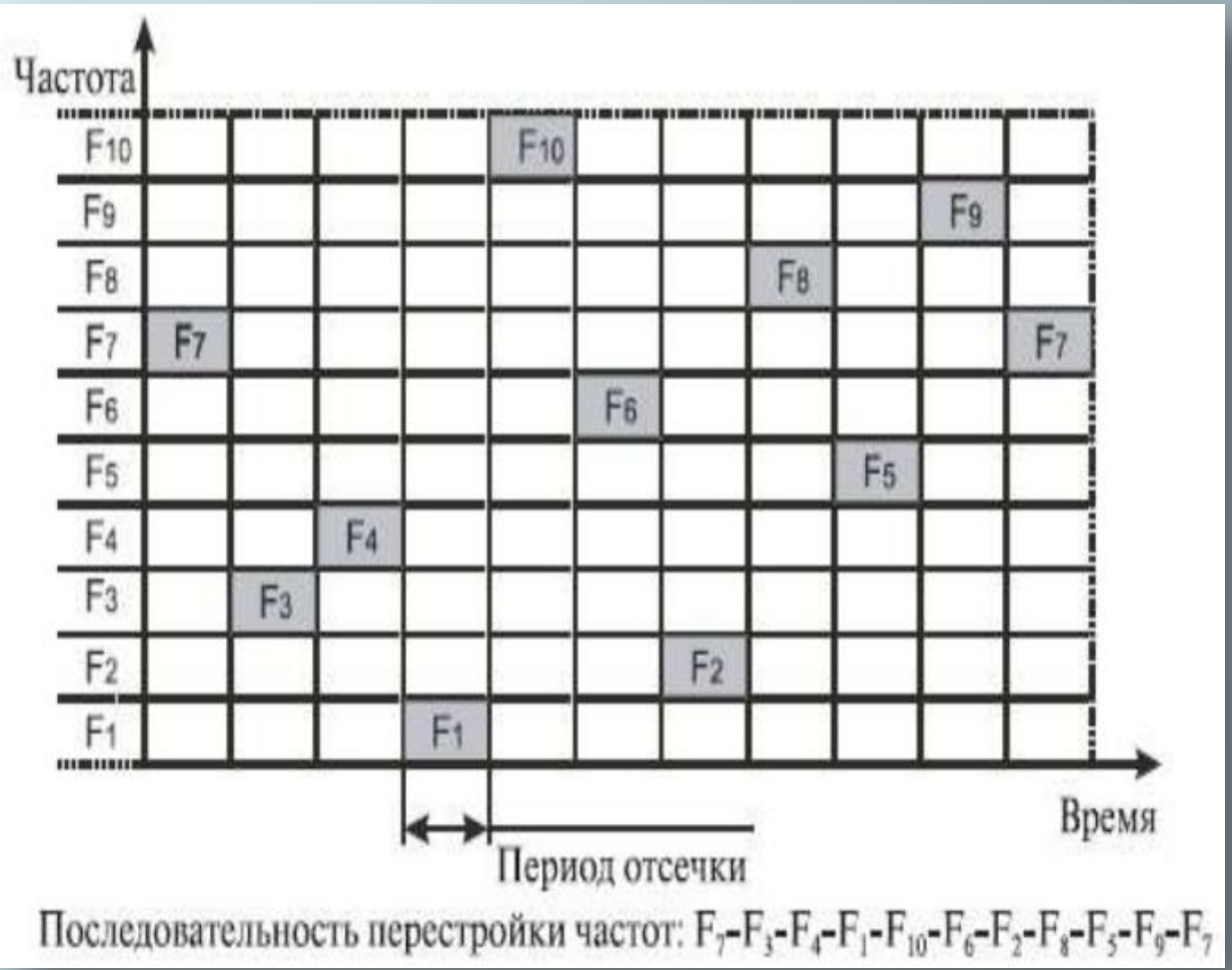
Для того чтобы радиообмен нельзя было перехватить или подавить узкополосным шумом, было предложено вести передачу с постоянной сменой несущей в пределах широкого диапазона частот.

В результате мощность сигнала распределялась по всему диапазону, и прослушивание какой-то определенной частоты давало только небольшой шум.

Последовательность несущих частот была псевдослучайной, известной только передатчику и приемнику.

Попытка подавления сигнала в каком-то узком диапазоне также не слишком ухудшала сигнал, так как подавлялась только небольшая часть информации.

1. Расширение спектра скачкообразной перестройкой частоты (Frequency Hopping Spread Spectrum - FHSS)



1. Медленное и быстрое расширение спектра

Если частота смены подканалов ниже, чем скорость передачи данных в канале, то такой режим называют *медленным расширением спектра*; в противном случае мы имеем дело с *быстрым расширением спектра*.

Метод быстрого расширения спектра более устойчив к помехам, поскольку узкополосная помеха, которая подавляет сигнал в определенном подканале, не приводит к потере бита, так как его значение повторяется несколько раз в различных частотных подканалах. В этом режиме не проявляется эффект межсимвольной интерференции, потому что ко времени прихода задержанного вдоль одного из путей сигнала система успевает перейти на другую частоту.

Метод медленного расширения спектра таким свойством не обладает, но зато он проще в реализации и сопряжен с меньшими накладными расходами.

1. Прямое последовательное расширение спектра (Direct Sequence Spread Spectrum - DSSS)

В методе прямого последовательного расширения спектра 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. А это, в свою очередь, 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 и 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.

1. Расширяющая последовательность

Код, которым заменяется двоичная единица исходной информации, называется *расширяющей последовательностью*, а каждый бит такой последовательности - чипом.

Соответственно, 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. Как и в случае FHSS, для кодирования битов результирующего кода может использоваться любой вид модуляции, например FSK.

Чем больше коэффициент расширения, тем шире спектр результирующего сигнала и выше степень подавления помех. Но при этом растет занимаемый каналом диапазон спектра. Обычно коэффициент расширения имеет значение от 10 до 100.

1. Стандарт 802.11

Исходный стандарт 802.11 определяет три метода передачи на физическом уровне:

- передача в диапазоне инфракрасных волн;
- технология расширения спектра путем скачкообразной перестройки частоты (FHSS) в диапазоне 2,4 ГГц;
- технология широкополосной модуляции с расширением спектра методом прямой последовательности (DSSS) в диапазоне 2,4 ГГц.

1. Беспроводная среда

Беспроводная среда образуется совокупностью радиоканалов, сгруппированных в несколько частотных диапазонов.

Три частотных диапазона: 900 МГц, 2,4 ГГц и 5 ГГц рекомендованы ITU для использования в промышленности, науке и медицине (Industrial, Scientific, Medical – ISM) и не требуют лицензирования.

1. Борьба с ошибками

Существует три наиболее распространенных орудия борьбы с ошибками в процессе передачи данных:

- коды обнаружения ошибок;
- коды с коррекцией ошибок, называемые также схемами прямой коррекции ошибок (Forward Error Correction - FEC);
- протоколы с автоматическим запросом повторной передачи (Automatic Repeat Request - ARQ).

1. Стандарт IEEE 802.11b

Технология Wi-Fi – беспроводной аналог стандарта Ethernet, на основе которого сегодня построена большая часть офисных компьютерных сетей. Он был зарегистрирован в 1999 году.

Wireless Fidelity – обозначает стандарт беспроводной (радио) связи, который объединяет несколько протоколов и имеет официальное наименование IEEE 802.11

IEEE 802.11b – стандарт, определяющий функционирование беспроводных сетей, в которых для передачи данных используется диапазон частот от 2,4 до 2.4835 Гигагерца и обеспечивается максимальная скорость 11 Мбит/сек. Максимальная дальность передачи сигнала в такой сети составляет 100 метров, однако на открытой местности она может достигать и больших значений (до 300-400 м).

1. Контроллеры доступа

• **Аутентификация.** Большинство контроллеров доступа используют для аутентификации пользователей встроенную базу данных, однако некоторые предлагают осуществлять для этого взаимодействие с внешним сервером аутентификации, таким как Служба удаленной аутентификации пользователей по телефонной сети ***(Remote Authentication Dial-In User Service, RADIUS)*** и используют Облегченный протокол службы каталогов ***(Lightweight Directory Access Protocol, LDAP)***. Для небольших частных сетей подойдет внутренняя база данных. На предприятиях лучшие результаты достигаются при использовании внешних и централизованных серверов аутентификации.

• **Шифрование.** Некоторые контроллеры доступа обеспечивают шифрование данных, передаваемых от клиента к серверу и обратно, используя при этом такой распространенный метод, как ***IPSec***. Это обеспечивает дополнительную защиту по сравнению с той, которую дают методы, регламентированные стандартами на беспроводные сети. Некоторые из этих особенностей реализуются Web-браузерами.

1. Контроллеры доступа

- **Роуминг через подсети.** Для поддержания роуминга из одной сети в другую контроллеры доступа обеспечивают роуминг через подсети (subnets) без необходимости проведения реаутентификации в системе. В результате пользователь может без перерывов пользоваться сетевыми приложениями, даже если он перемещается по зданию. Это особенно полезно для обширных сетей, когда доступ к сети отдельного пользователя приходится обеспечивать через несколько подсетей.

- **Управление пропускной способностью.** Поскольку пользователи совместно используют полосу пропускания беспроводной сети, важно иметь механизм, не позволяющий отдельным пользователям использовать всю пропускную способность сети. Контроллеры доступа обеспечивают подобную форму управления пропускной способностью за счет назначения профилей пользователей, основанных на требуемых уровнях качества связи. Профиль регламентирует типы предоставляемых услуг, таких как просмотр Web-страниц, электронная почта и потоковое видео, а также ограничения характеристик. Например, неподписанный на сервисы сети визитер, пытающийся воспользоваться услугами общедоступной беспроводной локальной сети, может быть классифицирован как имеющий профиль «визитера», доступ которому может быть разрешен только к информации «горячей» точки. Но абонент может получить и другие права доступа, позволяющие ему использовать широкополосное Internet-соединение

1. Варианты стандартов

Помимо 802.11b существуют еще беспроводной стандарт 802.11a, использующий частоту 5 ГГц и обеспечивающий максимальную скорость 54 Мбит/с, а также 802.11g, работающий на частоте 2,4 ГГц и тоже обеспечивающий 54 Мбит/с.

Однако, из-за меньшей дальности, значительно большей вычислительной сложности алгоритмов и высокого энергопотребления эти технологии не получила большого распространения. Стандарт 802.11n обеспечил скорость до 320 Мбит/с.

Применяемый вид модуляции – OFDM. Устройства стандарта 802.11a не могут взаимодействовать с устройствами стандарта 802.11b и 802.11g, поскольку последние работают в диапазоне 2,4 ГГц.

1. Применение Wi-Fi

Подобно традиционным проводным технологиям, Wi-Fi обеспечивает доступ к серверам, хранящим базы данных или программные приложения, позволяет выйти в Интернет, распечатывать файлы и т. д.

Но при этом компьютер, с которого считывается информация, не нужно подключать к компьютерной розетке. Достаточно разместить его в радиусе 300 м от так называемой точки доступа (Wireless Access Point – **WAP**) – Wi-Fi-устройства, выполняющего примерно те же функции, что обычная офисная АТС.

Wi-Fi-технология позволяет решить три важных задачи:

- упростить общение с мобильным компьютером;
- обеспечить комфортные условия для работы деловым партнерам, пришедшим в офис со своим ноутбуком;
- создать локальную сеть в помещениях, где прокладка кабеля невозможна или чрезмерно дорога.

1. Точка доступа

Ядром беспроводной сети Wi-Fi является так называемая **точка доступа** (Access Point), которая подключается к какой-либо наземной сетевой инфраструктуре (например, офисной Ethernet-сети) и обеспечивает передачу радиосигнала.

Обычно точка доступа состоит из приемника, передатчика, интерфейса для подключения к проводной сети и программного обеспечения для обработки данных. После подключения вокруг точки доступа образуется территория радиусом 50-100 метров (её называют **хот-спотом** или **зоной Wi-Fi**), на которой можно пользоваться беспроводной сетью.

2. Семейство стандартов IEEE 802.15

Семейство стандартов IEEE 802.15 образует беспроводную сеть **WPAN** (Wireless Personal Area Network), которая обеспечивает беспроводную связь между различного типа устройствами на небольших расстояниях.

Стандарты, которые входят с это семейство:

- **Bluetooth** (IEEE 802.15.1)
- **IEEE 802.15.3, ZigBee** (IEEE 802.15.4)
- **UWB** (Ultra Wideband) (IEEE 802.15.4a/b).

2. Bluetooth

Bluetooth – технология беспроводной передачи данных по радиоканалу между различными типами электронных устройств с целью обеспечения их взаимодействия. Разработка этой системы была начата в 1998 г. компаниями Ericsson, IBM, Intel, Nokia, Toshiba, а позднее - группой SIG (Special Interest Group), в которую входят многие фирмы, в том числе корпорации Lucent, Microsoft и другие.

При разработке Bluetooth-интерфейса выдвигались следующие требования:

- аппаратура должна быть компактной,
- недорогой и экономичной,
- должна быть способна работать при малых значениях потребляемого тока.

2. Методы передачи

Система Bluetooth работает в диапазоне 2.4 - 2.48 ГГц (диапазон ISM – Industry, Science, Medicine - промышленный, научный, медицинский) и предназначена для передачи на дальность от 10 до 100 метров голоса или данных.

Передача голоса возможна по трем каналам со скоростью 64 Кбит/с.

Передача данных возможна с помощью:

- асимметричного метода, обеспечивающего скорость передачи 721 Кбит/с в одном направлении и 57,6 Кбит/с в другом;
- симметричного метода, обеспечивающего одинаковую скорость 432,6 Кбит/с в обоих направлениях.

2. Передача данных пакетами

В Bluetooth реализована передача данных пакетами с использованием скачкообразной перестройкой частоты 1600 раз в секунду по псевдослучайному закону или шаблону (pattern), составленному из 79 подчастот (принцип FHSS – Frequency-Hopping Spread Spectrum).

Настройка на один шаблон позволяет использующим Bluetooth устройствам осуществлять обмен данными, в то время как другие устройства будут воспринимать передаваемую информацию как шум.

2. Информационная безопасность

Информационная безопасность системы беспроводной передачи данных Bluetooth базируется на использовании:

- частотных шаблонов и необходимости синхронизации процессов приема и передачи данных;
- возможности реализации односторонней или двусторонней аутентификации;
- шифрования передаваемых данных.

Длина ключа шифрования может варьироваться от 8 до 128 бит, что дает возможность регулировать криптостойкость используемого алгоритма шифрования.

Система Bluetooth позволяет объединять в одну беспроводную пикосеть (piconet) от двух до восьми различных электронных устройств, таких как, например, сотовый телефон, беспроводная гарнитура, ноутбук, цифровой фотоаппарат, принтер, клавиатура и др., но общее количество объединяемых устройств (как результат объединения пикосетей) может достигать 71.

2. Информационная безопасность

По сравнению с интерфейсом беспроводной связи IEEE 802.11, работающим в том же диапазоне частот – 2,4 ГГц, Bluetooth-система обеспечивает:

- меньшую скорость передачи информации (721 Кбит/с против 11 Мбит/с в стандарте IEEE 802.11b);
- меньшую дальность и меньшее число объединяемых в сеть устройств (максимально до 71 устройства у Bluetooth, 128 на одну сеть у IEEE 802.11).

Но система Bluetooth может по трем каналам передавать голосовую информацию, а главное, более дешевая (в десятки раз), малогабаритная и экономичная.

2. Принцип работы Bluetooth

Bluetooth способна осуществлять передачу данных даже при наличии препятствий и не только по принципу «точка–точка», но и по принципу «точка–много точек», что в положительную сторону отличает Bluetooth от технологии беспроводной инфракрасной связи IrDa, которая обеспечивает связь лишь в зоне прямой видимости и только по принципу «точка–точка».

Хотя в Bluetooth предусмотрена криптографическая защита конфиденциальности передаваемых данных, а также процедура аутентификации, предназначенная для защиты от несанкционированного доступа к системе, нарушения информационной безопасности устройств, снабженных Bluetooth, являются реальностью.

2. Угрозы

Угрозы информационной безопасности сотовых систем связи, реализуемые через Bluetooth-интерфейс:

- проникновение в абонентский аппарат мобильных вирусов и связанные с этим угрозы потери конфиденциальности передаваемой информации, а также целостности, доступности и конфиденциальности информации, хранящейся в абонентском аппарате;
- перехват информации, передаваемой по радиоканалу системы Bluetooth;
- дистанционный перехват управления абонентским аппаратом, позволяющий злоумышленнику осуществлять звонки и/или отсылку SMS и MMS сообщений за счет законного владельца аппарата, изменять настройки аппарата, считывать информацию, хранящуюся в памяти аппарата.

Важной задачей является защита конфиденциальности информации, хранящейся в памяти мобильных устройств.

2. Атаки

Виды атак на устройства с поддержкой Bluetooth могут быть классифицированы следующим образом.

1. ***Bluejacking*** - атака, использующая способность устройств Bluetooth обнаруживать другие близко расположенные Bluetooth-устройства и посылать на них сообщения, которые отображаются на дисплее атакуемого устройства. Bluejacking может использоваться для рассылка спама и распространения вредоносных программ, а также в хулиганских целях.
2. ***Bluesnarfing*** – атака, основанная на несанкционированном соединении с другим Bluetooth-устройством без уведомления его владельца с целью получения доступа к данным, записанным в памяти аппарата, таким как, например, телефонные номера, записи в адресной книге и ежедневнике. На практике доказана возможность осуществления таких соединений, несмотря на использование так называемого «невидимого» режима работы атакуемого Bluetooth-устройства.
3. ***Bluebug*** – атака, направленная на установление последовательного соединения с атакуемым Bluetooth-устройством с тем, чтобы осуществлять контроль за его службами обмена данными, посылать и получать сообщения, а также производить телефонные звонки с атакованного аппарата.

2. Bluetooth (IEEE 802.15.1)

Bluetooth – это беспроводная технология, являющаяся стандартом, который обеспечивает беспроводную передачу данных на небольших расстояниях между мобильными персональными компьютерами, мобильными телефонами и другими устройствами в режиме реального времени как цифровых данных, так и звуковых сигналов.

Стандарт IEEE 802.15.1 базируется на спецификациях Bluetooth v. 1.x. Bluetooth - это недорогой радиоинтерфейс с низким уровнем энергопотребления (порядком 1 mW).

Сначала дальность действия Bluetooth была в радиусе 10 м, позже увеличилось до 100 м.

Для работы Bluetooth используется так называемый нижний 2,45 ГГц диапазон ISM (industrial, scientific, medical), который предназначен для работы промышленных, научных и медицинских приборов.

2. Типы соединения

Протокол Bluetooth поддерживает соединения типа:

- точка-точка,
- также и соединения типа точка-многоточка.

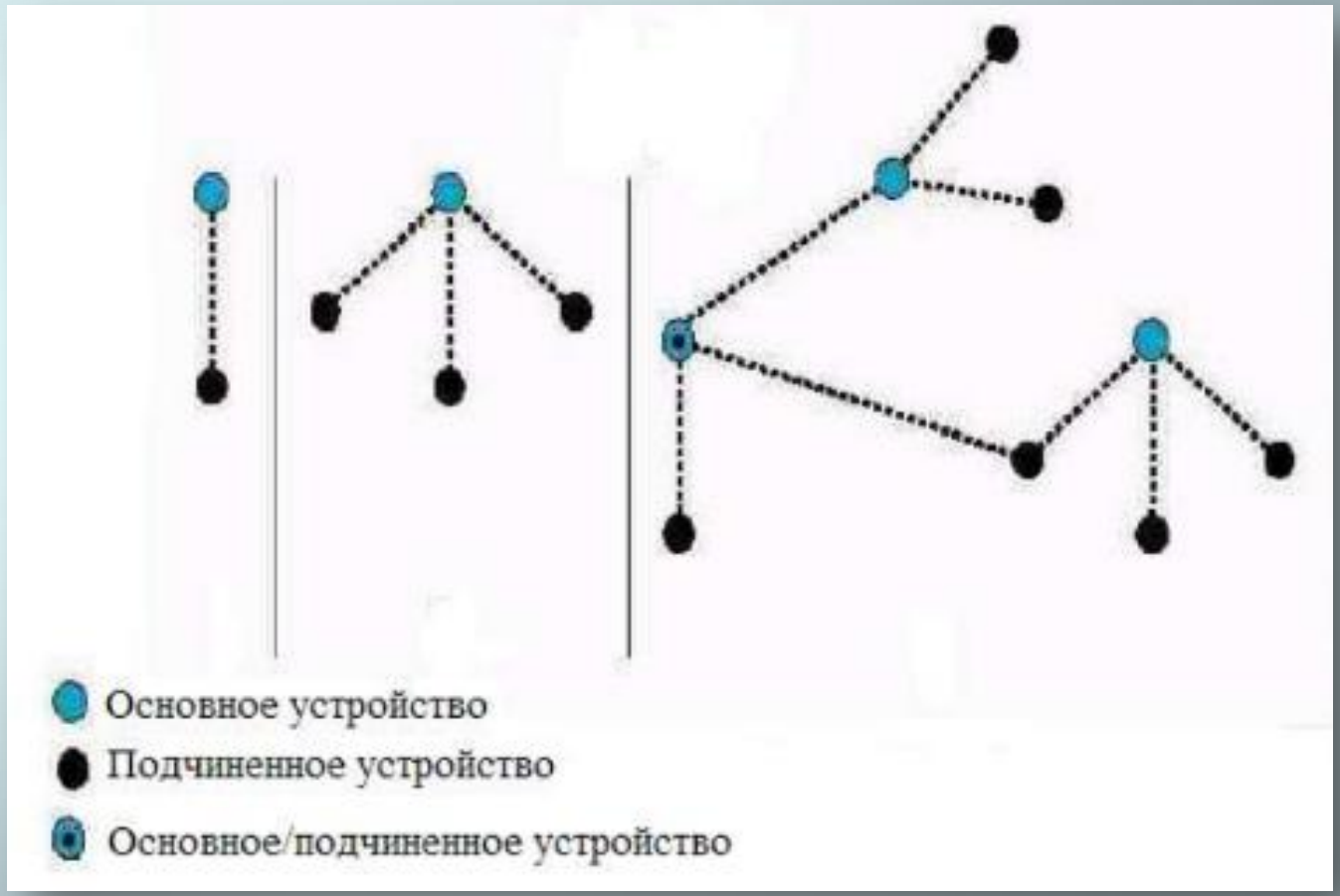
Два устройства или более, которые используют один и тот же канал образуют пикосеть (piconet). Одно из устройств работает как основное (мастер) (master), а остальные – как подчиненные (slave) устройства. В одной пикосети может быть до восьми активных подчиненных устройств, при этом остальные

подчиненные устройства находятся в состоянии "парковки", которые синхронизированны с основным устройством. На расстоянии 10 м может существовать до 10 пикосетей.

«Распределенную сеть» (scatternet) образуют взаимодействующие пикосети.

В каждой пикосети действует только одно основное устройство, но подчиненные устройства могут входить в различные пикосети. Помимо этого, основное устройство одной пикосети может быть подчиненным устройством в другой.

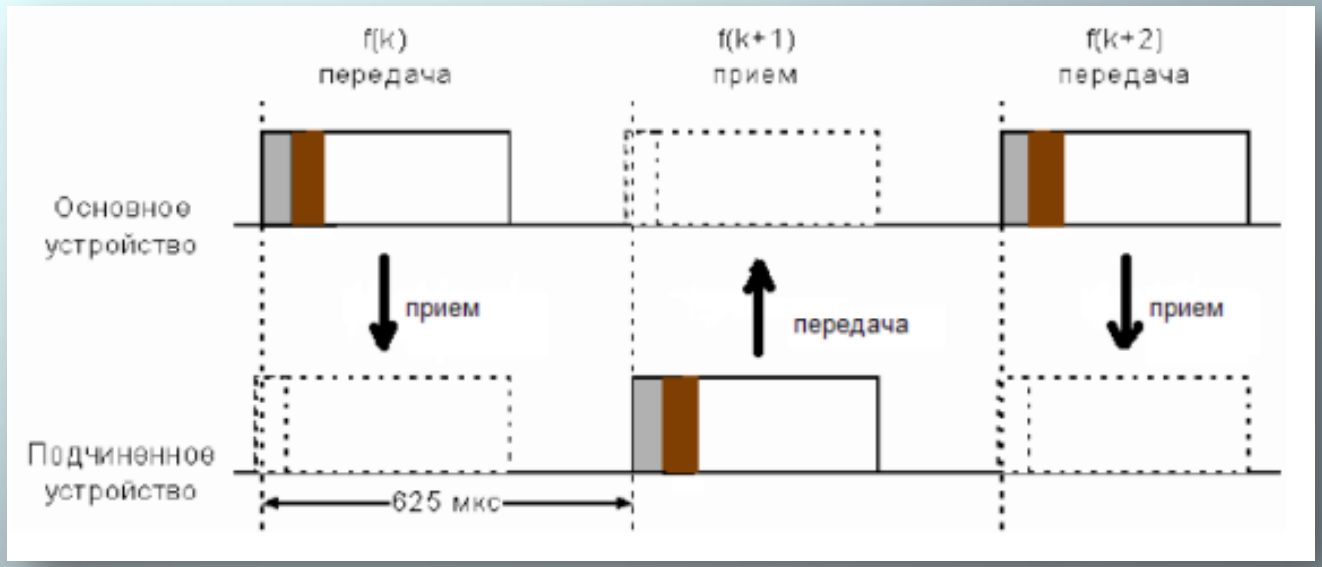
2. Различные виды пикосети Bluetooth



2. Передача данных Bluetooth

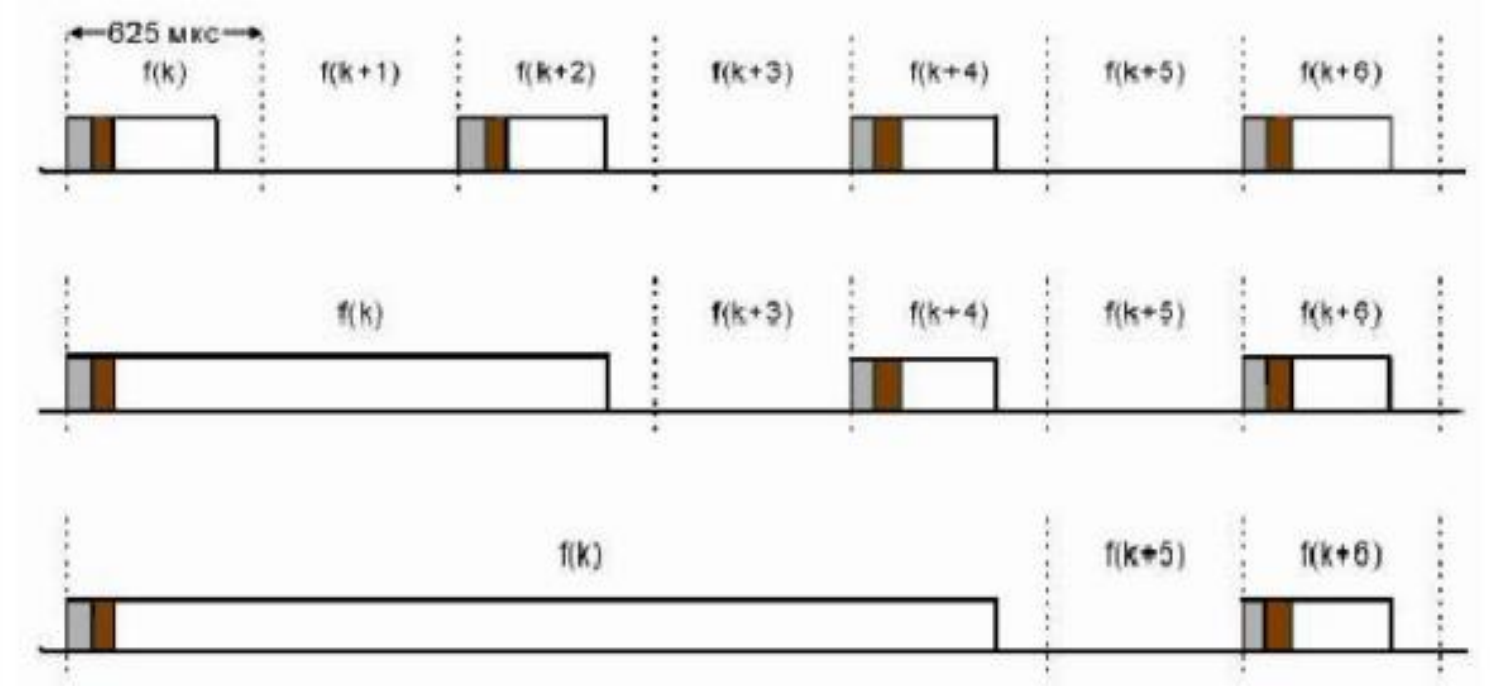
В стандарте Bluetooth предусмотрена дуплексная передача на основе разделения времени (Time Division Duplexing - TDD).

Основное устройство передает пакеты в нечетные временные сегменты, а подчиненное устройство – в четные.



2. Передача данных Bluetooth

Пакеты в зависимости от длины могут занимать до пяти временных сегментов. При этом частота канала не меняется до окончания передачи пакета.



2. Характеристики Bluetooth

Протокол Bluetooth может поддерживать:

- асинхронный канал данных,
- до трех синхронных (с постоянной скоростью) голосовых каналов;
- канал с одновременной асинхронной передачей данных и синхронной передачей голоса.

Скорость каждого голосового канала – 64 Кбит/с в каждом направлении, асинхронного в асимметричном режиме – до 723,2 Кбит/с в прямом и 57,6 кбит/с в обратном направлениях или до 433,9 Кбит/с в каждом направлении в симметричном режиме.

2. Синхронное соединение

Синхронное соединение (SCO – Synchronous Connection Oriented) возможно только в режиме точка-точка. Такой вид связи применяется для передачи информации, чувствительной к задержкам – например, голоса.

Основное устройство поддерживает до трех синхронных соединений, подчиненное – до трех синхронных соединений с одним основным устройством или до двух – с разными основными устройствами.

При синхронном соединении основное устройство резервирует временные сегменты, следующие через так называемые SCO-интервалы. Даже если пакет принят с ошибкой, повторно при синхронном соединении он не передается.

2. Асинхронное соединение

При асинхронной связи (ACL – Asynchronous Connection Less) используются временные сегменты, не зарезервированные для синхронного соединения.

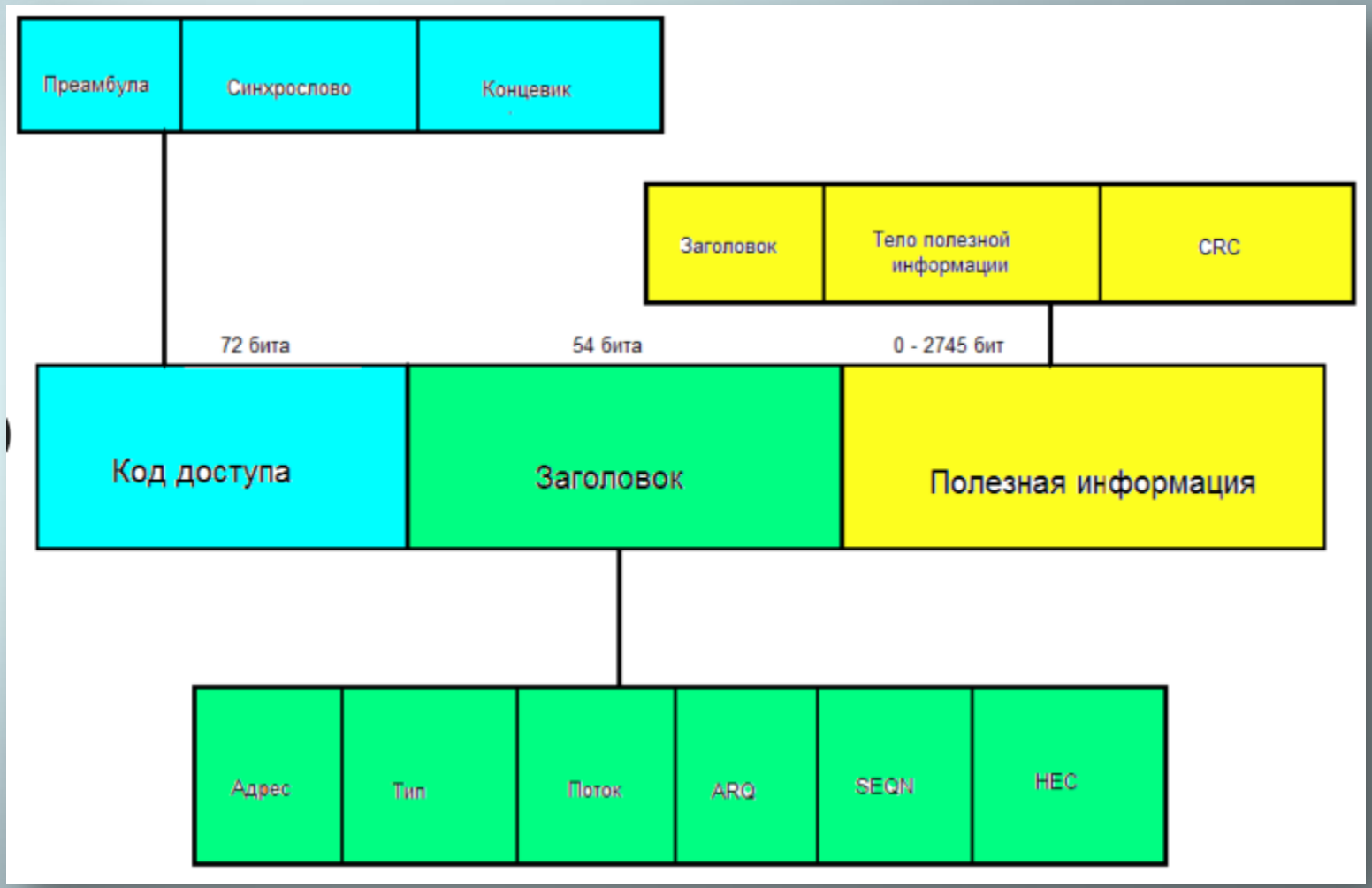
Асинхронное соединение возможно между основным и всеми активными подчиненными устройствами в пикосети (точка - многоточка).

Основное и подчиненное устройства могут поддерживать только одно асинхронное соединение.

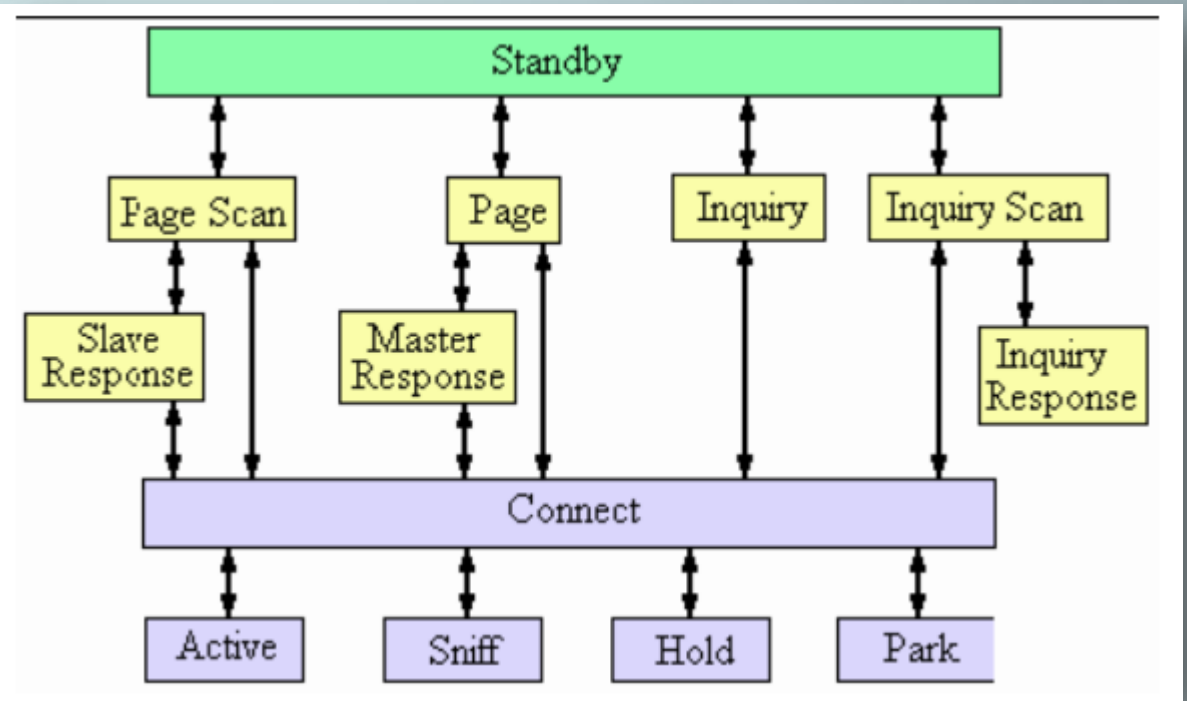
Поскольку в пикосети может быть несколько подчиненных устройств, конкретное подчиненное устройство отправляет пакет основному, только если в предыдущем временном интервале на его адрес пришел пакет от основного устройства. Если в адресном поле ACL-пакета адрес не указан, пакет считается «широковещательным» – его могут принимать все устройства.

Асинхронное соединение позволяет повторно передавать пакеты, принятые с ошибками.

2. Структура пакета



2. Работа Bluetooth



Есть два основных состояния для устройств Bluetooth:

- соединение (Connection);
- режим ожидания (Standby).

Предусмотрено семь субсостояний, которые используются для добавления клиента или подключения к пикосети: page, page scan, inquiry, inquiry scan, master response, slave response и inquiry response.

2. Протоколы Bluetooth

При работе устройств Bluetooth используются специфические протоколы для Bluetooth и общие, которые используются в различных телекоммуникационных системах. Все они образуют стек протоколов Bluetooth.

Все эти протоколы можно разделить на 4 слоя:

1. Корневые протоколы.
2. Протокол замены кабеля
3. Протокол управления телефонией
4. Заимствованные протоколы

2. Профили Bluetooth

Специальная рабочая группа Bluetooth SIG определила различные модели использования, каждая из которых сопровождается профилем.

Профили определяют протоколы и функции, которые поддерживают определенные модели использования. Если устройства от различных производителей соответствуют одному профилю, определенному в спецификации Bluetooth, они смогут взаимодействовать.

Четыре общих профиля применяются для различных моделей использования:

- профиль общего доступа;
- профиль последовательного порта;
- профиль приложения обнаружения услуг;
- профиль общего обмена объектами.

Остальные профили применяются непосредственно для определенных моделей использования.

2. Остальные профили Bluetooth

- профиль общего доступа (Generic Access Profile);
- профиль приложения обнаружения услуг (Service Discovery Application Profile);
- профиль беспроводной телефонии (Cordless Telephony Profile);
- профиль внутренней связи (Intercom Profile);
- профиль последовательного порта (Serial Port Profile);
- профиль гарнитуры (Headset Profile);
- профиль коммутируемого выхода на сеть (Dial-up Networking Profile);
- профиль факса (Fax Profile);
- профиль доступа к локальной сети (LAN Access Profile);
- профиль общего обмена объектами (Generic Object Exchange Profile);
- профиль помещения объекта в стек (Object Push Profile);
- профиль передачи файла (File Transfer Profile);
- профиль синхронизации (Synchronization Profile).

2. Основные конкуренты

IrDA (Infrared Data Association) – это стандарт инфракрасного интерфейса, который составляет альтернативу для Bluetooth в области беспроводных устройств. Преимуществами IrDA являются:

- дешевле, чем Bluetooth;
- скорость передачи данных выше, чем у Bluetooth. У IrDA – 4 Мбит/с, а у Bluetooth – 1 Мбит/с.

К недостаткам можно отнести:

- расстояние, на которое можно передать данные относительно мало – 1м;
- ограниченное только до соединения точка-точка;
- порты устройств должны находиться в прямой видимости друг от друга;
- не все устройства поддерживают стандарт (несовместимость между некоторыми продуктами).

UWB (Ultra-Wideband Radio) - это сверхширокополосные технологии радиосвязи, которые работают по тому же принципу, что и радары: посылаются короткие импульсы в большой частотной области. К преимуществам можно отнести также отнести малое энергопотребление и невысокую стоимость.