**Лабораторная работа №6 – Работа с интерфейсом Bluetooth**

# **Каковы основные принципы работы технологии Bluetooth?**

* Радиочастотная связь: Использует частоту 2,4 ГГц, что обеспечивает компактность и энергоэффективность устройств.
* Спецификация IEEE 802.15: Основывается на стандарте IEEE 802.15.1 для персональной беспроводной связи.
* Автоматическое обнаружение: Устройства автоматически находят друг друга для упрощения сопряжения.
* Частотные прыжки (FHSS): Использует частотные прыжки до 1600 раз в секунду для уменьшения помех.
* Многоканальный режим: Поддерживает одновременную передачу данных несколькими устройствами в одном радиочастотном диапазоне.
* Пакетная передача и сжатие: Данные передаются в пакетах с контрольными битами для повышения устойчивости к помехам.
* Топология сети: Включает пикосети (до 7 устройств) и скатернет (несколько пикосетей).
* Энергосбережение: Оптимизирован для минимального энергопотребления с короткими активными периодами и длительными периодами "сна".
* Безопасность: Обеспечивает шифрование и аутентификацию для предотвращения несанкционированного доступа.

# **Какие основные версии Bluetooth существуют, и в чем заключаются их отличия?**

***Версия 1.0***

Вышла в свет в 1998г. и позволяла передавать данные на расстоянии нескольких метров. Для нее были характерны плохая совместимость между изделиями разных производителей и невозможность реализации анонимного соединения на протокольном уровне. Эта версия уже давно не используется.

***Версии 1.1 и 1.2***

В этих обновлениях введены поддержка нешифрованных каналов, отображение мощности входящего сигнала и ускорен процесс обнаружения/подключения устройств. Также была увеличена помехостойкость, увеличена скорость трансляции (721Кбит/с) и реализована сетевая анонимность. Эти версии позволяли передавать уже и речевые сообщения и стереозвук (A2DP-профиль). В настоящее время можно купить дешевый телефон китайского производителя с обновлением 1.2***.***

***Версии 2.0 и 2.1***

Обновление 2.0 вышло в 2004г., 2.1 – в 2007г. Разница между ними заключается в большей энергоэкономичности последней версии. Главная особенность Bluetooth 2.0 – внедрение технологии EDR, повышавшей скорость до теоретических 3Мбит/с (на практике чаще всего получалось 1,5-2Мбит/с. Сегодня можно купить недорогой смартфон, поддерживающий эту технологию.

Версия 2.1 – самое популярное обновление Bluetooth. Она совместима фактически со всеми устройствами, представленными на мобильном рынке. Причем если в смартфонах/планшетах используется Bluetooth более свежих обновлений, то в беспроводных мышах, клавиатурах, гарнитурах и т.д. нередко реализован именно стандарт 2.1+EDR. В этих обновлениях введены поддержка нешифрованных каналов, отображение мощности входящего сигнала и ускорен процесс обнаружения/подключения устройств. Также была увеличена помехостойкость, увеличена скорость трансляции (721Кбит/с) и реализована сетевая анонимность. Эти версии позволяли передавать уже и речевые сообщения и стереозвук (A2DP-профиль).

Энергопотребление в версии 2.1 снизилось почти в 10 раз, появилась дополнительная полоса пропускания, что облегчило использование нескольких подключений одновременно. Реализовано подключение нажатием одной кнопки.

***Версия 3.0***

Вышла в 2009г и впервые использовала высокоскоростную (HS) трансляцию данных. Скорость возросла до 24Мбит/с. Реализовано это было за счет установки двух модулей (Bluetooth2.1+EDR и модуля, функционирующего по протоколу 802.11, как и Wi-Fi). Именно второй модуль и «выдает» скачок скорости, но не дает Wi-Fi-совместимость. Файлы небольшого объема передаются при помощи модуля 2.1+EDR, объемные – по протоколу 802.11.

Недостатком такого решения стало возросшее энергопотребление.

***Версии 4.0 и 4.1***

Обновление 4.0 вышло в 2010г. В нем был исправлен основной недостаток HS – чрезмерное потребление энергии. Спецификация 4.0 включала в себя «традиционный» модуль Bluetooth и высокоскоростную передачу (основанную на Wi-Fi). Также был добавлен Bluetooth-протокол с минимальным энергопотреблением. Они используется главным образом в электронных датчиках, мини-сенсорах (в том числе и медицинских) и т.д.

Время установления соединения снизилось до 5мс, расстояние передачи возросло до 100м. Введено AES-шифрование для защиты данных. Эта версия реализована в свежих моделях крупных производителей и установлена на флагманских смартфонах Хайскрин.

Обновление 4.1 представлено в 2013г. Главные доработки касаются совместного функционирования Bluetooth и LTE-стандарта. Пакеты данных автоматически координируются для взаимной помехозащиты.

При выборе смартфона не стоит путать версии и профили Bluetooth. Профиль – это набор функциональных возможностей, один и тот же профиль могут реализовывать разные версии. К примеру, речь и стереозвучание передаются, начиная с обновления 1.2. При этом для каждого конкретного устройства может быть доступным только определенный функциональный набор, меньший, чем заложенный в используемой версии Bluetooth. Таким образом, для успешного взаимодействия Bluetooth-устройств у них должна быть реализована поддержка одного и того же профиля (версии Bluetooth могут быть разным).

***Версии 4.0, 4.2 и 5.0***

В 2018-2019 наибольшее распространение имеют версии Bluetooth 4.0 - 4.2 и 5.0. При этом, стандарт Bluetooth 4.2, анонсируется как версия с улучшенными параметрами, предоставляющая новые решения для "умного дома", новые профили, как IPSP. Версия же 5.0 предлагается, как новый стандарт с более высокой скоростью передачи данных, что оценят по большей части разработчики и улучшенным возможностями для беспроводных технологий

# **Какие уровни безопасности предусмотрены в технологии Bluetooth, и какие методы защиты данных используются?**

Security Mode 1 – отсутствие какой-либо защиты. Чаще всего используется только в рамках тестирования. NIST рекомендует никогда не применять этот режим. До сих пор существует для поддержки обратной совместимости со старыми устройствами.

Security Mode 2 – функции безопасности могут быть инициированы после установления соединения, но до установления логического канала. Функции безопасности контролируют доступ к службам. В этом режиме вводится понятие авторизации — процесс определения того, разрешено ли конкретному устройству иметь доступ к определенной службе.

Security Mode 3 – режим безопасности, функции которого работают на уровне канала. В данном режиме Bluetooth устройство инициирует процедуры безопасности до того, как соединение полностью установлено. Устройства Bluetooth, работающие в режиме безопасности 3, выполняют аутентификацию и шифрование для всех подключений к устройству и с него.

Security Mode 4 – по сути усовершенствование режима безопасности 2. Функции безопасности реализуются после установления соединения. Для генерации ключа соединения (link key) используется ECDH (Протокол Диффи-Хеллмана на эллиптических кривых). Данный режим также имеет 5 уровней требований (от 0 до 4) к реализации:

Методы защиты данных:

**Аутентификация:**

Перед установлением соединения устройства могут обмениваться ключами аутентификации. Это предотвращает несанкционированный доступ.

**Шифрование:**

Bluetooth использует алгоритмы шифрования, такие как E0 (для базового Bluetooth) и более современные алгоритмы, такие как AES для Bluetooth 2.1 и выше. Это обеспечивает защиту данных от перехвата.

**Парные ключи:**

Устройства создают временные ключи сессии, которые используются для шифрования и аутентификации в рамках конкретного соединения. Это делает атаки на основе перехвата менее эффективными.

**Секретность и конфиденциальность:**

Используются различные механизмы для обеспечения конфиденциальности передаваемых данных, включая адресацию (например, случайные адреса в BLE).

**Защита от атак:**

Bluetooth включает в себя защиту от атак типа "человек посередине" (MITM) с помощью механизмов аутентификации, таких как Secure Simple Pairing (SSP).

**Обновление безопасности:**

Bluetooth регулярно обновляет свои спецификации, чтобы включать новые методы защиты и улучшать существующие механизмы безопасности.

# **Каковы принципы работы беспроводной технологии Wi-Fi?**

Если говорить просто, то передача данных с помощью Wi-Fi работает следующим образом:

* На антенны роутера или маршрутизатора подаётся ток, который используется для генерации радиоволн.
* Здесь происходит модулирование сигнала. Это означает, что его характеристики, такие как амплитуда, частота или фаза, изменяются в соответствии с битами информации, которые требуется передать. Модуляция «упаковывает» передаваемые данные (набор нулей и единиц) в форму радиоволны, пригодную для беспроводной передачи.
* На компьютере или другом гаджете приёмник демодулирует сигнал, переводя радиоволну в исходные данные, то есть в набор нулей и единиц, с которыми способны работать устройства.

Для беспроводной связи используются радиоволны в диапазоне частот 2,4, 5 и 6 ГГц. Внутри диапазона есть отдельные каналы для подключения:

* Для Wi-Fi с частотой 2,4 ГГц используется три непересекающихся канала с шириной 20 МГц каждый.
* Для частоты 5 ГГц используются 33 канала, 19 из которых не пересекаются. При этом каналы имеют ширину 40 МГц, то есть в два раза больше, чем у Wi-Fi с частотой 2,4.
* Для стандарта с частотой 6 ГГц используется уже 59 каналов различной ширины. В нём появляются 14 дополнительных каналов шириной 80 МГц и семь дополнительных каналов шириной 160 МГц.

Простое правило: чем больше непересекающихся каналов и чем больше их ширина, тем меньше помех будет возникать из-за одновременной работы нескольких сетей. Поэтому в многоквартирных домах или в бизнес-центрах, где одновременно существуют десятки или сотни беспроводных сетей, лучше использовать Wi-Fi с частотой 5 ГГц, а не 2,4 ГГц. В последнем случае они будут пересекаться, снижая стабильность друг друга.

Для безопасности передачи данных по Wi-Fi используются различные методы шифрования, например [WPA](https://ru.wikipedia.org/wiki/WPA) (Wi-Fi Protected Access) и WPA2. Это стандарты безопасности, которые защищают беспроводные сети от взлома.

# **Какие стандарты Wi-Fi существуют, и в чем основные отличия между ними?**

**Wi-Fi**, который является сокращением от Wireless Fidelity, - это технология беспроводной передачи данных, которая используется для подключения устройств к локальной сети и Интернету. Существует несколько разных версий Wi-Fi, каждая из которых имеет свои особенности и ограничения.

* **Wi-Fi 1 (802.11b)** - это первая версия Wi-Fi, которая была выпущена в 1999 году. Она поддерживает скорость передачи данных ***до*** ***11 Мбит/с*** и работает на частоте 2,4 ГГц. Эта версия быстро стала не популярной из-за своей низкой скорости и высокой чувствительности к помехам.
* **Wi-Fi 2 (802.11a)** - это вторая версия Wi-Fi, которая была выпущена в 1999 году. Она поддерживает скорость передачи данных ***до 54 Мбит/с*** и работает на частоте 5 ГГц. Эта версия была более дороже и менее популярна, чем Wi-Fi 1.
* **Wi-Fi 3 (802.11g)** - это третья версия Wi-Fi, которая была выпущена в 2003 году. Она поддерживает скорость передачи данных ***до 54 Мбит/с*** и работает на частоте 2,4 ГГц. Эта версия была более доступной и популярной, чем Wi-Fi 2, поскольку она была совместима со старыми устройствами Wi-Fi 1 и имела более высокую скорость передачи данных.
* **Wi-Fi 4 (802.11n)** - это четвертая версия Wi-Fi, которая была выпущена в 2009 году. Она поддерживает скорость передачи данных ***до 600 Мбит/с*** и работает на частоте 2,4 или 5 ГГц. Эта версия имеет более высокую скорость и более широкую область покрытия сигнала, чем Wi-Fi 3.
* **Wi-Fi 5 (802.11ac)** - это пятая версия Wi-Fi, которая была выпущена в 2014 году. Она поддерживает скорость передачи данных ***до 3,5 Гбит/с*** и работает на частоте 5 ГГц. Эта версия имеет более высокую скорость и более широкую область покрытия сигнала, чем Wi-Fi 4. Она также использует мультиплексирование каналов для увеличения пропускной способности сети и поддержку мульти-user ***MIMO*** (MU-MIMO) для увеличения количества устройств, которые могут одновременно подключаться к сети.
* **Wi-Fi 6 (802.11ax)** - это шестая версия Wi-Fi, которая была выпущена в 2019 году. Она поддерживает скорость передачи данных **до 10 Гбит/с** и работает на частоте 2,4 или 5 ГГц. Wi-Fi 6 имеет более высокую скорость, более широкую область покрытия сигнала и более эффективное управление энергопотреблением, чем Wi-Fi 5. Он также использует мульти-user ***MIMO*** и другие технологии, чтобы улучшить общую производительность сети и снизить задержки.

# **Какие частоты используются для беспроводной передачи данных по Wi-Fi, и как это влияет на дальность и скорость соединения?**

***Диапазон 2,4 ГГц:***

* *Преимущества*: Длинные радиоволны позволяют этому диапазону проходить через стены и преграды, что увеличивает дальность соединения.
* *Недостатки*: Диапазон более подвержен помехам, так как используется многими устройствами (микроволновыми печами, Bluetooth-устройствами и пр.). Кроме того, в нем меньше каналов, что может приводить к перегрузке.
* *Скорость*: В диапазоне 2,4 ГГц максимальная скорость ниже, чем в 5 ГГц. Стандарт 802.11n может обеспечивать скорость до 600 Мбит/с, но в реальных условиях скорость обычно ниже.

***Диапазон 5 ГГц:***

* *Преимущества*: Этот диапазон имеет более высокую пропускную способность и меньше подвержен помехам из-за наличия большего количества каналов. Благодаря этому в 5 ГГц можно достичь более высокой скорости передачи данных.
* *Недостатки*: Более короткие радиоволны плохо проходят через стены и преграды, что снижает дальность соединения по сравнению с 2,4 ГГц.
* *Скорость*: В диапазоне 5 ГГц поддерживаются более высокие скорости (до 1300 Мбит/с по стандарту 802.11ac и выше в более новых стандартах, таких как Wi-Fi 6 и Wi-Fi 6E).

***Влияние частоты на дальность и скорость соединения***

* Дальность: Чем ниже частота, тем дальше распространяется сигнал. Поэтому диапазон 2,4 ГГц обеспечивает большее покрытие, особенно в условиях наличия препятствий (стены, мебель и т.д.), тогда как 5 ГГц лучше подходит для небольших пространств с прямой видимостью между устройствами.
* Скорость: Диапазон 5 ГГц обеспечивает более высокие скорости передачи данных благодаря большей пропускной способности и меньшему количеству помех. Однако, на больших расстояниях или при наличии препятствий скорость 5 ГГц быстро падает.

Таким образом, диапазон 2,4 ГГц оптимален для увеличенной дальности, а 5 ГГц — для более высокой скорости в условиях прямой видимости и малых расстояний. Современные двухдиапазонные роутеры автоматически переключаются между диапазонами для достижения наилучших характеристик связи.

# **Какие меры безопасности обеспечивает Wi-Fi, и как можно защитить беспроводную сеть от несанкционированного доступа?**

Wi-Fi-сети обладают рядом встроенных мер безопасности, обеспечивающих защиту данных и предотвращение несанкционированного доступа. Основные протоколы безопасности включают:

1. **WEP (Wired Equivalent Privacy)** — ранний стандарт, который уже считается устаревшим из-за уязвимостей. Он использует статический ключ для шифрования, что делает его недостаточно надежным для современных требований безопасности.
2. **WPA (Wi-Fi Protected Access)** и его улучшенная версия **WPA2** — более безопасные протоколы. WPA использует динамические ключи, обеспечивая более надежное шифрование, а WPA2, в дополнение к этому, использует шифрование AES (Advanced Encryption Standard), что делает его устойчивым к большинству атак. В 2018 году был также разработан **WPA3**, который обеспечивает дополнительные меры защиты, такие как более безопасная аутентификация и шифрование данных, даже если пароль является слабым.

Для защиты беспроводной сети от несанкционированного доступа можно применить следующие меры:

1. **Настройка надежного пароля** для Wi-Fi. Пароль должен быть длинным и содержать символы, цифры и буквы разного регистра, чтобы его было сложно подобрать.
2. **Выбор WPA2 или WPA3** в качестве протокола безопасности. Эти протоколы обеспечивают максимальную защиту для большинства маршрутизаторов.
3. **Отключение трансляции SSID** (имени сети) скрывает сеть от других пользователей, не позволяя ее случайно обнаружить. Хотя это не предотвращает все попытки доступа, оно добавляет дополнительный уровень защиты.
4. **Использование фильтрации по MAC-адресам** позволяет вручную указать, какие устройства могут подключаться к сети, что ограничивает доступ посторонних.
5. **Регулярное обновление прошивки маршрутизатора**. Обновления прошивки могут содержать исправления уязвимостей и улучшения безопасности.
6. **Ограничение мощности сигнала** Wi-Fi так, чтобы его радиус охвата не выходил за пределы помещения, уменьшает вероятность перехвата сигнала за пределами защищенной зоны.

Эти меры позволяют повысить безопасность сети и минимизировать риск несанкционированного доступа и кражи данных.

# **Что представляют собой сокеты в контексте сетевого программирования, и какие основные функции они выполняют?**

Сокет — это программный интерфейс, который позволяет обеспечивать связь между различными компьютерами в компьютерной сети.

Можно представить, что сокет — это виртуальная труба, которую строят между двумя приложениями, чтобы гонять между ними данные. Приложения видят только концы трубы, а как проходит трубопровод — они не знают и им неважно.

Сокеты используют для двух вещей:

* для передачи данных по сети;
* и для связи между приложениями.

Сокеты работают посредством двух основных протоколов: протоколы TCP (Transmission Control Protocol) и UDP (User Datagram Protocol). TCP обеспечивает надежную доставку данных и устанавливает стабильное соединение между отправителем и получателем. UDP, в свою очередь, работает без установления соединения и обеспечивает быструю передачу данных.

Сокеты работают по принципу передачи данных через IP-адреса и порты. Каждый сокет идентифицируется комбинацией IP-адреса и порта, что обеспечивает уникальность подключения. Клиентское приложение устанавливает соединение с сервером, указывая его IP-адрес и порт. Затем сервер принимает соединение, и между ними устанавливается канал для обмена информацией.

# **Какие типы сокетов существуют, и в чем основные различия между ними?**

1. TCP сокеты

TCP (Transmission Control Protocol) сокеты используются для установления надежного и устойчивого соединения между клиентом и сервером. Они обеспечивают проверку доставки данных, управление потоком данных и гарантированную доставку пакетов в правильном порядке.

2. UDP сокеты

UDP (User Datagram Protocol) сокеты работают на более низком уровне, обеспечивая ненадежную и безгарантированную передачу данных. Они часто используются для передачи данных в реальном времени, таких как видео и аудиопотоки, где скорость передачи данных важнее, чем надежность.

3. RAW сокеты

RAW сокеты предоставляют доступ к сырым сетевым пакетам без обработки стеком протоколов. Они позволяют осуществлять полный контроль над данными, включая заголовки пакетов, и могут использоваться для различных сетевых задач, таких как сканирование портов или анализ сетевого трафика.

4. Unix доменные сокеты

Unix доменные сокеты предназначены для взаимодействия между различными процессами на одном компьютере. Они работают на уровне файловой системы Unix и обеспечивают быструю и безопасную передачу данных между процессами без использования сети.

5. Bluetooth сокеты

Bluetooth сокеты используются для передачи данных по беспроводному интерфейсу Bluetooth между устройствами. Они позволяют установить соединение и обмениваться данными на короткие расстояния, что делает их идеальным выбором для мобильных устройств и периферийного оборудования.

# **Каковы преимущества использования сокетов в сравнении с другими методами взаимодействия между приложениями через сеть?**

**1. Гибкость и контроль**

Настройка соединения: Сокеты позволяют разработчикам настраивать параметры соединения, такие как тайм-ауты, режимы передачи данных (например, потоковая или датаграммная) и другие параметры.

Протоколы: Вы можете использовать сокеты с различными протоколами (TCP, UDP и др.), что дает возможность оптимизировать взаимодействие под конкретные задачи.

**2. Производительность**

Низкий уровень абстракции: Сокеты обеспечивают более низкий уровень абстракции, что позволяет избежать дополнительных накладных расходов, связанных с высокоуровневыми протоколами.

Быстрая передача данных: В случае TCP-сокетов, данные передаются последовательно и надежно, что может быть более эффективным для приложений, требующих высокой производительности.

**3. Двусторонняя связь**

Дуплексное соединение: Сокеты поддерживают двустороннюю связь, что позволяет обеим сторонам отправлять и получать данные одновременно без необходимости устанавливать отдельные соединения.

**4. Асинхронность**

Неп блокирующий ввод-вывод: Сокеты могут использоваться в асинхронном режиме, что позволяет приложениям не блокироваться во время ожидания данных, улучшая отзывчивость и производительность.

**5. Поддержка различных типов взаимодействия**

Многочисленные клиенты: Сокеты позволяют легко реализовывать серверные приложения, которые могут обрабатывать несколько клиентов одновременно.

Разнообразие типов данных: Вы можете передавать любые типы данных, включая текстовые и бинарные, без ограничений, налагаемых на высокоуровневые протоколы.

**6. Кроссплатформенность**

Поддержка различных ОС: Сокеты поддерживаются практически во всех операционных системах и языках программирования, что делает их универсальным решением для сетевого взаимодействия.

**7. Открытость и стандартность**

Широкая поддержка: Сокеты являются стандартным механизмом для сетевого взаимодействия и имеют обширную документацию и примеры, что упрощает их использование.

# **Какие технологии и протоколы можно использовать в сочетании с сокетами для реализации различных видов сетевого взаимодействия?**

|  |  |  |
| --- | --- | --- |
| **Технология/Протокол** | **Уровень модели OSI** | **Основные Применения** |
| **TCP (Transmission Control Protocol)** | Транспортный | Основной протокол для надёжной передачи данных, используется в веб-серверах, базах данных. |
| **UDP (User Datagram Protocol)** | Транспортный | Быстрая передача данных без подтверждения, подходит для видеопотоков, онлайн-игр. |
| **IP (Internet Protocol)** | Сетевой | Базовый протокол для маршрутизации данных между устройствами, основа для всех сетевых взаимодействий. |
| **HTTP/HTTPS (Hypertext Transfer Protocol)** | Прикладной | Передача данных для веб-приложений. HTTPS обеспечивает шифрование. |
| **WebSocket** | Прикладной | Постоянное соединение для обмена данными в реальном времени, используется для чатов и уведомлений. |
| **MQTT (Message Queuing Telemetry Transport)** | Прикладной | Лёгкий протокол обмена данными для IoT, поддерживает асинхронное взаимодействие. |
| **SSH (Secure Shell)** | Управление соединением | Защищённый удалённый доступ и передача команд. |
| **SSL/TLS** | Управление соединением | Шифрование для защиты соединений (например, HTTPS). |
| **DNS (Domain Name System)** | Приложение | Преобразует доменные имена в IP-адреса. |

# **Стандарт IEEE 802.15.4**

EEE 802.15.4 — это стандарт для беспроводных персональных сетей (WPAN) с низкой скоростью передачи данных, разработанный для применения в устройствах с низким энергопотреблением и увеличенным сроком службы, таких как датчики и устройства интернета вещей (IoT). Этот стандарт используется в приложениях для мониторинга и управления, где предпочтительны невысокие скорости и энергоэффективность.

Основные особенности IEEE 802.15.4:

1. **Уровни PHY и MAC**: Стандарт определяет физический (PHY) и уровень управления доступом к среде (MAC), где PHY задает частоту, мощность и модуляцию, а MAC — обработку данных. Эти уровни обеспечивают взаимодействие с верхними уровнями других протоколов.
2. **Частотные диапазоны**: Поддерживает частоты 2,4 ГГц, 915 МГц и 868 МГц, из которых 2,4 ГГц наиболее распространена благодаря доступности чипов и модулей.
3. **Модуляция и защита от помех**: Использует модуляцию DSSS (модуляция с расширенным спектром прямой последовательности), которая устойчивее к шуму. В стандарте применяются BPSK для низких скоростей и O-QPSK для высокой скорости передачи данных, что снижает энергопотребление.
4. **Доступ к каналу**: Для передачи данных применяется многостанционный доступ CSMA-CA, который снижает вероятность конфликтов. Данные передаются короткими пакетами, что снижает энергопотребление за счет минимального рабочего цикла.

Дальность и мощность

Стандарт определяет мощность передачи на уровне –3 дБм (0,5 мВт) и до 20 дБм (100 мВт) для усиленных модулей, с дальностью до 1000 метров в условиях прямой видимости (LOS), но чаще используется на расстояниях от 10 до 75 метров.

IEEE 802.15.4 предоставляет базовую платформу для создания сетей, к которой могут добавляться верхние уровни протоколов, такие как Zigbee, 6LoWPAN и другие, ориентированные на разные типы IoT-систем.

# **Что такое нуль-модемное соединение, и как оно отличается от обычного последовательного соединения?**

**Нуль-модемное соединение**  — соединение двух [компьютерных устройств](https://ru.ruwiki.ru/wiki/%D0%9E%D0%BA%D0%BE%D0%BD%D0%B5%D1%87%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%BE%D1%80%D1%83%D0%B4%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85) по интерфейсу [RS-232](https://ru.ruwiki.ru/wiki/RS-232) без [модема](https://ru.ruwiki.ru/wiki/%D0%9C%D0%BE%D0%B4%D0%B5%D0%BC).

В нуль-модемном соединении линии передачи и приёма соединены непосредственно, [крест-накрест](https://ru.ruwiki.ru/wiki/%D0%9A%D1%80%D0%BE%D1%81%D1%81%D0%BE%D0%B2%D0%B5%D1%80%D0%BD%D1%8B%D0%B9_%D0%BA%D0%B0%D0%B1%D0%B5%D0%BB%D1%8C), без использования модемов. Нуль-модемное соединение не [стандартизовано](https://ru.ruwiki.ru/wiki/%D0%A1%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F), поэтому существуют несколько разводок.

Нуль-модемное соединение — это тип последовательного соединения, при котором для связи двух компьютеров напрямую используется кабель без модемов или других промежуточных устройств. Такое подключение имитирует связь через модем, но без его участия, и осуществляется с использованием обычного последовательного порта (например, RS-232) на каждом устройстве.

Отличия от обычного последовательного соединения

1. **Прямая связь без модема**: В обычном последовательном соединении для передачи данных используются модемы, которые модулируют и демодулируют сигнал. Нуль-модемное соединение исключает модем и передает данные напрямую между компьютерами.
2. **Перекрестная распайка проводов**: Нуль-модемный кабель включает перекрестное подключение передающих и принимающих линий, что позволяет устройствам общаться напрямую. В обычном последовательном кабеле линии подключения идут параллельно, поскольку модемы на каждом конце обрабатывают сигнал.
3. **Назначение и область применения**: Нуль-модемные соединения используются для связи между двумя компьютерами или устройствами на небольших расстояниях, например, для передачи файлов, обновлений прошивок или совместного использования данных. Обычное последовательное соединение чаще применяется для связи компьютера с периферийными устройствами, такими как принтеры или сканеры, а также для удаленных соединений через модем.
4. **Протоколы управления потоком**: Нуль-модемное соединение может использовать аппаратное (DTR/DSR, RTS/CTS) или программное управление потоком (XON/XOFF), чтобы согласовывать передачу данных между устройствами напрямую, в отличие от последовательного соединения, где модемы обеспечивают контроль и модуляцию сигнала.

# **Bluetooth Low Energy (BLE)**

Bluetooth Low Energy (BLE) - это технология беспроводной связи с низким энергопотреблением для обмена данными на небольших расстояниях. Она была создана для устройств, которым необходимо длительный период времени поддерживать между собой связь.

Обычный Bluetooth подходит для непрерывной обработки, передачи и обмена больших объемов данных (например, аудио). Однако он потребляет больше энергии и в конечном итоге стоит дороже. В BLE данные передаются короткими пакетами, после чего передатчик отключается - именно по такому принципу удается добиться низкого потребления энергии. И, в отличие от классического Bluetooth, устройства с BLE связываются друг с другом лишь для того, чтобы отправить или получить информацию.

Низкое энергопотребление - это основное преимущество Bluetooth Low Energy. Как правило, BLE потребляет в десятки раз меньше энергии, чем Bluetooth. Это значительно экономит заряд аккумуляторов устройств. Технология проста в развертывании и использует для работы тот же диапазон, что и обычный Bluetooth.

# **\*Интерфейс IEEE 1284**

**LPT (IEEE 1284)** (Line Print Terminal) - параллельный порт, порт для подключения принтера. Является международным стандартом параллельного интерфейса, предназначенного для подключения периферийных устройств ПК.

В основном используется для подключения принтера, сканера и прочих внешних устройств, в том числе и устройств хранения данных. Кроме того, данный интерфейс может использоваться и для осуществления связи между двумя компьютерами, создания телесигнализации.

Стандарт LPT построен на базе интерфейса Centronics и его расширенных версий (ECP, EPP).

Имя «LPT» является образованием от имени стандартного устройства принтера «LPT1» (Line Printer Terminal/Line PrinTer), которое используется в ОС MS-DOS.

# **\*Интерфейс RS-232-С**

RS-232 - является дуплексным интерфейсом с последовательной передачей данных в асинхронном и синхронном режимах со скоростью до 115 Кбит/сек и топологией «точка-точка».

Интерфейс RS-232 чаще всего использовался для подключения различного типа манипуляторов, для связи двух компьютеров, подключения принтеров и плоттеров, а также электронных ключей (Security Devices), предназначенных для защиты от нелицензированного использования программного обеспечения. Этот интерфейс позволяет эмулировать специальные терминалы (UT-52, UT-100 и т.д.). Он используется для беспроводных коммуникаций с применением излучателей и приемников инфракрасного диапазона - IR Connection.