ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ
БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
**ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ**

А. В. Росляков, С. В. Ваняшин, А. Ю. Гребешков

ИНТЕРНЕТ ВЕЩЕЙ

Учебное пособие

Самара – 2015

Поволжский государственный университет телекоммуникаций и информатики

А.В. Росляков, С.В. Ваняшин, А.Ю. Гребешков

ИНТЕРНЕТ ВЕЩЕЙ

Учебное пособие

Самара
2015

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования «ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ»

Кафедра автоматической электросвязи

А.В. Росляков, С.В. Ваняшин, А.Ю. Гребешков

ИНТЕРНЕТ ВЕЩЕЙ

Учебное пособие по направлению подготовки «Инфокоммуникационные технологии и системы связи» 11.03.02 - бакалавриат и 11.04.02 - магистратура

Самара
2015

УДК 004.738.5: 621.391
ББК
Р75

Рекомендовано к изданию методическим советом ПГУТИ
протокол №5 от 19.03.2015г.

Рецензия ФГОБУ ВПО МТУСИ, зарегистрированная в ФГОБУ ВПО МГУП №2974 от 03.02.2015

Росляков, А.В.

Р75 Интернет вещей: учебное пособие [текст] / А.В. Росляков, С.В. Ваняшин, А.Ю. Гребешков. – Самара: ПГУТИ, 2015. – 200 с.

В учебном пособии систематизированы сведения, стандарты и подходы к технической реализации концепции Интернета вещей (Internet of Things, IoT), а также смежных с ним инфокоммуникационных технологий (радиочастотной идентификации RFID, беспроводным сенсорным сетям WSN, межмашинным коммуникациям M2M). Рассмотрены протоколы и технологии передачи данных, приведены многочисленные примеры практической реализации Интернета вещей.

Пособие предназначено для бакалавров и магистров, обучающихся по направлению «Инфокоммуникационные технологии и системы связи», а также полезно для студентов, обучающихся по следующим направлениям: «Информатика и вычислительная техника», «Информационные системы и технологии», «Интеллектуальные системы в гуманитарной сфере», «Прикладная информатика

ВВЕДЕНИЕ

Идея Интернета вещей сама по себе очень проста. Представим, что все окружающие нас предметы и устройства (домашние приборы и утварь, одежда, продукты, автомобили, промышленное оборудование и др.) снабжены миниатюрными идентификационными и сенсорными (чувствительными) устройствами. Тогда при наличии необходимых каналов связи с ними можно не только отслеживать эти объекты и их параметры в пространстве и во времени, но и управлять ими, а также включать информацию о них в общую «умную планету». В самом общем виде с инфокоммуникационной точки зрения Интернет вещей можно записать в виде следующей символической формулы:

IoT = Сенсоры (датчики) + Данные + Сети + Услуги.

Проще говоря, Интернет вещей – это глобальная сеть компьютеров, датчиков (сенсоров) и исполнительных устройств (актуаторов), связывающихся между собой с использованием интернет протокола IP (Internet Protocol). Например, для решения определенной задачи компьютер связывается через публичный интернет с небольшим устройством, к которому подключен соответствующий датчик (например, температуры), как это показано на рисунке.

Очевидно, что при внедрении Интернета вещей вся наша повседневная жизнь кардинально изменится. Уйдут в прошлое поиски нужных вещей, дефициты товаров или их перепроизводство, кражи автомобилей и мобильных телефонов, поскольку будет точно известно, что, в каком месте и в каком количестве находится, производится и потребляется. Если все объекты (вещи) будут снабжены миниатюрными радиометками, то их можно будет дистанционно идентифицировать, а при наличии определенного «интеллекта» – и управлять ими. По оценкам экспертов компании Cisco количество объектов, которые Интернет вещей сможет соединить между собой, будет сравнимо с количеством атомов на поверхности Земли.

Концепция IoT играет определяющую роль в дальнейшем развитии инфокоммуникационной отрасли. Это подтверждается как позицией Международного союза электросвязи (МСЭ) и Европейского Союза в данном вопросе, так и включением Интернета вещей в перечень прорывных технологий в США, Китае и других странах. И хотя на международном уровне данная концепция уже обретает черты сформировавшейся технологии, для нее ведутся активные работы в области стандартизации архитектуры, технических компонентов, приложений, но одновременно столь же велико количество мнений о том, как именно будет построен Интернет вещей.

В учебном пособии систематизированы многочисленные сведения, стандарты и подходы к технической реализации концепции Интернета вещей (Internet of Things, IoT), а также смежных с ним инфокоммуникационных технологий (радиочастотной идентификации RFID, беспроводным сенсорным сетям WSN, межмашинным коммуникациям M2M). Рассмотрены протоколы и технологии передачи данных, приведены многочисленные примеры практической реализации Интернета вещей.

Пособие предназначено для бакалавров и магистров, обучающихся по направлению «Инфокоммуникационные технологии и системы связи». Оно может быть также полезно для

студентов, обучающихся по следующими направлениям: «Информатика и вычислительная техника», «Информационные системы и технологии», «Интеллектуальные системы в гуманитарной сфере», «Прикладная информатика».

ГЛАВА 1 ОБЩИЕ ПОЛОЖЕНИЯ ИНТЕРНЕТА ВЕЩЕЙ

1.1 Что такое Интернет вещей?

В связи с бурным развитием сетей с пакетной коммутацией и прежде всего Интернета в начале 2000-х годов мировое телекоммуникационное сообщество сначала выработало, а затем и приступило к реализации новой парадигмы развития коммуникаций – сетей следующего поколения NGN (Next Generation Networks). Технологии NGN уже прошли эволюционный путь развития от гибких коммутаторов (Softswitch) до подсистем мультимедийной связи IMS (IP Multimedia Subsystem) и беспроводных сетей долговременной эволюции LTE (Long Term Evolution). При этом всегда предполагалось, что основными пользователями сетей NGN будут люди и, следовательно, максимальное число абонентов в таких сетях всегда будет ограничено численностью населения планеты Земля.

Однако в последнее время значительное развитие получили методы радиочастотной идентификации RFID (Radio Frequency IDentification), беспроводные сенсорные сети WSN (Wireless Sensor Network), коммуникации малого радиуса действия NFC (Near Field Communication) и межмашинные коммуникации M2M (Machine-to-Machine), которые, интегрируясь с интернет, позволяют обеспечить простую связь различных технических устройств («вещей»), число которых может быть огромным. По расчетам консалтингового подразделения Cisco IBSG в промежутке между 2008 и 2009 годами количество подключенных к интернету предметов превысило количество людей, к 2015 году количество подключенных устройств достигнет 25 миллиардов, а к 2020 году – 50 миллиардов (рис. 1.1). Таким образом, в настоящее время происходит эволюционный переход от «Интернета людей» к «Интернету вещей», IoT (Internet of Things).

В общем случае под Интернетом вещей понимается совокупность разнообразных приборов, датчиков, устройств, объединённых в сеть посредством любых доступных каналов связи, использующих различные протоколы взаимодействия между собой и единственный протокол доступа к глобальной сети. В роли глобальной сети для Интернет-вещей в настоящий момент используется сеть Интернет. Общим протоколом является IP.

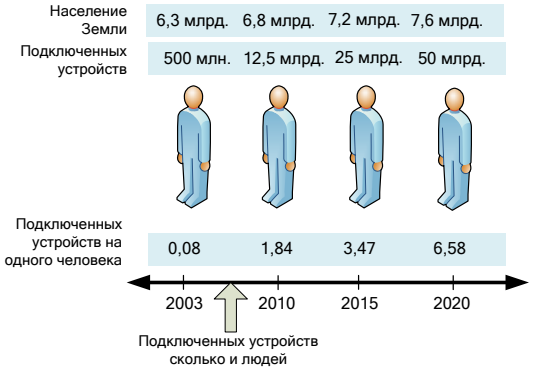


Рис. 1.1 – Временная шкала изменения количества людей и предметов, подключенных к интернет (источник: Cisco IBSG, 2011)

Следует особо отметить, что Интернет вещей не исключает участие человека. IoT не полностью автоматизирует вещи, так как он ориентирован на человека и предоставляет ему возможность доступа к вещам. Но многие вещи смогут вести себя иначе, чем мы представляем себе сегодня. В IoT каждая вещь имеет свой уникальный идентификатор, которые совместно образуют континуум вещей, способных взаимодействовать друг с другом, создавая временные или постоянные сети. Так вещи могут принимать участие в процессе их перемещения, делясь сведениями о текущей геопозиции, что позволяет полностью автоматизировать процесс логистики, а имея встроенный интеллект, вещи могут менять свои свойства и адаптироваться к окружающей среде, в том числе для уменьшения

энергопотребления. Они могут обнаруживать другие, так или иначе связанные с ними вещи, и налаживать с ними взаимодействие. IoT позволяет создавать комбинацию из интеллектуальных устройств, объединенных сетями связи, и людей. Совместно они могут создавать самые разнообразные системы, например, для работы в средах, неудобных или недоступных для человека (в космосе, на большой глубине, на ядерных установках, в трубопроводах и т.п.).

Считается, что первую в мире интернет-вещь создал один из отцов протокола TCP/IP Джон Ромки в 1990 году, когда он подключил к сети свой тостер. Но только в 21 веке в связи с бурным развитием инфокоммуникационных технологий сформировалась концепция IoT и получила свое практическое воплощение. Процесс развития Интернета вещей проиллюстрирован технологической дорожной картой, приведенной на рис. 1.2. Все началось с необходимости оптимизации системы логистики и управления системой снабжения предприятий. Вторая волна инноваций была обусловлена необходимостью сокращения затрат в системах наблюдения, безопасности, транспорта и др. Третья была вызвана потребностью в геолокационных сервисах. Четвертая волна будет обусловлена необходимостью дистанционного присутствия человека на месте совершения требующего его внимания событий, которое станет возможным благодаря миниатюрным встроенным процессорам. А следующим шагом будет возможность создания будущих сетей (Future Networks) с ячеистой топологией, включающих в себя метки, датчики, средства измерения и управляющие устройства.

Рис. 1.2 – Технологическая дорожная карта Интернета вещей (источник: SRI Consulting Business Intelligence)

С развитием Интернета вещей все больше предметов будут подключаться к глобальной сети, тем самым создавая новые возможности в сфере безопасности, аналитики и управления, открывая все новые и более широкие перспективы и способствуя повышению качества жизни населения. Предполагается, что в будущем «вещи» станут активными участниками бизнеса, информационных и социальных процессов, где они смогут взаимодействовать и общаться между собой, обмениваясь информацией об окружающей среде, реагируя и влияя на процессы, происходящие в окружающем мире, без вмешательства человека.

1.2 Базовые принципы IoT

Интернет вещей основывается на трех базовых принципах. Во-первых, повсеместно распространенную коммуникационную инфраструктуру, во-вторых, глобальную идентификацию каждого объекта и, в-третьих, возможность каждого объекта отправлять и получать данные посредством персональной сети или сети Интернет, к которой он подключен.

Наиболее важными отличиями Интернета вещей от существующего интернета людей являются:

– фокус на вещах, а не на человеке;

– существенно большее число подключенных объектов;

– существенно меньшие размеры объектов и невысокие скорости передачи данных;

– фокус на считывании информации, а не на коммуникациях;

– необходимость создания новой инфраструктуры и альтернативных стандартов.

Концепция сетей следующего поколения NGN предполагала возможность коммуникаций людей (непосредственно или через компьютеры) в любое время и в любой точке пространства. Концепция Интернета вещей включает еще одно направление – коммуникация любых устройств или вещей (рис. 1.3).

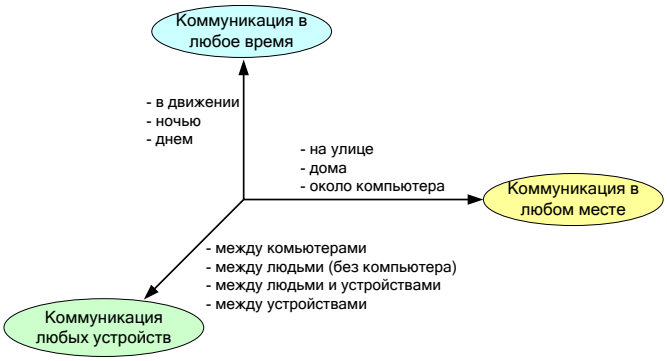


Рис. 1.3 – Новое направление коммуникаций, реализуемое Интернетом вещей (источник: МСЭ-Т Y.2060)

Концепция IoT и термин для неё впервые сформулированы основателем исследовательской группы Auto-ID при Массачусетском технологическом институте Кевином Эштоном в 1999 году на презентации для руководства компании Procter & Gamble. В презентации рассказывалось о том, как всеобъемлющее внедрение радиочастотных меток RFID сможет видоизменить систему управления логистическими цепями в корпорации.

Официальное определение Интернета вещей приведено в Рекомендации МСЭ-Т Y.2060, согласно которому IoT – глобальная инфраструктура информационного общества, обеспечивающая передовые услуги за счет организации связи между вещами (физическими или виртуальными) на основе существующих и развивающихся совместимых информационных и коммуникационных технологий.

Под «вещами» (things) здесь понимается физический объект (физическая вещь) или объект виртуального (информационного) мира (виртуальная вещь, например мультимедийный контент или прикладная программа), которые могут быть идентифицированы и объединены через коммуникационные сети.

Кроме понятия «вещь», МСЭ-Т также использует понятие «устройство» (device), под которым понимается часть оборудования с обязательными возможностями по коммуникации и необязательными возможностями по сенсорингу/зондированию, приведению в действие вещи, сбору, обработке и хранению данных. Отсюда следует, что МСЭ-Т в большей степени уделяет вниманию аспектам коммуникаций и межсоединений, нежели приложениям IoT.

Схема отображения физических и виртуальных вещей представлена на рис. 1.4. Из рисунка следует, что виртуальные вещи могут существовать без их физических воплощений, в то время как физическим объектам/вещам обязательно соответствует минимум один виртуальный объект. При этом ведущую роль играют именно устройства, которые могут собирать различную информацию и распространять её по коммуникационным сетям различными способами: через шлюзы и через сеть; без шлюзов, но через сеть; напрямую между собой. Рекомендация Y.2060 описывает различное сочетание перечисленных

способов соединений. Это указывает на то, что МСЭ-Т предусматривает использование для IoT множества сетевых технологий – глобальных сетей, локальных сетей, беспроводных самоорганизующихся (ad-hoc) и ячеистых (mesh) сетей. Указанные сети связи переносят данные, собранные устройствами, к соответствующим программным приложениям, а также передают команды от программных приложений к устройствам.

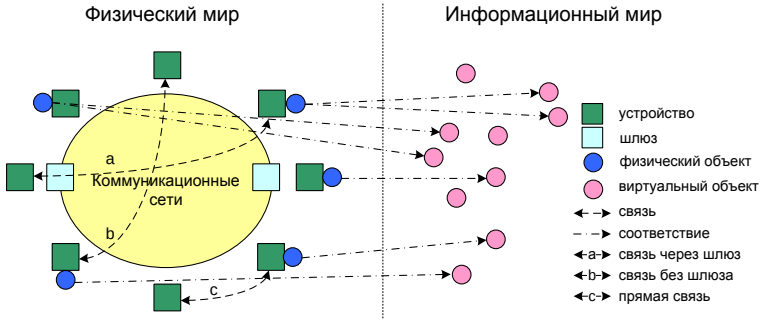


Рис. 1.4 – Схема отображения физических и виртуальных вещей (источник: МСЭ-Т Y.2060)

Следует отметить, что вещи и связанные с ними устройства могут обладать полноценными управляющими процессорами для обработки данных в виде «системы-на-кристалле», в том числе с собственной операционной системой, блоком сенсоринга/зондирования окружающей среды и блоком коммуникации.

Следует различать понятия «Интернет вещей» и «интернет-вещь». Под интернет-вещью понимается любое устройство, которое:

– имеет доступ к сети Интернет с целью передачи или запроса каких-либо данных,

– имеет конкретный адрес в глобальной сети или идентификатор, по которому можно осуществить обратную связь с вещью,

– имеет интерфейс для взаимодействия с пользователем.

Интернет-вещи имеют единый протокол взаимодействия, согласно которому любой узел сети равноправен в предоставлении своих сервисов. На пути перехода к воплощению идеи Интернета вещей стояла проблема, связанная с протоколом IPv4, ресурс свободных сетевых адресов которого уже практически исчерпал себя. Однако подготовка к повсеместному внедрению версии протокола IPv6 позволяет решить эту проблему и приближает идею Интернета вещей к реальности.

Каждый узел сети интернет-вещей предоставляет свой сервис, оказывая некую услугу поставки данных. В то же время узел такой сети может принимать команды от любого другого узла. Это означает, что все интернет-вещи могут взаимодействовать друг с другом и решать совместные вычислительные задачи. Интернет-вещи могут образовывать локальные сети, объединённые какой-либо одной зоной обслуживания или функцией.

1.3 Стандартизация IoT

Вопросами стандартизации и практического внедрения отдельных составляющих Интернета вещей (M2M, RFID, всепроникающие сенсорные сети и др.) занимаются многие международные организации, неправительственные ассоциации, альянсы производителей и операторов, партнерские проекты. В целом для Интернета вещей, как нового направления развития инфокоммуникаций, в настоящее время определены самые общие концептуальные и архитектурные решения. В ближайшее время основной проблемой будет гармонизации различных стандартов с целью формирования единой и непротиворечивой нормативной базы для практической реализации Интернета вещей.

В рамках деятельности сектора стандартизации телекоммуникаций Международного союза электросвязи (МСЭ-Т) имеются три глобальных инициативы GSI (Global Standards

Initiative). Под глобальной инициативой понимается комплекс работ, выполняемых параллельно разными исследовательскими комиссиями МСЭ в соответствии со скоординированным планом работы. Одна из таких инициатив посвящена стандартизации Интернета вещей – IoT-GSI (Global Standards Initiative on Internet of Things). Две другие глобальные инициативы – по стандартизации сетей последующих поколений NGN-GSI и систем телевидения на основе протокола Интернет IPTV-GSI – также базируются на использовании IP-технологий, как и IoT-GSI.

IoT-GSI строит свою работу на основе усилий МСЭ-Т в таких областях, как сетевые аспекты идентификационных систем (Network Identificator, NID), всепроникающие сенсорные сети (Ubiquitous Sensor Networks, USN), межмашинная связь (M2M), WEB вещей (WoT) и т.п. В рамках серии МСЭ-Т Y.2xxx, посвященной сетям следующего поколения NGN, уже утверждены первые рекомендации, посвященные специально Интернету вещей: Y.2060 «Обзор Интернета вещей», Y.2063 «Основа WEB вещей» и Y.2069 «Термины и определения Интернета вещей» и др.

В Рекомендации Y.2060 приведена эталонная модель IoT, которая очень похожа на модель NGN и также включает четыре базовых горизонтальных уровня (рис. 1.5):

- уровень приложений IoT;
- уровень поддержки приложений и услуг;
- сетевой уровень;
- уровень устройств.

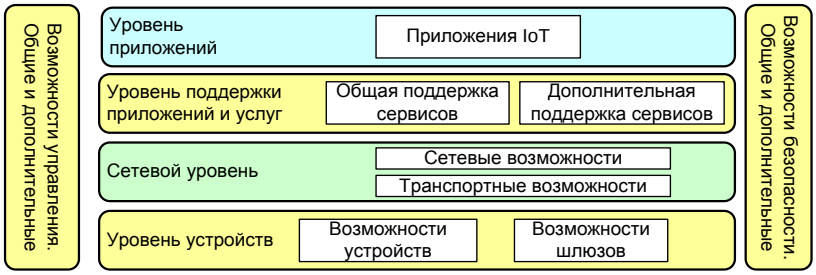


Рис. 1.5 – Эталонная модель IoT согласно МСЭ-Т Y.2060

Уровень приложений IoT в Рекомендации Y.2060 детально не рассматривается. Уровень поддержки приложений и услуг включает общие возможности для различных объектов IoT по обработке и хранению данных, а также возможности, необходимые для некоторых приложений IoT или групп таких приложений. Сетевой уровень включает сетевые возможности (функция управления ресурсами сети доступа и транспортной сети, управления мобильностью, функции авторизации, аутентификации и расчетов, AAA) и транспортные возможности (обеспечение связности сети для передачи информации приложений и услуг IoT). Наконец, уровень устройств включает возможности устройства и возможности шлюза. Возможности устройства предполагают прямой обмен с сетью связи, обмен через шлюз, обмен через беспроводную динамическую ad-hoc сеть, а также временный останов и возобновление работы устройства для энергосбережения. Возможности шлюза предполагают поддержку множества интерфейсов для устройств (шина CAN, ZigBee, Bluetooth, WiFi и др.) и для сетей доступа/транспортных сетей (2G/3G, LTE, DSL и др.). Другой возможностью шлюза является поддержка конверсии протоколов, в случае, если протоколы интерфейсов устройств и сетей отличаются друг от друга.

Существует также два вертикальных уровня – уровень управления и уровень безопасности, охватывающие все четыре горизонтальных уровня. Возможности вертикального уровня эксплуатационного управления предусматривают управление последствиями отказов, возможностями сети, конфигурацией, безопасностью и данными для биллинга. Основными объектами управления являются устройства, локальные сети и их

топология, трафик и перегрузки на сетях. Возможности вертикального уровня безопасности зависят от горизонтального уровня. Для уровня поддержки приложений и услуг определены функции AAA, антивирусная защита, тесты целостности данных. Для сетевого уровня – возможности авторизации, аутентификации, защиты информации протоколов сигнализации. На уровне устройств – возможности авторизации, аутентификации, контроль доступа и конфиденциальность данных.

Основной целью проекта Европейского интеграционного проекта IoT-A (Internet of Things – Architecture), участниками которого являются различные компании, является разработка эталонной архитектурной модели Интернета вещей с описанием основных составляющих компонентов, которая бы позволила интегрировать разнородные технологии IoT в единую взаимосвязанную архитектуру.

Функциональная модель IoT-A (рис. 1.6) несколько отличается от модели МСЭ (см. рис. 1.5), хотя она тоже является иерархической, но состоит уже из семи горизонтальных уровней, дополняемых двумя вертикальными (управление и безопасность), которые участвуют во всех процессах.

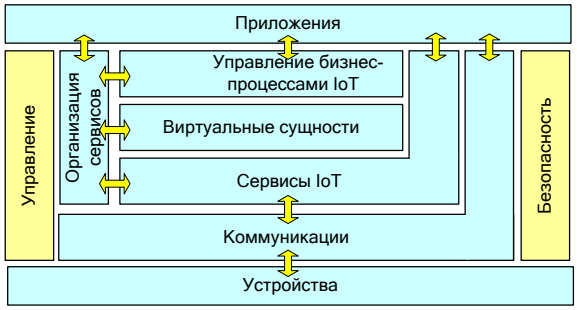


Рис. 1.6 – Функциональная модель архитектуры IoT-A

Если обратиться к техническим особенностям модели на рис. 1.7, то можно сказать, что модель передачи данных в Интернете вещей IoT-A будет отличаться от существующей модели передачи данных через Интернет. В модели архитектуры IoT-A фигурируют два важных понятия. Сеть с ограничениями характеризуется относительно низкими скоростями передачи – менее 1 Мбит (например, стандарт IEEE 802.15.4) и достаточно высокими задержками. Сеть без ограничений соответственно характеризуется высокими скоростями передачи данных (десятки Мбит/с и более) и похожа на существующую сеть Интернет. Различие данных моделей сетей показано на рис. 1.7.

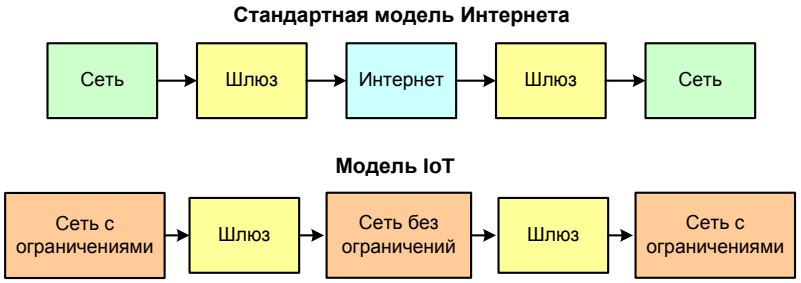


Рис. 1.7 – Сравнение моделей передачи данных в Интернете и в IoT

1.4 Архитектура IoT

Интернет вещей концептуально принадлежит к сетям следующего поколения, поэтому его архитектура во многом схожа с известной четырехслойной архитектурой NGN. IoT состоит из набора различных инфокоммуникационных технологий, обеспечивающих функционирование Интернета вещей, и его архитектура показывает, как эти технологии

связаны друг с другом. Архитектура IoT включает четыре функциональных уровня (рис. 1.8), описанных ниже.

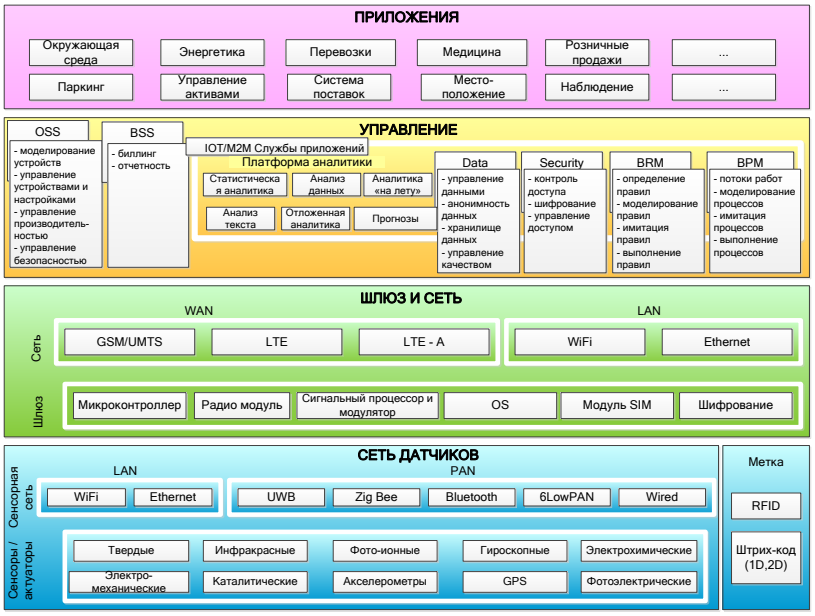


Рис. 1.8 – Архитектура IoT

1. *Уровень сенсоров и сенсорных сетей.*

Самый нижний уровень архитектуры IoT состоит из «умных» (smart) объектов, интегрированных с сенсорами (датчиками). Сенсоры реализуют соединение физического и виртуального (цифрового) миров, обеспечивая сбор и обработку информации в реальном масштабе времени. Миниатюризация, приведшая к сокращению физических размеров аппаратных сенсоров, позволила интегрировать их непосредственно в объекты физического мира. Существуют различные типы сенсоров для соответствующих целей, например, для измерения температуры, давления, скорости движения, местоположения и др. Сенсоры могут иметь небольшую память, давая возможность записывать некоторое количество результатов измерений. Сенсор может измерять физические параметры контролируемого объекта/явления и преобразовать их в сигнал, который может быть принят соответствующим устройством. Сенсоры классифицируются в соответствии с их назначением, например, сенсоры окружающей среды, сенсоры для тела, сенсоры для бытовой техники, сенсоры для транспортных средств и т.д.

Большинство сенсоров требует соединения с агрегатором сенсоров (шлюзом), которые могут реализоваться быть реализованы с использованием локальной вычислительной сети (LAN, Local Area Network), таких как Ethernet и Wi-Fi или персональной сети (PAN, Personal Area Network), таких как ZigBee, Bluetooth и ультраширокополосной беспроводной связи на малых расстояниях (UWB, Ultra-Wide Band). Для сенсоров, которые не требуют подключения к агрегатору, их связь с серверами/приложениями может предоставляться с использованием глобальных беспроводных сетей WAN, таких как GSM, GPRS и LTE. Сенсоры, которые характеризуются низким энергопотреблением и низкой скоростью передачи данных, образуют широко известные беспроводные сенсорные сети (WSN, Wireless Sensor Network). WSN набирают все большую популярность, поскольку они могут содержать гораздо больше сенсоров с поддержкой работы от батарей и охватывают большие площади.

2. *Уровень шлюзов и сетей.*

Большой объем данных, создаваемых на первом уровне IoT многочисленными миниатюрными сенсорами, требует надежной и высокопроизводительной проводной или беспроводной сетевой инфраструктуры в качестве транспортной среды. Существующие сети

связи, использующие различные протоколы, могут быть использованы для поддержки межмашинных коммуникаций M2M и их приложений. Для реализации широкого спектра услуг и приложений в IoT необходимо обеспечить совместную работу множества сетей различных технологий и протоколов доступа в гетерогенной конфигурации. Эти сети должны обеспечивать требуемые значения качества передачи информации, и прежде всего по задержке, пропускной способности и безопасности. Данный уровень состоит из конвергентной сетевой инфраструктуры, которая создается путем интеграции разнородных сетей в единую сетевую платформу. Конвергентный абстрактный сетевой уровень в IoT позволяет через соответствующие шлюзы нескольким пользователям использовать ресурсы в одной сети независимо и совместно без ущерба для конфиденциальности, безопасности и производительности.

3. Сервисный уровень

Сервисный уровень содержит набор информационных услуг, призванных автоматизировать технологические и бизнес операции в IoT: поддержки операционной и бизнес деятельности (OSS/BSS, Operation Support System/Business Support System), различной аналитической обработки информации (статистической, интеллектуального анализа данных и текстов, прогностическая аналитика и др.), хранения данных, обеспечения информационной безопасности, управления бизнес-правилами (BRM, Business Rule Management), управления бизнес-процессами (BPM, Business Process Management) и др.

4. Уровень приложений

На четвертом уровне архитектуры IoT существуют различные типы приложений для соответствующих промышленных секторов и сфер деятельности (энергетика, транспорт, торговля, медицина, образование и др.). Приложения могут быть «вертикальными», когда они являются специфическими для конкретной отрасли промышленности, а также «горизонтальными», (например, управление автопарком, отслеживание активов и др.), которые могут использоваться в различных секторах экономики. Конкретные IoT приложения более подробно рассмотрены в главе 9.

1.5 Веб вещей WoT

Составной частью Интернета вещей является Веб вещей (WEB of Things, WoT), который обеспечивает взаимодействие различных интеллектуальных объектов («вещей») с использованием стандартов и механизмов Интернет, таких как унифицированный (единообразный) идентификатор ресурса URI (Uniform Resource Identifier), протокол передачи гипертекста HTTP (HyperText Transfer Protocol), стиль построения архитектуры распределенного приложения REST (Representational State Transfer) и др. Фактически WoT предусматривает реализацию концепции IoT на прикладном уровне с использованием уже существующих архитектурных решений, ориентированных на разработку web-приложений. Другими словами данные с умных вещей или управление ими должно быть доступно через WWW-страницы. На рис. 1.9 показан пример, как используя специальную страницу в интернет через браузер можно считать данные с датчика света в беспроводной сенсорной сети или изменить цвет четвертого индикатора в сенсоре.

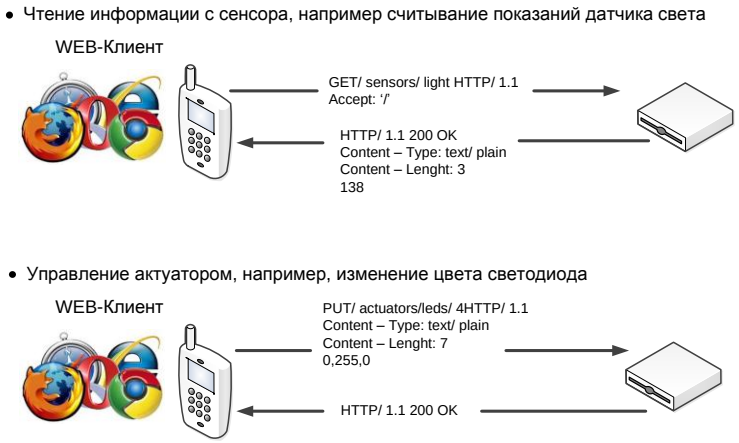


Рис. 1.9 – Примеры веб-взаимодействия с устройствами сенсорной сети

Основные свойства WoT:

1. Использует протокол HTTP в качестве приложения, а не в качестве транспортного механизма передачи данных, как он применяется для традиционных WWW-услуг.

2. Обеспечивает синхронную работу интеллектуальных (смарт) объектов через прикладной программный интерфейс REST (также известный как RESTful API) и в целом соответствует ресурсно-ориентированной архитектуре ROA (Resource-Oriented Architecture).

3. Предоставляет асинхронный режим работы интеллектуальных объектов с использованием в значительной степени стандартных Web-технологий, таких как Atom, содержащей формат для описания ресурсов на веб-сайтах и протокол для их публикации, или Web-механизмов передачи данных, таких как модель работы веб-приложения Comet, при которой постоянное HTTP-соединение позволяет веб-серверу отправлять данные браузеру без дополнительного запроса со стороны браузера.

Эти характеристики WoT обеспечивают простое взаимодействие интеллектуальных объектов через Интернет, кроме того они реализуют единообразный интерфейс для доступа и поддержки функциональности смарт-объектов.

С концепцией WoT перекликается идея *Семантической паутины* (Semantic Web) – это направление развития Всемирной паутины WWW, целью которого является представление информации в виде, пригодном для машинной обработки. Термин «семантическая паутина» был впервые введён Тимом Бернерсом-Ли (изобретателем Всемирной паутины) в мае 2001 года. Концепция семантической паутины была принята и продвигается Консорциумом Всемирной паутины W3C (World Wide Web Consortium).

В обычной Паутине, основанной на HTML-страницах, информация заложена в тексте страниц и извлекается человеком с помощью браузера. Семантическая же паутина предполагает запись информации в виде семантической сети с помощью онтологий. Под онтологией понимается формальное явное описание понятий в рассматриваемой предметной области (классов). Онтология вместе с набором индивидуальных экземпляров классов образует базу знаний. Таким образом, программа-клиент может непосредственно извлекать из паутины факты и делать из них логические заключения. Семантическая паутина работает параллельно с обычной Паутиной и на её основе, используя протокол HTTP и идентификаторы URI.

Несмотря на все преимущества, предоставляемые семантической паутиной в случае её внедрения, существуют определенные сомнения в возможности её полной реализации. Указываются различные причины, которые могут быть препятствием к этому, начиная с человеческого фактора (люди склонны избегать работы по поддержке документов с метаданными, открытыми остаются проблемы истинности метаданных и т. д.). Кроме того необходимость описания метаданных так или иначе приводит к дублированию информации.

Каждый документ должен быть создан в двух экземплярах: размеченным для чтения людьми, а также в машинно-ориентированном формате.

1.6 Интернет нано-вещей

Нано-технологии привели к разработке миниатюрных устройств, размеры которых варьируются от одного до нескольких сотен нано-метров. На этом уровне нано-машины состоят из нано-компонентов и представляют себя отдельные функциональные блоки, способные выполнять простые измерительные, регулирующие или управляющие операции. Координация и обмен информацией между нано-устройствами позволяют образовывать так называемые нано-сети. В случае соединения нано-устройств с существующими сетями и Интернетом возникает новая сетевая парадигма, называемая Интернетом нано-вещей.

Для взаимодействия нано-устройств с существующими сетями и Интернетом требуется разработка новых сетевых архитектур. На рис. 1.10 представлена архитектура Интернета нано-вещей в двух различных реализациях – сеть на теле человека для мониторинга показателей здоровья и отправки их в медицинский центр, и современная офисная сеть, соединяющая множество различных устройств.

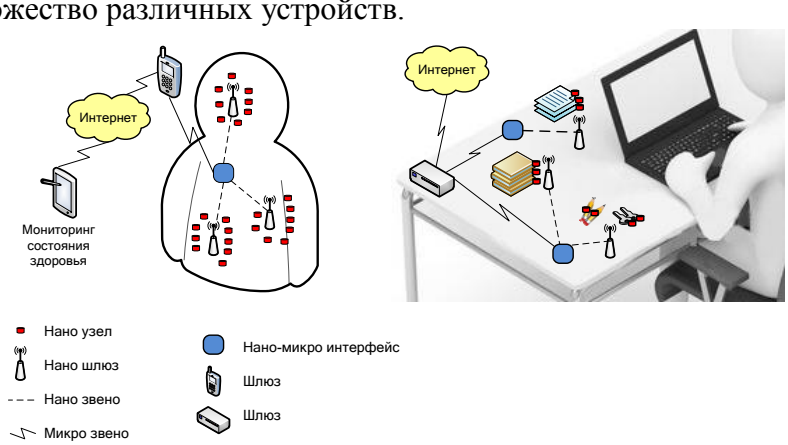


Рис. 1.10 – Примеры архитектуры Интернета нано-вещей

Сеть на теле человека состоит из нано-сенсоров и нано-актуаторов, которые могут отправлять информацию через внешний шлюз в медицинское учреждение. В данном случае на нано-уровне используются молекулы, протеины, ДНК, органические вещества и основные компоненты клеток. Таким образом, биологические нано-сенсоры и нано-актуаторы обеспечивают интерфейс между биологической средой человека и электронными нано-устройствами, которые могут использоваться в новой сетевой парадигме – Интернете нано-вещей.

Внутриофисная сеть соединяет множество даже самых небольших устройств с нано-приемопередатчиками, обеспечивающими соединение с сетью Интернет. В результате этого взаимодействия пользователь может отслеживать состояние и местонахождение любых вещей, без каких либо усилий и временных затрат. При разработке новых миниатюрных устройств могут использоваться самые передовые энергосберегающие технологии, позволяющие получать механическую, электромагнитную и другие виды энергии из окружающей среды.

Независимо от области применения, основными компонентами архитектуры сети Интернета нано-вещей являются:

1. *Нано-узлы* - миниатюрные и простейшие нано-устройства. Позволяют выполнять простейшие расчеты, имеют ограниченную память и ограниченную дальность передачи сигналов. Примерами нано-узлов могут быть биологические нано-сенсоры на человеческом теле или внутри него или нано-устройства, встроенные в повседневные окружающие нас вещи – книги, часы, ключи и т.д.

2. *Нано-шлюзы* – данные нано-устройства имеют относительно высокую производительность по сравнению с нано-узлами и выполняют функцию сбора информации от нано-узлов. Кроме того, нано-шлюзы могут контролировать поведение нано-узлов путем выполнения простых команд (вкл./выкл., режим сна, передать данные и т.д.).

3. *Нано-микро интерфейсы* – устройства, собирающие информацию от нано-шлюзов, и передающие её во внешние сети. Данные устройства включают в себя как нано-технологии коммуникаций, так и традиционные технологии для передачи информации в существующие сети.

4. *Шлюз* – данное устройство осуществляет контроль всей нано-сети через сеть Интернет. Например, в случае сети с сенсорами на теле человека данную функцию может выполнять мобильный телефон, транслирующий информацию о нужных показателях в медицинское учреждение.

1.7 Когнитивный Интернет вещей CIoT

Интернет вещей является открытой парадигмой, которая чрезвычайно восприимчива и адаптивна для новых принципов и архитектур, относящихся к различным направлениям развития науки и техники. В этой связи чрезвычайно плодотворным может оказать использование в IoT принципов и методов когнитивности (лат. cognitio, «познание, изучение, осознание») путем создания когнитивного Интернета вещей CIoT (Cognitive Internet of Things).

Когнитивность означает наличие у объекта IoT следующих общих свойств:

– способность к самоанализу и реконфигурации с учётом имеющегося окружения, а также имея в виду достижение целей, обусловленных выполняемыми задачами;

– способность адаптировать своё состояние согласно имеющимся условиям или событиям, на основе определенных критериев и знаний о предыдущих состояниях;

– возможность динамически изменять свою топологию и/или эксплуатационные параметры в соответствии с требованиями конкретного пользователя, когда это необходимо в рамках текущей политики обслуживания, оптимизации пропускной способности сети или иных показателей;

– самоконфигурация с наличием распределенного управления на основе правил;

– возможность самостоятельного определения своего текущего состояния и, с учетом этого состояния – планирование своей работы, принимая определенные решения в ответ на сложившуюся ситуацию.

Представляется, что на практике когнитивные интернет-вещи смогут:

– использовать технологии получения знаний о своей операционной и географической среде, местонахождении, например с помощью стандартных технологий позиционирования GPS/ГЛОНАСС;

– устанавливать самостоятельно или использовать готовые правила взаимодействия между объектами (интернет-вещами);

– динамически и автономно корректировать свои операционные (рабочие) параметры и протоколы в соответствии с полученными знаниями для достижения заранее определенных целей, в частности выбирать наиболее подходящую технологию передачи радиосигнала;
обучаться на основе достигнутых результатов с использованием лучших практик и наиболее эффективных политик для достижения целей создания IoT.

Рассмотрим некоторые предположения относительно создания архитектуры когнитивного Интернета вещей. Концепция CIoT предполагает наличие IoT с механизмами кооперации и «разумности». Объекты CIoT смогут составить определенное представление о состоянии и условиях функционирования окружающих объектов, воспринимать знания об окружающих объектах, продуцировать логические выводы из накопленных знаний и

осуществлять действия по адаптации к внешним и внутренним условиям. Соответственно, в архитектуре CIoT (рис 1.11) появляются когнитивные узлы CN (cognitive node) или когнитивные элементы CE (cognitive element), которые способны автономно оптимизировать, например, технические характеристики сети в соответствии с определенными условиями. В свою очередь CE или CN объединяются в домены автономности AD (Autonomous Domain), где эти устройства относительно тесно связаны между собой, в том числе на определенной территории, и могут кооперировать своё поведение. При этом каждое CE или CN сохраняет свойство автономности. В свою очередь, многие домены AD могут трансгранично взаимодействовать и кооперироваться через мультидоменную кооперацию MDC (Multi-Domain Cooperation). Для организации такого взаимодействия в каждом автономном домене используется когнитивный агент CA (Cognitive Agent), который взаимодействует с CE или CN в своем домене. Таким образом, взаимодействие доменов возможно как в целом, так и на уровне отдельного когнитивного элемента. При этом в каждом домене AD существуют и простые, не когнитивные узлы, которые, находятся под контролем когнитивных узлов.

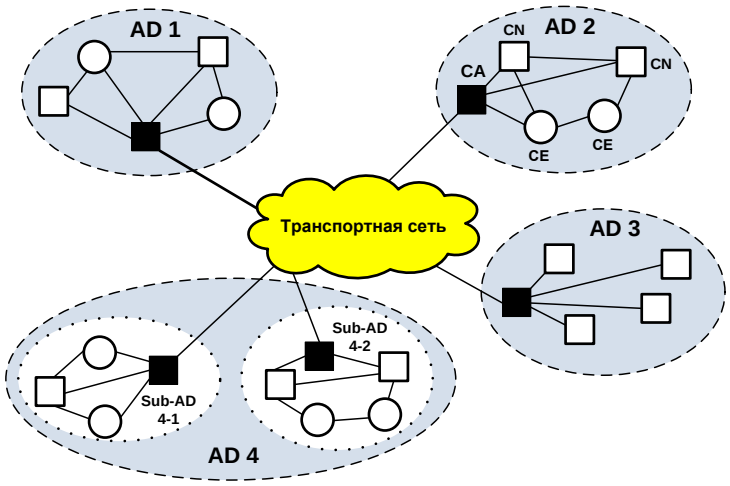


Рис 1.11 – Архитектура когнитивного Интернета вещей CIoT

Основой для развития схемы когнитивного управления является концепция виртуального объекта VO (Virtual Object), который является представлением физического объекта или объекта реального мира RWO (Real-World Object), что в принципе не противоречит требованиям Рекомендации МСЭ-Т Y.2060. Виртуальный объект динамически создается или удаляется, создавая тем самым представление динамики изменений RWO. Для описания возможностей автоматической агрегации VO, чтобы обеспечить условия для исполнения приложений в предлагаемой схеме когнитивного управления вводится понятие концепции композитных (сложносоставных) виртуальных объектов CVO (Composite VO) (рис. 1.12).

Рис. 1.12 – Схема когнитивного управления

Рассмотрим применение концепции CIoT на примере оптимизации времени оказания неотложной помощи больному по конкретному адресу. Больной находится под дистанционным контролем системы медицинского мониторинга на базе услуги IoT. Пусть сенсорная система на теле больного («body sensor») зафиксировала резкое и продолжительное изменение параметров состояния человека – резкое учащение дыхания, пульса, сердечную аритмию, признаки обморока. Показания сенсоров – RWO, приводят к изменению состояния объектов VO, связанных с RWO через шлюз. Специальное приложение для обработки и трансляции показаний сенсоров обрабатывает указанную информацию VO и преобразует её к виду, который может быть использован CVO, в данном случае – медицинским центром с помощью процедуры запроса и совпадения ситуации RSM «Request and Situation Matching». Однако если в ходе поиска требуемый CVO не найден, или отсутствует свободный медицинский автомобиль (ситуация «все на выезде»), то с помощью процедуры принятия решений задействуется другой подходящий для данного случая VO, например сенсор пожарной сигнализации. В результате в схеме принимает участие новый CVO – служба спасения – на основе анализа близости ситуации к опасной для здоровья человека. В итоге скорая помощь может быть оказана больному не медицинским центром, а службой спасения, специалисты которой также имеют навыки медицинской помощи. С учетом того, что событие происходит в «умном городе», медицинская информация о состоянии больного может транслироваться параллельно на CVO медицинского центра и на CVO «умного автомобиля» службы спасения. Одновременно тревожное сообщение транслируется на CVO службы регулирования дорожного движения, которая организует «зеленую улицу» в направлении дома больного. Таким образом, описанная ситуация наглядно показывает преимущества когнитивности и когнитивного управления применительно к интернету вещей.

1.8 Способы взаимодействия с интернет-вещами

Используют 3 способа взаимодействия с интернет-вещами:

1) прямой доступ;
2) доступ через шлюз;
3) доступ через сервер.

В случае прямого доступа интернет-вещи должны иметь собственный IP-адрес или сетевой псевдоним, по которому к ним можно обратиться из любого клиентского приложения и они должны выполнять функции веб-сервера. Интерфейс с такими вещами обычно выполнен в виде web-ресурса с графическим интерфейсом для управления посредством веб-браузера. Возможно использование специализированного программного обеспечения. В такие веб-устройства должен быть интегрирован прикладной программный интерфейс RESTful API для прямого доступа к ним через Интернет. Соответствующая архитектура WoT показана на рис. 1.13. Каждое устройство имеет собственный IP-адрес, работает как веб-сервер и использует интерфейс RESTful API для реализации веб-приложения, объединяющего данные из нескольких источников в один интегрированный сервис. При таком объединении получается новый уникальный веб-сервис, изначально не предлагаемый ни одним из источников данных.

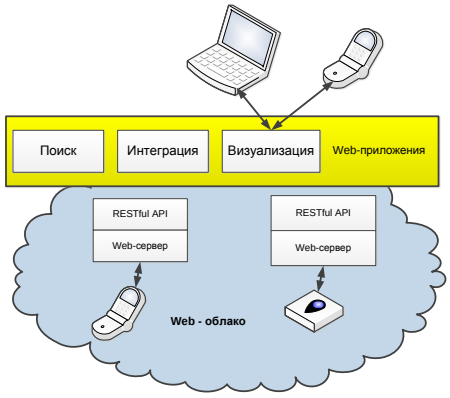


Рис. 1.13 – Прямой доступ к IP-устройствам через API

Недостатки такого способа очевидны:

– необходимость иметь фиксированный адрес в сети, что зависит от провайдера услуги связи с Интернетом таких вещей; другим выходом из ситуации является использование сетевого псевдонима IP-адреса (alias), что требует постоянного обращения интернет-вещи к специальному серверу с запросом об обновлении сетевого адреса по псевдониму;

– лимит подключений к устройству – вызвано низким качеством связи интернет-вещей, а также их слабыми вычислительными ресурсами. Такая проблема решается путём включения в состав интернет-вещи высокопроизводительного оборудования и подключения вещей к стабильному источнику связи с Интернетом. Это вызывает необходимость в большем потреблении энергии такой вещью и часто вынуждает делать такие вещи стационарными, питающимися от постоянных источников электроэнергии.

Если интерент-вещи не имеют встроенной поддержки протоколов IP и HTTP, а поддерживают частные протоколы, например Bluetooth или ZigBee, то для взаимодействия с ними можно использовать специальный Интернет-шлюз (рис. 1.14). Он является веб-сервером, который через интерфейс REST-API взаимодействует с IP-устройствами, и преобразует поступающие от них запросы в запрос к специфическому API устройства, подключенного к этому шлюзу. Основное преимущество использования Интернет шлюза в том, что он может поддерживать несколько типов устройств, использующих собственные протоколы для связи.

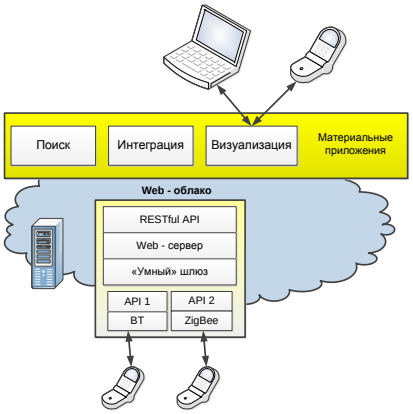


Рис. 1.14 – Доступ к не IP-устройствам через интеллектуальный шлюз

Доступ к интернет-вещам через шлюз является более рациональным способом организации взаимодействия и полностью вытесняет метод прямого доступа в случае необходимости организации связи беспроводных сенсорных сетей или сети Интернет-вещей с глобальной сетью Интернет. Большинство стандартов беспроводных сенсорных сетей не поддерживают протокол IP, используя собственные протоколы взаимодействия. Такая особенность вызывает необходимость наличия устройства для ретрансляции сообщений из сенсорной сети в сеть Интернет для совместимости протоколов.

Недостатки такого подхода те же, что и в случае прямого доступа, но распространяются они уже на шлюз.

Третья форма взаимодействия устройств в IoT через сервер подразумевает наличие посредника между интернет-вещами и пользователем и может быть реализована с помощью посреднической платформы данных. Данный подход предполагает наличие централизованного сервера или группы серверов, в основные функции которых входит:

– приём сообщений от интернет-вещей и передача их пользователям;

– хранение принятой информации и её обработка;

– обеспечение пользовательского интерфейса с возможностью двустороннего обмена между пользователем и интернет-вещью.

Основной целью использования посреднических платформ данных является упрощение поиска, контроля, визуализации и обмена данными с разными «вещами». В основе данного подхода лежит централизованное хранилище данных. Каждое устройство, имеющее доступ в сеть Интернет (прямой или через интернет-шлюз), должно быть зарегистрировано в системе, прежде чем оно сможет начать передачу данных. При этом существенно снижаются требования к производительности устройств, так как от них не требуется выполнение функций web-сервера. Набор инструментов, предоставляемых платформами, существенно упрощает разработку новых приложений для взаимодействия и управления объектами WoT.

Такой способ доступа является наиболее рациональным и часто используемым, поскольку позволяет перенести нагрузку обработки запросов пользователей с интернет-вещей на централизованный сервер, тем самым разгружая слабый радиоканал связи интернет-вещей, перенося нагрузку на проводные каналы связи между сервером и пользователями.

Метод централизованного сервера также предоставляет надёжные средства хранения и обработки информации, позволяет интернет-вещам взаимодействовать друг с другом и пользоваться облачными вычислениями. Данный подход может использовать также метод шлюза для соединения локальных беспроводных сетей с сервером.

В Интернете вещей шлюз используется не только для прямой связи интернет-вещей с пользователем, но и при использовании централизованного сервера. Шлюзы служат средством для объединения локальных сетей интернет-вещей с глобальной сетью и связью с

сервером управления или конечным пользователем. Поскольку локальные сети интернет-вещей представляют собой в основном беспроводные сенсорные сети, то шлюзы, используемые в Интернете вещей, аналогичны используемым в территориально-распределённых сенсорных сетях. Существует несколько способов организации шлюзов.

Первый способ заключается в использовании компьютеров, которые имеют точку доступа к глобальной сети Интернет, и каждая из объединяемых сетей подключена к такому компьютеру. Основными недостатками такого подхода являются стоимость и громоздкость. Сенсорные сети состоят из миниатюрных датчиков и должны работать автономно, однако территориально-распределённая сенсорная сеть при таком подходе теряет свойство автономности, поскольку теперь она зависит от наличия электричества и точки доступа в Интернет на компьютере.

Второй способ заключается в использовании устройства-шлюза, позволяющего соединить сенсорную сеть с ближайшей проводной сетью, имеющей выход в Интернет. Такой проводной сетью, как правило, является Ethernet-сеть. Устройство имеет в себе приёмопередатчик, совместимый с объединяемой сенсорной сетью, порт для подключения к сети Ethernet и микроконтроллер, выполняющий функции преобразования пакетов одной сети в формат другой. Такой способ отличается меньшей стоимостью, чем первый и размер такого устройства небольшой, но оно нуждается в относительно высоком энергопотреблении из-за того, что стандартные проводные сети не рассчитаны на низкий уровень сигнала и потребления энергии. Также такое устройство не может гарантировать наличие точки доступа в ближайшей проводной сети.

Третий способ заключается в использовании устройства-шлюза, которое является полностью автономным и само предоставляет точку доступа к сети Интернет. Это возможно при использовании беспроводных технологий передачи данных. Устройство состоит из одного приёмопередатчика, совместимого с сенсорной сетью и второго – совместимого с той или иной глобальной беспроводной сетью, в область действия которой попадает сенсорная сеть. Такими сетями могут служить GSM или WiMAX. Использование сети GSM является более экономичным в плане энергопотребления.

Существуют также шлюзы, предоставляющие доступ сенсорным сетям к ближайшим сетям Wi-Fi для поиска точки доступа к сети Интернет.

Таким образом, если необходимо организовать полностью автономную территориально-распределённую сенсорную сеть, то следует использовать третий способ. Если же сенсорная сеть используется как часть какой-либо крупной проводной сети, то нет необходимости в её полной автономности и возможно использование первых двух способов.

1.9 Зрелость концепции IoT и составляющих ее технологий

Известная исследовательская компания Gartner с 1995 года регулярно составляет графики цикла зрелости технологий (так называемая *S*-образная кривая или кривая хайпа[1]), где отмечает технологии, которые нашли свою нишу и продолжили уверенное развитие, к которым проявляется избыточное внимание и которые находятся в самом начале своего зарождения. Начиная с 2011 года Gartner помещает Интернет вещей в общий цикл зрелости новых технологий на начальный этап «технологического триггера» с указанием срока становления более 10 лет, а в 2012 году был выпущен специальный цикл зрелости для технологий, составляющих основу IoT (рис. 1.15).

Конечно, трудно точно предсказать, когда именно технология IoT достигнет полной зрелости. В любом случае преимущества Интернета вещей очевидны и это дает основание утверждать, он станет повсеместно распространен.

[1] англ. hype – назойливая рекламная кампания, заявляющая о том, что продвигаемый товар непременно должен быть у каждого

Так как базовые составляющие Интернета вещей, такие как беспроводные сенсорные сети (Wireless Sensor Network, WSN), коммуникации малого радиуса действия (NFC, Near Field Communication) и межмашинные коммуникации (M2M, Machine-to-Machine), уже прошли пик завышенных ожиданий и находятся на третьем этапе – избавления от иллюзий, для того чтобы концепция IoT получила стабильное развитие в будущем, необходима ее практическая востребованность. А это случиться, если Интернет вещей продемонстрирует на практике новые, более широкие возможности коммуникаций любых вещей в различных областях человеческой деятельности.

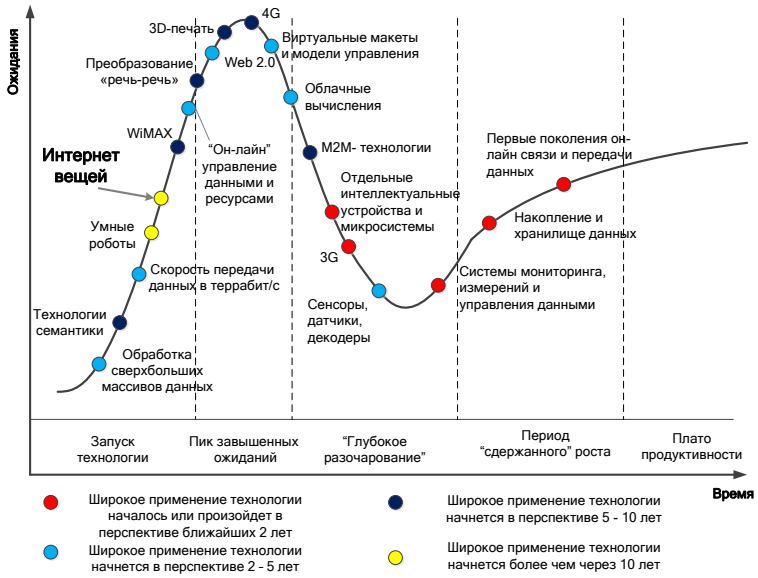


Рис. 1.15 – Цикл зрелости технологий IoT (источник: Gartner, 2012)

1.10 Взаимодействие IoT с перспективными инфокоммуникационными технологиями

Важную роль в становлении и успешном внедрении Интернета вещей играют различные перспективные инфокоммуникационные технологии, такие как большие данные, облачные технологии и повсеместная компьютеризация, с которыми IoT активно взаимодействует. Эволюция Интернета вещей и сопутствующих инфокоммуникационных технологий на ближайшую перспективу показана на рис. 1.16. В настоящее время IoT находит свое практическое воплощение в основном в виде систем M2M, в ближайшей перспективе на базе чипсетов с ультранизким энергопотреблением и миниатюрных RFID-меток будут созданы интегральные сенсорные сети, а затем и когнитивные сети («умные» сети на основе знаний).

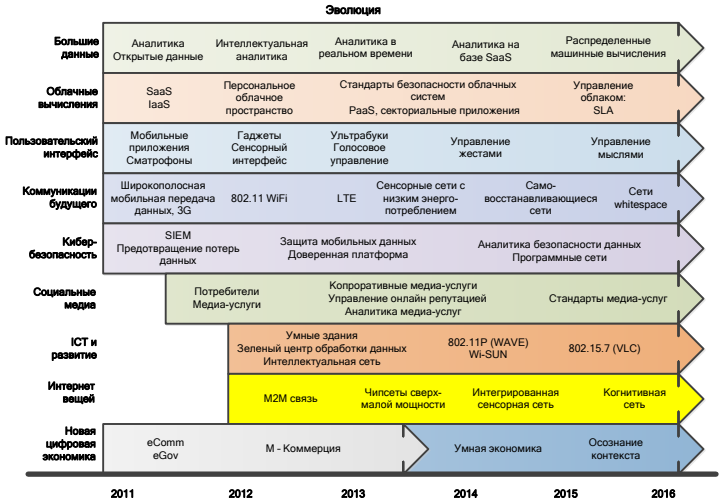


Рис. 1.16 – Эволюция Интернета вещей и сопутствующих инфокоммуникационных технологий
(источник: компания IDA, Сингапур, 2012)

Большие данные (Big Data)

До начала XX века объем знаний удваивался каждое столетие, сегодня объем знаний человечества удваивается каждые 2-3 года. 70% всей доступной информации появилось после изобретения Интернета. Интернет вещей радикальным образом увеличивает объем собираемых данных, что является следствием огромного количества источников информации (прежде всего различные сенсоры). Гигантские сенсорные сети уже сейчас производят огромные потоки данных, которые надо уметь не только хранить, но и обрабатывать, делать по ним выводы, принимать решения – и все это с учетом неточности как оригинальных данных, так и процедур обработки. В конце 2000-х годов для обработки большого объема данных сформировался подход, который называется «большие данные» (англ. Big Data) – это серия инструментов и методов обработки структурированных и неструктурированных данных огромных объёмов и значительного многообразия для получения необходимых результатов обработки. В качестве определяющих характеристик для больших данных отмечают «три V»: объём (англ. volume, в смысле величины физического объёма), скорость (англ. Velocity, в смыслах как скорости прироста, так и необходимости высокоскоростной обработки и получения результатов), многообразие (англ. variety, в смысле возможности одновременной обработки различных типов структурированных и неструктурированных данных) (рис. 1.17).

Рис. 1.17 – Три основные характеристики больших данных

Основное отличие больших данных от «обычных» заключается в том, что эти данные невозможно обработать традиционными системами управления базами данных (СУБД) и решениями класса Business Intelligence из-за их большого объема и разнообразного состава. Другое важное их свойство – феноменальное ускорение накопления данных и постоянное изменение. Такие популярные задачи, как сведение данных, полученных из разных источников (Data Cleaning, Data Merging, De-deduplication), требуют особых методов анализа в случае неточных данных, особенно данных огромных размеров. В связи с этим и был разработан набор инструментов, получивший название «большие данные», позволяющих работать с данными вне зависимости от их типа и объема.

Прогнозируется, что внедрение технологий больших данных наибольшее влияние окажет на информационные технологии в производстве, здравоохранении, торговле, государственном управлении, а также в сферах и отраслях, где регистрируются индивидуальные перемещения ресурсов и где потенциально могут быть использованы технологии Интернета вещей.

Облачные вычисления (Cloud Computing)

Так как Интернет вещей порождает «большие данные», поэтому возникает закономерный вопрос: где их хранить и чем обрабатывать? Ответом этот вопрос является перспективная инфокоммуникационная технология – *облачные вычисления* (CC, Cloud Computing). Облачные вычисления подразумевают аренду услуг и ресурсов для хранения и обработки данных в глобальной сети вместо собственной инфраструктуры. У систем CC должны быть пять основных характеристик: самообслуживание по требованию, широкополосный сетевой доступ, пул ресурсов, возможность быстрой перенастройки или расширения и измеряемое обслуживание.

Существуют четыре модели развёртывания облачной инфраструктуры (так называемых «облаков»):

1. *Частное облако* (англ. private cloud) – инфраструктура, предназначенная для использования одной организацией, включающей несколько потребителей (например, подразделений одной организации), возможно также клиентами и подрядчиками данной организации. Частное облако может находиться в собственности, управлении и эксплуатации, как самой организации, так и третьей стороны (или какой-либо их комбинации), и оно может физически существовать как внутри, так и вне юрисдикции владельца.

2. *Публичное облако* (англ. public cloud) – инфраструктура, предназначенная для свободного использования широкой публикой. Публичное облако может находиться в собственности, управлении и эксплуатации коммерческих, научных и правительственных организаций (или какой-либо их комбинации). Публичное облако физически существует в юрисдикции владельца – поставщика услуг.

3. *Гибридное облако* (англ. hybrid cloud) – это комбинация из двух или более различных облачных инфраструктур (частных, публичных или общественных), остающихся уникальными объектами, но связанных между собой стандартизованными или частными технологиями передачи данных и приложений.

4. *Общественное облако* (англ. community cloud) – вид инфраструктуры, предназначенный для использования конкретным сообществом потребителей из организаций, имеющих общие задачи (например, миссии, требований безопасности, политики, и соответствия различным требованиям). Общественное облако может находиться в кооперативной (совместной) собственности, управлении и эксплуатации одной или более из организаций сообщества или третьей стороны (или какой-либо их комбинации), и оно может физически существовать как внутри, так и вне юрисдикции владельца.

Различные услуги СС, обозначаемые в общем случае как XaaS (X as a Service), можно отнести к трем основным классам (рис. 1.18):

– «инфраструктура, как услуга» (IaaS, Infrastructure as a Service) – аренда мощности серверов и емкости систем хранения центров обработки данных (ЦОД);

– «программное обеспечение, как услуга» (SaaS, Software as a Service) – аренда программного обеспечения (ПО), которое запускается «из облака»;

– «платформа, как услуга» (PaaS, Platform as a Service) – аренда платформы разработки ПО коллективными или индивидуальными разработчиками.

Все остальные услуги систем СС (например, BPaaS – «бизнес-процесс, как услуга» или VSaaS – «видеонаблюдение, как услуга»), можно, так или иначе, отнести к трем вышеуказанным классам облачных услуг.

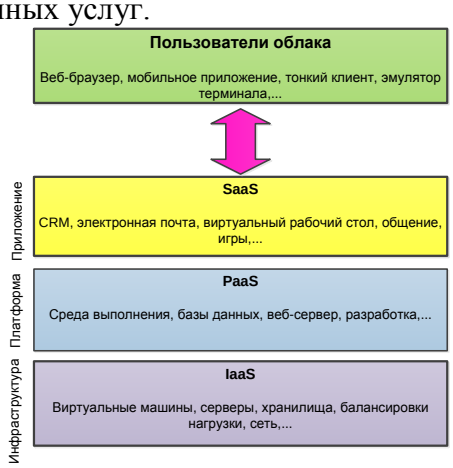


Рис. 1.18 – Классы услуг облачных вычислений

Для работы технологий Интернета вещей можно использовать и *туманные вычисления* (Fog Computing). Под «туманом» подразумевается приближение «облака» к земле, в данном случае «туман» — это разновидность облачных сервисов, расположенных не где-то в недоступных высотах, а в окружающей нас среде. Иначе говоря, Fog Computing не альтернатива, а дополнение к Cloud Computing, и могут возникнуть ситуации их совместного действия (например, выполнение аналитического приложения), и в таком случае Cloud окажет услугу Fog.

Туманные вычисления дополняют облачные вычисления и обеспечивают взаимодействие умных вещей между собой и облачными ЦОД в виде трехуровневой иерархической структуры. Верхний уровень занимают тысячи облачных ЦОД, предоставляющих ресурсы, необходимые для выполнения серьезных, например аналитических, программных приложений IoT. Уровнем ниже располагаются десятки тысяч распределенных управляющих ЦОД, в которых содержится «интеллект» Fog Computing, а на нижнем уровне находятся миллионы вычислительных устройств умных вещей.

Fog Computing можно определить как в максимальной степени виртуализированную платформу, поддерживающую три основных типа сервисов, образующих межмашинные коммуникации M2M: вычисления, хранение и сеть. Задача Fog Computing заключается в обеспечении взаимодействия миллиардов устройств между собой и с облачными ЦОД.

Парадигма Fog Computing отличается от Cloud Computing по целому ряду параметров.

1. *Распределение вычислительной мощности и реальное время*.

Значительные вычислительные ресурсы могут быть размещены на периферии Сети, причем не должно быть зависимости от координат того места, где находится устройство, и при этом работа в режиме реального времени предполагает низкий уровень задержек при обмене данными, к тому же в Fog Computing может произойти конвергенция двух существовавших долгое время автономно друг от друга систем — управления бизнесом и технологическими системами.

2. *Географическое распределение компонентов*.

Модель распределения сервисов в Fog Computing менее централизована, чем для облаков, а отдельные устройства могут быть связаны между собой потоками данных и предоставлять друг другу «тяжелые» сервисы.

3. *Большой объем внешних данных*.

Устройства, экипированные многочисленными сенсорами, могут в реальном времени генерировать гигантские объемы данных.

4. *Сложная топология*.

Миллионы географически распределенных узлов могут создавать разнообразные и не детерминированные заранее связи.

4. *Мобильность и гетерогенность*.

Мобильность устройств потребует использования альтернативных протоколов, например протокола маршрутизации LISP (Locator/ID Separation Protocol), который позволяет разделить функциональность IP-адресов на две части: идентификаторы хостов и локаторы маршрутизации. Концепция предусматривает установку туннельных маршрутизаторов, которые будут добавлять LISP-заголовки в информационные пакеты по мере их движения по сети.

Повсеместная компьютеризация (Ubiquitous Computing)

В 1991 году исследователь лаборатории Xerox PARC Марк Вейзер выдвинул концепцию будущего мира, «богато и незаметно насыщенного сенсорами, дисплеями и вычислительными элементами, соединенными в единую сеть и являющими неотъемлемые элементы предметов быта». Физическая возможность осуществления этой концепции появилась к концу 2000-х годов по мере тотального распространения дешевых и миниатюрных вычислительных мобильных устройств, беспроводных сетей и спутниковой навигации (рис. 1.19).

Повсеместный (вездесущий, всепроникающий, тотальный) компьютинг, фигурирующий в специальной литературе под терминами «ubiquitous computing» и «pervasive computing», попросту означает создание вездесущих интеллектуальных информационных систем, помогающих в ежедневной человеческой рутине – дома, в офисе, в больнице, на работе, в дороге. Тотальный компьютинг ставит во главу угла конечного пользователя, который должен получать вычислительное обслуживание непрерывно, 24 часа в сутки, 7 дней в неделю, причем обслуживание самого разного рода – от научных вычислений до управления кухонными агрегатами. Так, например, система персональной помощи (Personal Assistance System, PAS) помогает престарелым в самообслуживании с использованием беспроводной сети, объединяющей RFID-ридеры, медтехнику с Bluetooth-интерфейсом, программное обеспечение и аппаратуру, отслеживающую перемещения человека в жилище, датчики падения, системы безопасности и т.п.

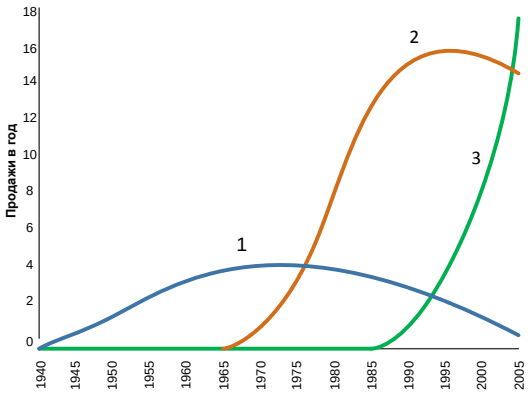


Рис. 1.19 – Эволюция вычислительных систем: мейнфреймы (кривая 1) – один компьютер, много пользователей; персональные компьютеры (кривая 2) – один компьютер, один пользователь; повсеместный компьютинг (кривая 3) – один пользователь, много компьютеров

Можно выделить четыре основные характеристики тотального компьютинга:

1) *эффективное использование персонального умного пространства*, имея в виду окружающие нас на работе, в транспорте, дома устройства с компьютерным управлением, необходимыми датчиками и исполнительными механизмами;

2) *невидимость* (умного пространства) – минимальное отвлечение внимания пользователя на управление окружающими вещами;

3) *местная масштабируемость* – любая точка персонального умного пространства должна быть сделана настолько вычислительно "мощной", насколько это необходимо пользователю;

4) *маскирование неоднородностей* – под неоднородностью понимаются различия как в техническом плане (называемые, обычно, гетерогенностью), так и не технические – организационные структуры, бизнес-процессы, экономические факторы.

К этому можно еще добавить знание контекста, т.е. пользователь существует в персональном умном пространстве не "вслепую", а представляя себе, сознавая контекст. В некотором отношении это противоречит свойству невидимости, однако, на самом деле, должен существовать разумный баланс между невидимостью и знанием контекста.

1.11 Направления практического применения IoT

На основе Интернета вещей могут быть реализованы всевозможные «умные» (smart) приложения в различных сферах деятельности и жизни человека (рис. 1.20):

- «Умная планета» – человек сможет буквально «держать руку на пульсе» планеты: своевременно реагировать на упущения в планировании хозяйств, загрязнения и другие экологические проблемы, а значит, эффективно распоряжаться невозобновляемыми ресурсами.
- «Умный город» – городская инфраструктура и сопутствующие муниципальные услуги, такие как образование, здравоохранение, общественная безопасность, ЖКХ, станут более связанными и эффективными.
- «Умный дом» – система будет распознавать конкретные ситуации, происходящие в доме, и реагировать на них соответствующим образом, что обеспечит жильцам безопасность, комфорт и ресурсосбережение.
- «Умная энергетика» – будет обеспечена надежная и качественная передача электрической энергии от источника к приемнику в нужное время и в необходимом количестве.
- «Умный транспорт» – перемещение пассажиров из одной точки пространства в другую станет удобнее, быстрее и безопаснее.
- «Умная медицина» – врачи и пациенты смогут получить удаленный доступ к дорогостоящему медицинскому оборудованию или к электронной истории болезни в любом месте, будет реализована система удаленного мониторинга здоровья, автоматизирована выдача лекарственных препаратов больным и многое другое.

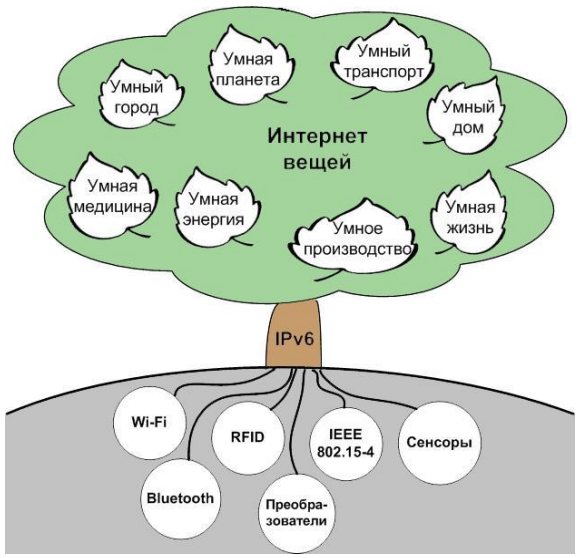


Рис. 1.20 – Умные приложения на основе Интернета вещей

Конкретные практические примеры для перечисленных выше направлений реализации Интернета вещей рассмотрены в главе 6.

1.12 Планы и прогнозы внедрения IoT

Возможности Интернета вещей в области генерирования, сбора, передачи, анализа и распределения огромного объема данных в мировом масштабе позволят человечеству, в конечном счете, получить новые знания, которые необходимы ему не только лишь для выживания, но и для настоящего процветания на протяжении многих веков. Подтверждение этому – включение Интернета вещей в перечень прорывных технологий в США и в число семи формирующихся национальных стратегических отраслей промышленности в Китае.

Единые стандарты только зарождаются, но масштабные проекты в данном направлении – своего рода «Интранеты вещей» – энергично развиваются уже сейчас. Так, американское агентство NASA при поддержке компании Cisco создает систему глобального сбора данных о Земле «Кожа планеты» (Planetary skin). Про «умные» дома наверняка многие слышали, в Японии уже не редкость «умные» заводы, а в США в рамках национальной инициативы оцифровки мегаполисов Connected Urban Development «умнеют» и города.

В разных странах существуют конкретные программы и планы практического внедрения интернета вещей. Так, Евросоюз развивает IoT по специальной программе, включающей 14 направлений. Согласно китайской государственной программе до 2015 г. планируется реализовать 149 проектов. Не менее активно ведутся разработки в Англии, Австралии, Японии, Южной Корее и других странах.

1.13 Проблемы внедрения IoT

Широкому внедрению Интернета вещей препятствуют сложные технические и организационные проблемы, в частности, связанные со стандартизацией. Единых стандартов для интернета вещей пока нет, что затрудняет возможность интеграции предлагаемых на рынке решений и во многом сдерживает появление новых. Сильнее всего глобальному внедрению препятствует расплывчатость формулировок концепции интернета вещей и большое число регуляторов и их нормативных актов.

К факторам, замедляющим развитие Интернета вещей, следует отнести сложности перехода существующего Интернета к новой, 6-й версии сетевого протокола IP, прежде всего необходимость больших финансовых затрат со стороны телекоммуникационных операторов и провайдеров услуг на модернизацию своего сетевого оборудования.

Если технологические платформы для Интернета вещей уже практически созданы, то, например, юридические и психологические ещё находятся только в стадии становления, равно как и проблемы взаимодействия пользователей, данных, устройств. Одна из проблем – защита данных в таких глобальных сетях. Существует также серьезная проблема, связанная с вторжением Интернета вещей в частную жизнь. Возможность отслеживать местонахождение людей и их собственности ставит вопрос о том, в чьем распоряжении окажутся эти сведения. Кто будет нести ответственность за хранение информации, собранной «умными вещами»? Кому и на каких условиях будет предоставляться эта информация? Можно ли ее собирать без согласия человека? Все эти вопросы пока остаются открытыми.

Также для полноценного функционирования такой сети необходима автономность всех «вещей», т.е. датчики должны научиться получать энергию из окружающей среды, а не работать от батареек, как это происходит сейчас.

Кроме того, с появлением Интернета вещей возникнет необходимость изменения общепринятых и проверенных бизнес-процессов и стратегий, что может привести к значительным финансовым затратам и рискам.

Основные драйверы и проблемы внедрения Интернета вещей приведены в табл. 1.1. Однако все перечисленные недостатки не существенны по сравнению с тем, какие возможности может дать Интернет вещей для человечества. Поэтому рано или поздно человечество неизбежно будет широко использовать технологии IoT. А вот чтобы эти технологии успешно внедрять, необходимо их знать. Краткому обзору технических особенностей различных составляющих Интернета вещей и посвящены остальные главы книги.

Таблица 1.1 Драйверы и барьеры рынка Интернета вещей

Драйверы	**Барьеры**
Стремительное развитие инфокоммуникационных технологий	Необходимость принятия общих стандартов
Мода на смартфоны, планшеты и другие мобильные устройства	Медленный переход к протоколу IPv6
Логистика и управление поставками	Риск закрытости частных сетей
Повышение безопасности и удобства автотранспорта	Несовместимость ряда компонентов
Необходимость сохранения окружающей среды и снижения энергозатрат	Проблема защиты персональных данных и безопасности
Развитие сферы контроля за контрафактной продукцией и защиты от краж	Сравнительно высокая стоимость внедрения
Поддержка государств и действия инноваторов	

Контрольные вопросы по главе 1

1. Что входит в понятие Интернета вещей?
2. Когда возник Интернет вещей и почему?
3. Укажите базовые принципы IoT.
4. Как соотносятся физические и виртуальные вещи?
5. Кто занимается стандартизацией Интернета вещей?
6. Поясните назначение функциональных уровней базовой архитектуры Интернета вещей.
7. Что общего и чем отличаются Интернет вещей и Веб вещей?
8. Из чего состоит интернет нано вещей?
9. Что такое когнитивный Интернет вещей?
10. Поясните основные способы взаимодействия с интерент-вещами.
11. Какова зрелость концепции IoT и ее базовых составляющих?
12. Укажите основные характеристики подхода «большие данные».
13. Что такое «облачные вычисления» и какие существуют модели «облаков»?
14. В чем суть идеи повсеместной компьютеризации?
15. Перечислите основные направления практического внедрения IoT.
16. Укажите основные движущие силы и барьеры на пути внедрения Интернета вещей.

ГЛАВА 2 РАДИОЧАСТОТНАЯ ИДЕНТИФИКАЦИЯ RFID

2.1 Общие сведения о радиочастотной идентификации RFID

Радиочастотная идентификация RFID (Radio Frequency IDentification) – общий термин, используемый для обозначения систем, которые беспроводным путем посредством радиоволн считывают идентификационный номер (в форме уникального серийного номера) какого-либо предмета или человека. RFID относится к обширной области технологий автоматической идентификации (Auto-ID), которые включают в себя также штриховые коды, оптические считыватели и некоторые биометрические технологии, как например, сканирование сетчатки глаза (рис. 2.1). В общем случае технологии Auto-ID используются с целью экономии времени и труда, затрачиваемых на ввод данных вручную и улучшения точности информации. Некоторые Auto-ID технологии, такие как системы штрихового кода, зачастую требуют участия человека, для сканирования и фиксирования информации вручную. Система RFID же сконструирована таким образом, что дает возможность считать и передавать данные в компьютерную систему без участия человека и в реальном масштабе времени. Технология RFID способна принести пользу в самых разных областях человеческой деятельности, включая промышленность, торговлю, образование, медицину и др.

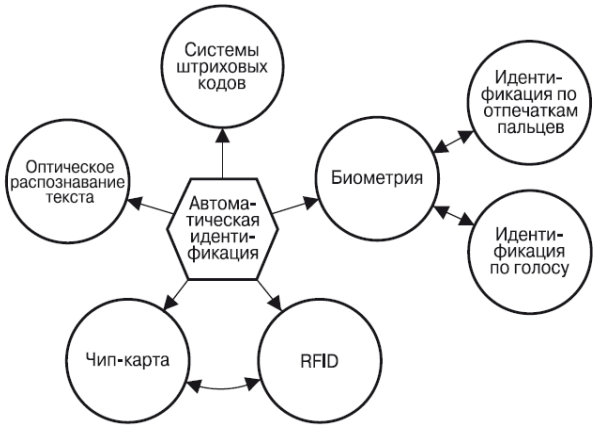


Рис. 2.1 – Основные системы автоматической идентификации

Любая RFID-система состоит из считывающего устройства (ридера) и небольших идентифицирующих устройств (RFID-меток), которые содержат обычно резонансный LC-контур, контроллер и электрически стираемое перепрограммируемое постоянное запоминающее устройство EEPROM (Electrically Erasable Programmable Read-Only Memory) (рис. 2.2). Содержимое памяти специфично для каждой метки и позволяет идентифицировать носителя метки (человека или объект).

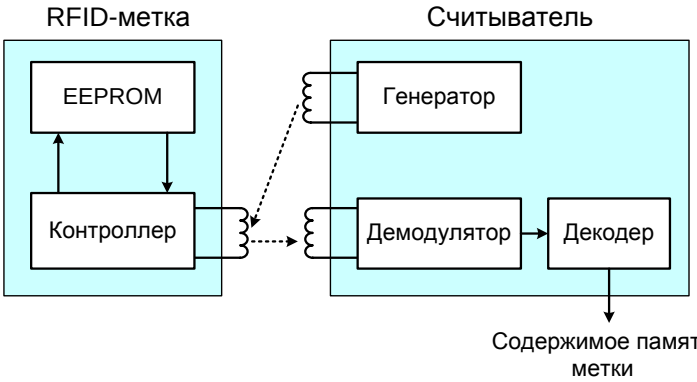


Рис. 2.2 – Основные компоненты системы RFID

Основной принцип работы такой системы сводится к следующему. Считыватель излучает радиоволну, которая принимается единственной меткой. Метка, таким образом, получает энергию и отражает радиоволну той же частоты (благодаря индуктивной связи), модулированную кодированным содержимым памяти. Считыватель принимает этот сигнал, демодулирует и декодирует его, чтобы определить содержимое памяти. Затем идентификационная система верхнего уровня проверяет эти данные и, соответственно, управляет процессом.

Привлекательность такой системы состоит в том, что она обеспечивает бесконтактное взаимодействие между считывателем и RFID-метками (избегая, таким образом, ограничений на позиционирование объекта с меткой), причем метки не требуют источника питания.

Однако когда в поле считывателя находятся две метки, они обе отвечают на излученный считывателем сигнал. При этом демодулированный сигнал считывателя является смесью двух компонент от двух меток и не может быть декодирован. Такая система неспособна одновременно идентифицировать два объекта. Известны несколько способов решения этой проблемы. Некоторые из них состоят в том, что считыватель и метки взаимодействуют в соответствии с заранее определенным протоколом, так что сигналы каждой метки успешно разделяются. Другой подход состоит в использовании меток на различных частотах.

По дальности считывания RFID-системы можно подразделить на следующие типы:

– ближней идентификации (считывание производится на расстоянии до 20 см);

– идентификации средней дальности (от 20 см до 5 м);

– дальней идентификации (от 5 м до 100 м).

Несмотря на то, что RFID-технология не нова и ее используют уже достаточно долго, о ее массовом применении заговорили не так давно. Это произошло потому, что до недавнего времени RFID-метки – основной компонент системы – стоили довольно дорого. И только некоторые компании могли себе позволить использование RFID-метки, цена на которые до недавнего времени превышала доллар и больше за единицу. Поэтому, в основном их использовали компании, которые выпускали продукцию многократного использования. В таком случае код продукта сохранялся и его можно было использовать в дальнейшем. Однако наиболее практичные современные RFID-метки являются одноразовыми, конечный потребитель может их выбросить вместе с ненужной ему упаковкой.

Использование RFID-систем наиболее актуально для компаний, которые участвуют в процессе производства, поставки и реализации различных товаров. Во-первых, используя RFID-системы, упрощается проведение инвентаризации товаров на складе. Также значительно упрощаются их прием и отгрузка. Кроме того, благодаря наличию RFID-меток и RFID-считывателей и специального компьютерного оборудования стало возможным создавать объемные базы данных по учету и движению товара.

По своему функционалу метод сбора данных на основе RFID-меток в значительной степени похож на технологию штрих-кода, широко применяемой во всем мире при маркировке различных товаров. Однако у RFID-систем есть много преимуществ по сравнению с системами на базе штрих-кода (табл. 2.1).

Табл. 2.1 Сравнение характеристик систем RFID и на базе штрих-кода

Характеристики технологии	**RFID**	**Штрих-код**
Необходимость в прямой видимости метки	Чтение даже скрытых меток	Чтение без прямой видимости невозможно
Объём памяти	От 10 до 10 000 байт	До 100 байт

Возможность перезаписи данных и многократного использования метки	Есть	Нет
Дальность регистрации	До 100 м	До 4 м
Одновременная идентификация нескольких объектов	До 200 меток в секунду	Невозможна
Устойчивость к воздействиям окружающей среды	Повышенная прочность и сопротивляемость	Зависит от материала, на который наносится
Срок жизни метки	Более 10 лет	Зависит от способа печати и материала объекта
Безопасность и защита от подделки	Подделка практически невозможна	Подделать легко
Работа при повреждении метки	Невозможна	Затруднена
Идентификация движущихся объектов	Да	Затруднена
Подверженность электромагнитным помехам	Есть	Нет
Идентификация металлических объектов	Возможна	Возможна
Использование стационарных и ручных считывателей	Да	Да
Возможность введения в тело человека/ животного	Возможна	Затруднена
Габаритные характеристики	Средние и малые	Малые
Стоимость	Средняя и высокая	Низкая

2.2 Метки RFID

Основой технологии RFID и главным ее компонентом является метка (англ. tag) или транспондер (transmitter – передатчик, responder – ответчик), содержащая определенную информацию (например, о продукте, о производстве, месте назначения, сроке реализации и

др.), передаваемую на считыватель, когда тот проводит опрос метки. Большинство RFID-меток состоит из двух частей (рис. 2.3). Первая – интегральная схема для хранения и обработки информации, модулирования и демодулирования радиочастотного сигнала и некоторых других функций. Вторая – антенна для приёма и передачи сигнала. RFID система работает по следующему принципу: радиосигнал посылается считывателем транспондеру (метке), который принимает его и отражает (пассивная метка) или генерирует выходной сигнал (активная метка). В процессе считывания метки происходит передача данных из ее памяти в компьютер, где информация обрабатывается и выводится в понятном для восприятия виде. Конструктивно RFID-метка обычно состоит из микрочипа, прикрепленного к радиоантенне. Компактность RFID-меток зависит от размеров внешних антенн, которые по размерам превосходят чип во много раз и, как правило, определяют габариты меток.

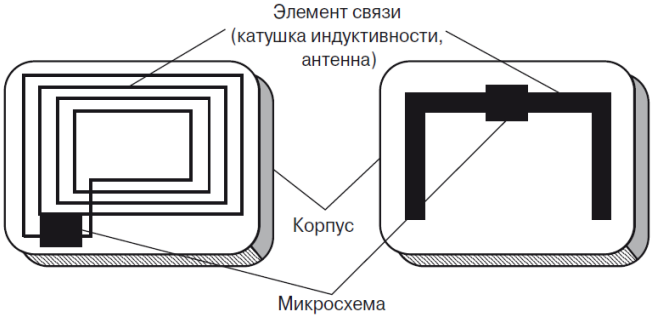


Рис. 2.3 – Принципиальная схема RFID метки: слева – метка с индуктивной связью, справа – микроволновая метка с антенной-диполем

RFID метки бывают *пассивные* и *активные* (рис. 2.4). Пассивные метки дешевле и не имеют батареи питания. В метке используется энергия электромагнитных волн, которые излучает считыватель. Такие метки применяются при отслеживании товаров, при контроле доступа, промышленной автоматизации и электронного слежения за товарами.

Рис. 2.4 – Пассивная (слева) и активная (справа) RFID метки

Активные RFID метки имеют батарею питания, которая позволяет работать с большей точностью и дальностью считывания. Но из-за наличия батареи активные метки имеют ограниченный срок службы и они более дорогие. Наиболее распространенный вариант их применения – удаленное слежение за объектами, имеющими высокую ценность и стоимость.

Существуют также *полуактивные* (*полупассивные*) метки, в которых имеется внутренний источник питания (например, батарея) и электроника для выполнения специализированных задач. Внутренний источник питания дает энергию для работы метки. Однако для передачи своих данных полуактивная метка использует энергию, излучаемую считывателем (ридером). Полуактивная метка также называется меткой со вспомогательной батареей. Обмен информацией между ридером и меткой такого типа всегда инициирует ридер, а затем начинает работу метка.

В свое время индустрия RFID столкнулась с проблемой «замкнутого круга» – метки не станут дешевле, пока не повысится спрос на них, а он не повысится, пока они не станут

дешевле. До недавнего времени относительно высокая стоимость RFID ограничивала ее использование. В настоящее время пассивные метки стоят от 20 центов, активные метки – от 10 до 50 долларов и выше.

По конструктивному исполнению выделяют следующие виды RFID меток: карты (пластиковые), самоклеящиеся этикетки бумажные и лавсановые, брелоки и диски.

Память метки – важный элемент RFID системы. В памяти может храниться различная информация, например, уникальный идентификатор объекта, место и дата выпуска продукта и т.п. Обычно объем памяти меток составляет от 16 бит до сотен килобит.

По типу памяти RFID-метки бывают следующих типов:

1) *только с чтением RO* (*Read Only*) – данные в них записывают только единожды, при их изготовлении, эти метки используются только для идентификации объекта;

2) с *однократной записью и многократным чтением WORM* (*Write Once Read Many*) – эти метки, кроме идентификатора содержат еще блок памяти, в которую можно однократно записать информацию и которую затем можно неоднократно считывать;

3) *с неоднократными записью и чтением RW* (англ. *Read and Write*) – содержат блок памяти и идентификатор, данные в этих метках можно перезаписывать неоднократно и соответственно стоят они дороже всех остальных меток;

4) *метки SAW-типа*, работающие на принципе поверхностной акустической волны ПАВ (Surface Acoustic Wave – SAW).

Метка SAW-типа в корне отличается от меток на основе микрочипов. Для работы меток SAW-типа используются радиоволны малой мощности в частотном диапазоне 2,45 ГГц. В отличие от меток с микрочипами SAW-метке не нужен источник постоянного тока для ее питания при передаче данных. SAW-метка состоит из дипольной антенны, присоединенной к встречно-штыревому преобразователю IDT (Interdigital TransDucer), расположенному на пьезоэлектрической подложке из ниобата лития или танталата лития (рис. 2.5). На подложке в точно рассчитанных местах расположены отдельные электроды, действующие как рефлекторы, изготовленные из алюминия или вытравленные на подложке. Антенна после приема радиочастотного сигнала от SAW-ридера подает электрический импульс на IDT. Этот импульс генерирует поверхностные волны, также называемые волнами Рэлея, и эти волны обычно проходят по подложке со скоростью от 3000 до 4000 м/с. Часть этих волн отражается рефлекторами обратно в IDT, а остальная часть поглощается подложкой. Отраженные волны образуют уникальную структуру, определяемую позициями рефлекторов и представляющую собой данные метки. Эти волны преобразуются в IDT обратно в радиосигнал и передаются через антенну метки назад RFID-ридеру. Затем ридер декодирует принятый сигнал и извлекает данные метки.

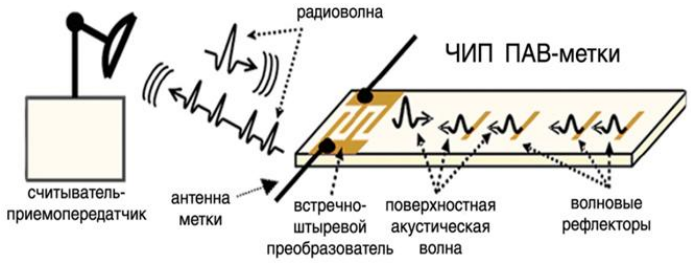


Рис. 2.5 – Конструкция SAW-метки

Основные технические характеристики системы радиочастотной идентификации на SAW-радиометках приведены в табл. 2.2.

Таблица 2.2 – Характеристики системы RFID на SAW-радиометках

Характеристика	**Значение**
Диапазон рабочих частот, ГГц	2,4 ÷ 2,483

Средняя мощность на выходе считывателя, мВт	не более 100
Вероятность ошибочного считывания или пропуска	10^{-9}
Количество кодов радиометок, шт.	10^{7} - 10^{9}
Рабочая температура считывателя, ^{o}C	от -40 до +50
Рабочая температура радиометки, ^{o}C	от -55 до +150
Дальность считывания, м	6 - 8

SAW-метка имеет следующие преимущества:

– очень малое потребление энергии, так как ей не нужен источник постоянного тока для своего питания;

– с ее помощью можно с хорошими результатами отмечать радионепрозрачные и радиопоглощающие материалы, например, металл и воду соответственно;

– большее расстояние чтения, чем у метки с микрочипом, работающей в том же частотном диапазоне;

– может работать с более короткими пачками радиосигналов в отличие от меток на микрочипах, требующих более продолжительного сигнала от ридера к метке;

– высокая степень точности чтения данных с метки;

– большая прочность вследствие простоты конструкции;

– не требует применения антиколлизионных протоколов;

– антиколлизионные протоколы необходимо реализовывать только на уровне ридера в отличие от меток с микрочипами, для которых такие протоколы нужны как на уровне ридера, так и на уровне метки (это снижает стоимость SAW-метки);

– SAW-ридеры менее подвержены влиянию помех от других SAW-ридеров.

SAW-метки могут, скорее всего, оказаться единственным вариантом в определенных ситуациях нанесения меток, и вероятно получат широкое распространение в будущем.

Рабочая частота метки – одна из самых важных характеристик соединения метки и считывателя. Значение используемой частоты зависит от приложений и мировых стандартов. Частоты определяют скорость передачи данных между меткой и считывателем. Чем ниже частота связи, тем меньше скорость. Однако здесь также огромную роль оказывает окружающая среда и тот объект, на котором размещается метка.

В RFID метках используется следующие диапазоны частот:

1. *Низкие частоты (НЧ) LF* (*Low Frequency*) – до 135 кГц. Регулирующий стандарт – ISO/IEC 18000-2. Такие метки лучше других работают вблизи жидкостей и металлов, из-за чего этот стандарт стал особенно популярным в области опознавания животных. НЧ метки могут считываться с расстояния в несколько сантиметров и имеют самую низкую скорость передачи данных. Пассивные метки данного диапазона имеют низкие цены, однако в связи с большой длиной волны существуют проблемы со считыванием на большие расстояния, а также проблемы, связанные с появлением коллизий при считывании.

2. *Высокая частота (ВЧ) HF* (*High Frequency*) – 13,56 МГц. Регулирующий стандарт – ISO/IEC 18000-3. Метки 13 МГц дешевые, не имеют экологических и лицензионных проблем, хорошо стандартизованы, имеют широкую линейку решений, в них используются стандартизованные алгоритмы шифрования. Широко применяются в таких областях, как карты контроля доступа, платежные карты, борьба с подделкой товаров, отслеживание книг и т.д. ВЧ метки могут считываться на расстоянии до 1м. Как и для диапазона LF, в системах, построенных в HF-диапазоне, существуют проблемы со считыванием на большие расстояния, считывание в условиях высокой влажности, при наличии металла, а также проблемы, связанные с появлением коллизий при считывании.

3. *Сверхвысокая частота UHF* (*Ultra High Frequency*) – 433 МГц. Регулирующий стандарт – ISO/IEC 18000-7. Метки данной частоты обладают наибольшей дальностью регистрации, во многих стандартах данного диапазона присутствуют антиколлизионные механизмы. В UHF RFID-системах по сравнению с LF и HF ниже стоимость меток, при этом выше стоимость прочего оборудования. Активные метки (радиометками с элементами питания) обеспечивают максимальную дальность считывания (до 1 км) и надежность считывания (100%). Основным минусом данных систем является стоимость меток, на порядок превышающая стоимость пассивных UHF меток.

5. *Сверхвысокие частоты (СВЧ) UHF (Ultra High Frequency)* – диапазон 860-930 МГц. Регулирующий стандарт – ISO/IEC 18000-6. Самый популярный диапазон в современных RFID системах. UHF метки могут считываться на расстоянии до 10 метров, и обеспечивают скорость передачи данных более 128 кбит/сек. Данный стандарт стал основным в таких областях, как логистика и управление цепочками поставок, благодаря усилиям мировых лидеров в этой области (Walmart, Metro Group, Департамент обороны США и др.). В настоящее время частотный диапазон СВЧ открыт для свободного использования в России в так называемом «европейском» диапазоне – 863-868 МГц.

6. *Микроволновые частоты SHF (Super High Frequency)* – 2,45-5,8 ГГц. Регулирующий стандарт – ISO/IEC 18000-3. Используются в таких областях, как промышленная автоматизация, электронный сбор платежей и контроль доступа. Имеют диапазон считывания, сопоставимый с UHF (СВЧ), и более высокие скорости передачи данных. Используемые метки являются в основном активными или полуактивными, что ограничивает области их применения.

Имеются также СВЧ метки UHF *ближнего поля* (*Near-Field*), которые, не являясь непосредственно радиометками, а используя магнитное поле антенны, позволяют решить проблему считывания в условиях высокой влажности, присутствия воды и металла. С помощью данной технологии ожидается начало массового применения RFID-меток в розничной торговле фармацевтическими товарами (нуждающимися в контроле подлинности, учёте, но при этом зачастую содержащими воду и металлические детали в упаковке) и в других областях. Более подробно коммуникации малого радиуса действия NFC рассмотрены в разд. 4.

В мире в основном используют HF и UHF частоты, поэтому в таблице 2.3 приведены различия между этими типами меток.

Таблица 2.3 – Характеристики и области применения HF и UHF меток

Частоты	**Основные характеристики**	**Область применения**
HF 13,56 МГц (высокая частота)	Соответствие общемировым стандартам Размер метки больше, чем UHF Дистанция считывания 1,2 м Низкая погрешность при чтении защитных ворот Цена меток выше, чем UHF Вблизи металлов работают недостаточно эффективно	Платежные карты и карты лояльности (смарт-карты) Контроль доступа Борьба с подделкой Различные решения для поштучного отслеживания книг, багажа, одежды и т.д. “Умные полки” Опознавание людей и личный контроль
UHF 860-930 МГц (сверхвысокие частоты)	Несовместимы из-за различия существующих региональных правил и нормативов Размер метки меньше, чем у HF Имеют больший, чем у HF- метки, диапазон считывания (более 3 м) Цена меток ниже, чем HF Получают развитие благодаря усилиям участников розничных цепочек поставок товаров Чувствительность к жидкостям и металлам	Логистика и цепочки поставок, включая: Управление запасами Складской менеджмент Отслеживание активов

2.3 Считывающие устройства RFID

Для извлечения данных, хранящихся на RFID-метке, используется считывающее устройство – ридер (англ., *reader*). Типичный ридер имеет одну или несколько антенн, которые излучают радиоволны и принимают сигналы от метки (рис. 2.6). Далее полученная информация (идентификационный номер метки, ID считывающего устройства и время, когда метка была прочитана) в цифровом виде передается в компьютерную систему для дальнейшей обработки. Следует учитывать, что считыватели должны работать на той частоте, для которой предназначены метки.

Функции, выполняемые RFID-считывателем:

1. Энергоснабжение пассивных меток за счет передачи энергии меткам с использованием электромагнитного поля.

2. Чтение данных, которые хранятся на метке.

3. Запись данных на метку – используя метки с возможностью чтения-записи, данные можно менять, добавлять новые и удалять старые, в любое время на протяжении всего жизненного цикла продукта.

4. Связь с компьютерной системой - считыватель отвечает за транспортировку информации между метками и компьютерной системой, это происходит посредством порта Bluetooth, сети Ethernet или других проводных или беспроводных технологий.

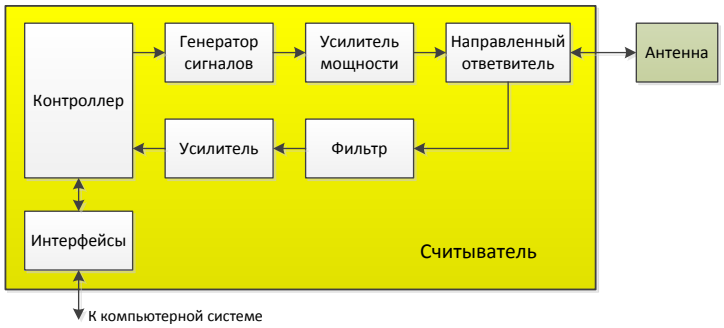


Рис. 2.6 – Структурная схема RFID-считывателя

Конструктивно считыватели бывают ручные, настольные и стационарные (рис. 2.7). Каждый из них используется в зависимости от необходимых потребностей. Ручные считыватели применяются для поиска нужных товаров и применяются на складах, в библиотеках, в розничных магазинах и т.д. Стационарные считыватели используются как для считывания, так и для программирования RFID меток. С помощью них можно записать, стереть, перезаписать информацию с метки. В основном они используется в библиотеках, на складах.

а) б) в)

Рис. 2.7 – Считыватели (ридеры) RFID-меток (изображения не в масштабе): а) портативный (ручной); б) настольный (RFID-планшет); в) стационарный (RFID-ворота)

Метку и считыватель соединяет радиоканал связи для передачи данных, который организуется с использованием антенн. Очевидно, что дальность действия системы RFID зависит от размеров антенн, имеющихся у меток и считывателей. Антенны могут быть двух видов: вмонтированные в метку и корпусированные. В первом случае антенна RFID-метки монтируется на ту же поверхность, что и микрочип и помещается с ней в один корпус. Размеры корпуса метки обычно определяется размером и формой антенны. Сам микрочип метки же может быть крайне мал.

В зависимости от потребностей приложений подходы к корпусировке антенн считывателей имеют свои различия. В переносных устройствах, антенна крепится на сам считыватель, в других, размещается на расстоянии от него. Здесь может быть смонтировано сразу несколько антенн (так называемые RFID-ворота, рис. 3.7в), которые расположены

таким образом, что позволяет повысить качество считывания и дальность сигналов радиоволн.

2.4 Стандартизация технологии RFID

В настоящее время не существует единых международных стандартов в технологии RFID. Далее представлен краткий обзор важнейших из них.

Международная организация по стандартизации ISO (International Organization for Standardization) совместно с Международным инженерным консорциумом IEC (International Electrotechnical Commission) разработала серию RFID-стандартов ISO/IEC 18000 для автоматической идентификации и контроля предметов снабжения. Эта серия охватывает протокол радиоинтерфейса для систем, используемых в системах поставок, и включает 7 основных радиочастот RFID-технологии со всего мира.

ISO разработала также международные стандарты, которые регулируют радиочастотную идентификацию животных, которая обычно осуществляется имплантацией транспондера (микрочипа) под кожу животного. Так ISO/IEC 11784 определяет, каким образом данные записаны на метку, а ISO/IEC 11785 устанавливает протокол радиоинтерфейса. Кроме этого ISO создала стандарт протокола для RFID-меток, используемых в платежных системах и бесконтактных смарт-картах (ISO/IEC 14443) и картах дальнего действия (ISO/IEC 15693). Организация также установила стандарты для тестирования RFID-меток и считывателей на соответствия техническим требованиям (ISO/IEC 18047) и на требования к проведению испытаний технических характеристик устройств (ISO/IEC 18046).

Центр Auto-ID, который был создан для разработки *электронного кода продукта EPC* (*Electronic Product Code*), предложил свой собственный протокол радиоинтерфейса (отличный от стандарта ISO) для отслеживания товаров в международной логистической цепи. Первоначально Центр планировал создать единый протокол, который бы мог связываться с различными типами (классами) меток. Каждый последующий тип меток должен быть более сложным, чем предыдущий:

Класс 1: простая, пассивная метка обратного рассеяния, доступная только для считывания, с программируемой долговременной памятью однократного использования.

Класс 2: пассивная метка обратного рассеяния с объемом памяти 65 Кбит, которую можно считывать и перезаписывать.

Класс 3: полупассивная метка обратного рассеяния с объемом памяти 65 Кбит, которую можно считывать и перезаписывать; фактически это Класс 2 со встроенной батареей для поддержания расширенной зоны действия считывателей.

Класс 4: активная метка со встроенной батареей для управления схемой микрочипа и снабжения радиопередатчика электроэнергией, чтобы излучать сигнал считывателю.

Класс 5: активная RFID-метка, которая может связываться с другими метками Класса 5 и/или другими устройствами.

Позже типы меток изменились и со временем Центр Auto-ID утвердил также метки Класса 0, доступные только для чтения и программируемые в момент сборки. Метка Класса 0 использовала отличный от Класса 1 протокол, а это означало, что потребителям приходилось покупать многопротокольные считыватели, чтобы иметь возможность считывать метки и Класса 1, и Класса 0.

Протоколы Класса 0 и Класса 1 имеют пару недостатков, включая тот факт, что они не могут взаимодействовать друг с другом. Одна из проблем заключается в том, что они несовместимы со стандартами ISO. Другая проблема – невозможность применения повсеместно. К примеру, Класс 0 излучает сигнал на одной частоте и принимает обратный уже на другой, но в СВЧ диапазоне, что запрещено в Европе.

С 2003 года после закрытия центра Auto ID Labs разработкой стандартов в области сверхвысоких частот UHF занимается организация EPCglobal Inc., целью которой является установление всемирных стандартов для разработки, реализации и принятия электронного кода продукта EPC и создание сети EPCglobal. Спецификация EPCglobal, нацеленная на операции в сетях сбыта, является наиболее глобальной спецификацией для RFID и применяется в очень широком наборе прикладных систем. Существует два поколения стандартов EPC. Первое поколение определяло только метки класса 0 и класса 1. Метки класса 0 программировались во время изготовления «R/O». В метки класса 1 информация могла быть записана только один раз пользователем, при создании метки для конкретного приложения «WORM». Класс 0 и класс 1 имеют различные протоколы для работы со считывателем.

Существуют модификации классов, которые поддерживаются «открытыми» стандартами EPC Global. Наиболее широко используемые модификации это класс 0 g1, который отличается размером памяти (96 бит вместо принятых изначально 64 бита) и класс 1b (C1bg2), где всего 128 бит, 96 бит из которых (EPC-код) доступны для многократной перезаписи.

Для устранения проблем, возникающих при работе с метками первого поколения, в 2004 году EPC Global введен стандарт второго поколения для транспондеров, работающих в области ультравысоких частот, именуемый EPC Generation 2 – общий протокол обмена данными для всех продуктов второго поколения. Протокол разработан для меток Класса 1 gen2, но должен подходить для работы с разрабатываемыми в перспективе классами (планируется создание меток класса 2, 3, 4 и 5).

2.5 Современное состояние и перспективы развития технологии RFID

Технологию радиочастотной идентификации вооруженные силы стали применять в середине XX века, а отправной точкой ее активного внедрения для гражданских нужд считают 1990-е годы, когда Международная организация по стандартизации (ISO) приняла ряд основополагающих стандартов в области RFID. В начале XXI века технология радиочастотной идентификации стала активно внедряться на практике, например компания Walmart и Министерство вооруженных сил США обязывали своих поставщиков использовать RFID для маркировки поставляемой им продукции. Прогнозировалось, что производство RFID-систем в скором времени выйдет на промышленные масштабы и технология начнет применяться повсеместно. Но к 2005 году темпы развития RFID-технологии несколько замедлились, и интерес к ее использованию снизился.

Основными причинами этого принято считать:

– появление ряда научных исследований, заверяющих о небезопасности использования радиометок;

– сложность изменения некоторых технических характеристик радиоидентификационных систем;

– сложности в снижении цены RFID-метки.

Наиболее востребованной в течение последних пяти лет технология RFID оказалась в сфере государственных проектов, розничной торговле, логистике и на транспорте, на которые приходилось около 60% доходов. В последние годы наибольшим спросом RFID-метки пользовались в сферах розничной торговли (27%), безопасности (15,2%) и документации населения (14,4%). Ожидается, что отрасли производства, транспорта и розничной торговли будут вносить наибольший доход в общий объем RFID-рынка. Помимо перечисленных направлений, ежегодно производители и интеграторы готовых решений выводят на рынок все больше идей по использованию RFID, что, несомненно, расширяет сферы применения этой технологии.

Причиной, мешающей успешной реализации RFID-проектов, становятся как финансовые, так и нефинансовые барьеры. Наиболее явной является проблема высокой цены

оборудования, вызванная неоправданными ожиданиями снижения стоимости меток в ближайшем будущем. Таким образом, возникает замкнутый круг: нет заказов – цена метки высока, нет доступных ценовых решений – нет заказов. Чтобы выйти из этой тупиковой ситуации, нужны крупномасштабные проекты, например государственные. Без вмешательства государства массовый переход на новый способ маркировки и идентификации товаров практически невозможен.

Многие эксперты оправдывают медленное развитие RFID-рынка отсутствием стандартов, способствующих возможности интеграции оборудования различных производителей в одной системе. Решением этой проблемы активно занимаются национальные представительства Ассоциации автоматической идентификации (GS1). Количество российских стандартов пока невелико, однако процесс их разработки происходит активно. Все принимаемые стандарты, как правило, аутентичны международным стандартам, которые разрабатываются ISO.

В целом, несмотря на сильную переоценку RFID-рынка в прошлом, следует отметить его сегодняшнее постепенное развитие. В настоящее время применение RFID-систем активно продвигается в тех отраслях, где-либо отсутствует возможность идентификации с помощью других технологий, либо же их применение экономически не оправдано. Таким образом, массовое внедрение RFID-технологий – это реальность, но далеко не всех сфер экономики.

2.6 Области применения RFID-технологий

Радиочастотная идентификация относится к ключевым технологиям будущего и является базовой технологий в Интернете вещей. Вот лишь несколько характерных примеров применения RFID в различных областях человеческой деятельности.

Промышленность и сельское хозяйство

Технология RFID обеспечивает улучшенное управление складскими запасами и позволяет значительно повысить эффективность логистических процессов в промышленности. Например, промышленные компании используют RFID-систему для контроля над важными комплектующими, перемещающимися от одного цеха к другому, что обеспечивает автоматический контроль, уменьшение количества ошибок и затрат на поиск необходимых деталей на производственной линии.

Реализованы проекты автоматизации заправки автотранспортных средств и автоматической идентификации автотранспорта с использованием технологии RFID. Система обеспечивает прозрачный и достоверный учет топлива при проведении всех технологических и документарных операций, эффективное планирование и контроль потребления моторного топлива по каждой единице автотехники, безоператорный отпуск топлива только авторизованным автомашинам при помощи RFID-меток без использования бумажных носителей и смарт-карт.

Чтобы защитить свою продукцию от подделок, фармацевтические предприятия помещают транспондеры на упаковках медикаментов. Благодаря этому удается отслеживать путь препаратов от изготовителя до аптеки.

Во многих странах фермеры маркируют крупный рогатый скот посредством помещения транспондеров на ухо животного. Таким образом, при внезапной вспышке болезни или эпидемии стадо становится возможным быстро изолировать.

Государственные и общественные учреждения

Некоторые библиотеки внедрили RFID в свои системы книгообмена. При этом в книгах, на пленках и на компакт-дисках размещаются транспондеры. В результате

посетители могут самостоятельно оперативно получать выбранные ими носители информации, причем благодаря транспондерам эти носители надежно защищены от кражи. Использование RFID-меток позволяет автоматизировать процесс выдачи и возврата носителей, более эффективно проводить инвентаризацию и защитить фонд от краж. Кроме того, читательские билеты также можно оснастить RFID-метками, что позволит бороться с их подменами и подделками.

Больницы также используют радиочастотную идентификацию для того, чтобы облегчить идентификацию пациентов и оптимизировать их размещение в палатах. Пациенты снабжаются ручными браслетами с интегрированными в них транспондерами, в которых закодированы имя пациента и номер истории его болезни, хранящейся в электронной базе данных. Посредством мобильного компьютера со считывающим устройством лечащий врач получает оперативный доступ к историям болезни своих пациентов.

В музеях посетители могут при помощи персонального цифрового помощника PDA (Personal Digital Assistant) запрашивать информацию о выставочных экспонатах, для чего экспонаты снабжаются транспондерами RFID. При этом сотрудники музеев получают информацию о том, какими экспонатами интересуются особенно часто.

Наука

Исследователи прослеживали с помощью технологии RFID жизнь пчел. Крошечные чипы приклеивались на спинки насекомых. Полученная при этом информация о деятельности пчел, помимо прочего, помогает эффективнее бороться с болезнями.

Ученые с помощью технологии RFID наблюдали рост генетически измененных деревьев. Эта система заметно превосходила все прежние методы маркировки, поскольку транспондер, помещенный внутрь дерева, защищен от воздействия окружающей среды.

Быт и досуг

Потребители уже сегодня практически ежедневно сталкиваются с системами RFID. Например, во многих странах транспондеры интегрируются в заграничные паспорта, а в некоторых клубах — в членские карточки.

Технология RFID уже долго и успешно используется как электронный ключ для управления доступом в помещения. Преимущество RFID-карты по сравнению с магнитной картой в том, что нет никакого контакта между картой и считывателем, она меньше изнашивается, меньше дополнительного обслуживания.

RFID технология также завоевывает популярность как удобный способ оплаты различных услуг. Один из популярных способов - оплата дорожных пошлин без остановки автомобиля. RFID также начинает использоваться как удобный способ оплаты проезда в автобусах, метро и поездах. Многие города в мире перешли от карт с магнитной полосой к RFID-картам, так как это позволяет людям быстрее проходить через турникеты, уменьшает скопление и ускоряет обслуживание в кассах.

В некоторых парках отдыха посетители могут с помощью RFID поддерживать связь друг с другом. Считывающие приборы регистрируют браслет с интегрированным транспондером и указывают местоположение пользователя на стационарно расположенных экранах. Посредством этих сенсорных экранов посетители могут посылать и принимать сообщения.

RFID также используется для охраны собственности. Большинство современных автомобилей идет в комплекте со считывающим RFID-устройством в рулевой колонке. Ретранслятор вставлен в пластмассу вокруг основы ключа. Ридер должен получить удостоверение личности от ключа или автомобиль не будет заводиться.

Активные RFID-метки могут быть объединены с датчиками тревоги: например, если оружие на объектах переносится без разрешения – раздается сигнал тревоги. RFID-метки

могут быть в компьютерах с ценной информацией: так файл не будет удалён без удостоверения личности и проверки прав доступа.

Приведенные примеры далеко не исчерпывают перечень основных приложений, в которых применение бесконтактной идентификации не только удобно, но и экономически оправдано.

Контрольные вопросы по главе 2

1. Каково назначение системы радиоидентификации RFID?
2. Какие элементы входят в состав RFID-системы?
3. Сравните характеристики систем RFID и на базе штрих-кода.
4. Как устроена RFID-метка? Какие метки бывают?
5. В чем особенность RFID-меток, работающих на принципе поверхностной акустической волны ПАВ?
6. Какие частотные диапазоны используются в RFID-метках?
7. Поясните функции и устройство считывающих устройств RFID-систем.
8. Каково состояние стандартизации технологии RFID?
9. Какие проблемы мешают более массовому внедрению технологии RFID?
10. Приведите примеры применений технологии RFID в различных областях деятельности.

ГЛАВА 3 БЕСПРОВОДНЫЕ СЕНСОРНЫЕ СЕТИ WSN

3.1 Основные понятия и принципы сенсорных сетей

Определим основные понятия сенсорных сетей.

Сенсор (англ., sensor) – устройство, которое воспринимает контролируемое воздействие (свет, давление, температуру и т. п.), измеряет его количественные и качественные характеристики и преобразует данные измерения в сигнал. Сигнал может быть электрический, химический или другого типа.

Датчик (англ., transducer) – устройство, которое используется для преобразования одного вида энергии в другой. Следовательно, сенсор также является датчиком, который преобразует физическую информацию в электрическую, которая может быть передана вычислительной системе или контроллеру для обработки.

Актуатор (англ., actuator) – исполнительное устройство, которое реагирует на поступивший сигнал для изменения состояния управляемого объекта. В актуаторе происходит преобразование типов энергии, например, электрическая энергия, либо энергия сжатого (разреженного) воздуха (жидкости, твёрдого тела) преобразуется в механическую.

Сенсорный узел (англ., sensor node) – это устройство, которое состоит, по крайней мере, из одного сенсора (может также включать один или нескольких актуаторов), и имеет вычислительные и проводные или беспроводные сетевые возможности.

Сенсорная сеть – система распределенных сенсорных узлов, взаимодействующих между собой, а также с другими сетями для запросов, обработки, передачи и предоставления информации, полученной от объектов реального физического мира с целью выработки ответной реакции на данную информацию. Таким образом, сенсорная сеть включает в себя как минимум сенсоры, актуаторы и коммуникационные узлы. Основной областью применения сенсорной сети является контроль и мониторинг измеряемых параметров физических сред и объектов и в некоторых случаях – управление этими объектами (активация в них определенных процессов). Примеры сенсорных сетей: всепроникающие сенсорные сети (USN – Ubiquitous Sensor Network), сети для транспортных средств (VANET – Vehicular Ad Hoc Network), муниципальные сети (HANET – Home Ad hoc Network), медицинские сети (MBAN(S) – Medicine Body Area Network (services)) и др. Основные действия, выполняемые при работе сенсорных сетей, представлены на рис. 3.1 (пунктиром показаны необязательные процессы).

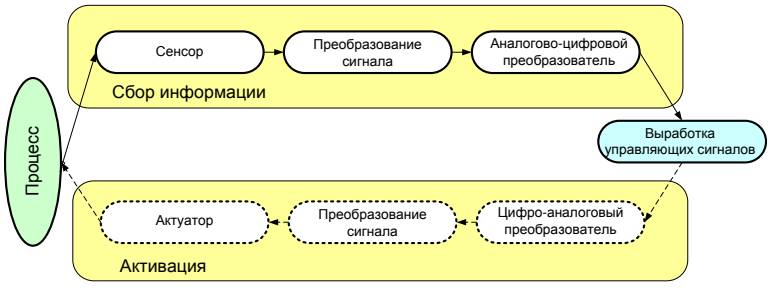


Рис. 3.1 – Сбор данных и управление в сенсорных сетях

Область покрытия сенсорной сети может составлять от нескольких метров до нескольких километров за счёт способности ретрансляции сообщений от одного элемента сети к другому. Сенсорная сеть обладает способностью к ретрансляции сообщений по цепочке от одного узла к другому, что позволяет в случае выхода из строя одного из узлов организовать передачу информации через соседние узлы без потери качества. Сама сеть определяет оптимальный маршрут движения информационных потоков (рис. 3.2).

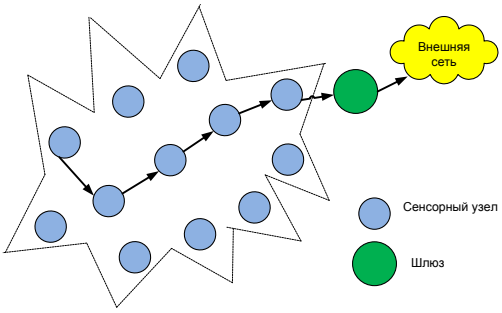


Рис. 3.2 – Маршрутизация информации в сенсорной сети

Самоорганизующаяся (лат. ad hoc – «по месту») сеть связи – сеть, в которой число узлов является случайной величиной во времени и может изменяться от 0 до некоторого максимального значения. Взаимосвязи между узлами в такой сети также случайны во времени и образуются для передачи информации между подобными узлами и во внешнюю сеть связи.

Беспроводная сенсорная сеть (БСС) (англ. WSN – Wireless Sensor Network) – распределённая, самоорганизующаяся сенсорная сеть множества сенсоров и исполнительных устройств, объединенных между собой посредством радиоканалов.

Достоинства беспроводных сенсорных сетей:

– способность к самовосстановлению и самоорганизации;

– способность передавать информацию на значительные расстояния при малой мощности передатчиков (путем ретрансляции);

– низкая стоимость узлов и их малый размер;

– низкое энергопотребление и возможность электропитания от автономных источников;

– простота установки, отсутствие необходимости в прокладке кабелей (благодаря беспроводной технологии и питанию от батарей);

– возможность установки таких сетей на уже существующий и эксплуатирующийся объект без проведения дополнительных работ;

– низкая стоимость технического обслуживания.

Так как на практике в наибольшей степени распространены беспроводные сенсорные сети, поэтому основная часть материала главы посвящена именно таким сетям.

3.2 Базовая архитектура сенсорной сети

Стандартизацией сенсорных сетей занимаются многие международные организации, среди которых ISO, IEC, ITU-T, IEEE и др. Так исследовательская группа по сенсорным сетям SGSN (Study Group on Sensor Networks) объединённого технического комитета №1 ISO/IEC JTC 1 (Joint Technical Committee 1) определила базовую архитектуру сенсорной сети и ее основные интерфейсы (рис. 3.3).

Как видно из рисунка, сенсорный узел состоит из:

– аппаратного обеспечения;

– базового программного обеспечения;

– прикладного программного обеспечения.

В составе архитектуры определены четыре базовых интерфейса:

1. Интерфейс между базовым и прикладным программным обеспечением сенсорного узла.

2. Интерфейс между базовым программным обеспечением и аппаратным обеспечением сенсорного узла (сенсоры, актуаторы и/или коммуникационный узел и т.д.).

3. Беспроводные или проводные интерфейсы между узлами в сенсорной сети.

4. Интерфейс между сенсорной сетью и внешней средой (провайдеры услуг, пользователи).

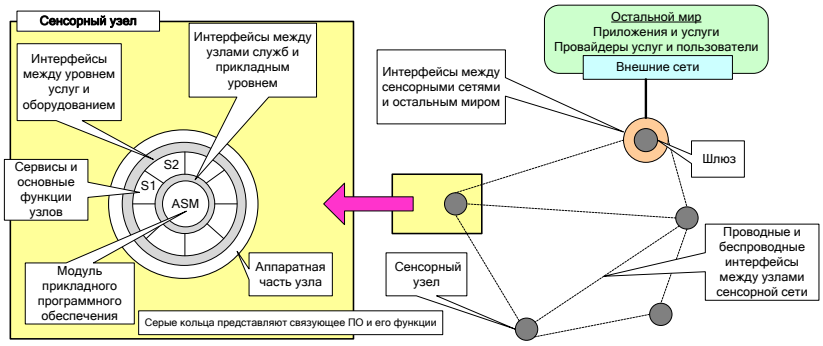


Рис. 3.3 – Основные элементы и интерфейсы сенсорной сети

3.3 Узлы беспроводной сенсорной сети

БСС состоят из миниатюрных вычислительных устройств, снабжённых датчиками, актуаторами и трансиверами (приемопередатчиками), работающими в заданном диапазоне радиочастот. Такой узел БСС называют *сенсорным узлом* или просто *сенсором*. Сенсорный узел представляет собой плату размером обычно не более одного кубического дюйма. На плате размещаются процессор, память - флэш и оперативная, цифро-аналоговые и аналого-цифровые преобразователи, радиочастотный приемопередатчик, источник питания и различные датчики, актуаторы. Таким образом, аппаратная часть узла беспроводной сети может быть разделена на следующие четыре подсистемы (рис. 3.4):

1) *коммуникационная подсистема* – обеспечивает беспроводные соединения с другими узлами в сенсорной сети и содержит радио приемопередатчик;

2) *вычислительная подсистема* – обеспечивает обработку данных и функциональность узла и состоящая из микроконтроллера MCU, в состав которого входят процессор, оперативная SRAM, энергонезависимая EEPROM и флэш-память, аналого-цифровой преобразователь ADC, таймер, порты ввода/вывода;

3) *сенсорная подсистема* – обеспечивает соединение сенсорного беспроводного узла с внешним миром, в состав которой могут входить аналоговые и цифровые сенсоры, актуаторы;

4) *подсистема электропитания* – обеспечивает энергетическое снабжение всех элементов беспроводного сенсорного узла и включает устройства генерации и аккумулирования энергии, а также регулировки напряжения.

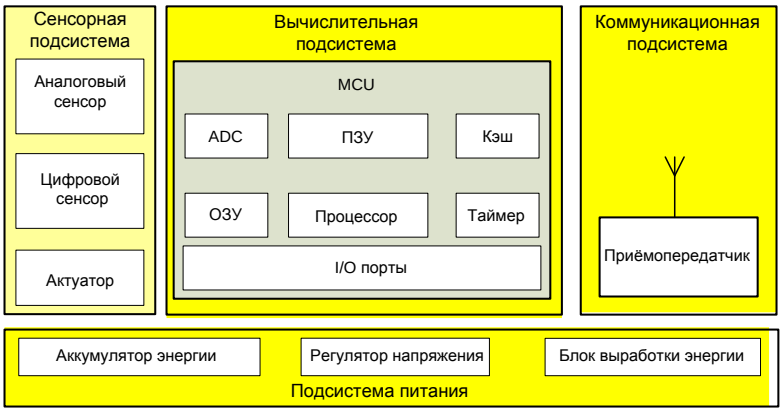


Рис. 3.4 – Узел беспроводной сенсорной сети

Датчики могут быть самыми разнообразными. Чаще других используются датчики температуры, давления, влажности, освещенности, вибрации, местоположения, реже – магнитоэлектрические, химические (например, измеряющие содержание CO, CO_2, уровень радиационного фона), звуковые и некоторые другие. Набор применяемых датчиков зависит от функций, выполняемых беспроводными сенсорными сетями.

Полученные от датчика электрические сигналы часто не готовы для обработки, поэтому они проходят в моте через стадию преобразования. Например, сигнал часто требует усиления для увеличения амплитуды, возможно применение фильтров для устранения нежелательного шума в определенных диапазонах частот и т.п. Преобразованный сигнал трансформируется при помощи аналого-цифрового преобразователя (АЦП) в цифровой сигнал. В итоге сигнал получается в цифровой форме и он готов к дальнейшей обработке в процессоре и хранению в памяти микроконтроллера. При наличии исполнительных механизмов возможна также передача управляющих воздействий от узлов сети к внешней среде через актуатор. Питание сенсорного узла осуществляется обычно от небольшой батареи.

Помимо размера, есть и другие жесткие ограничения для узлов БСС. Они должны:

- потреблять очень мало энергии;
- работать с большим количеством узлов на малых расстояниях;
- иметь низкую стоимость производства;
- быть автономными и работать без обслуживания;
- адаптироваться к окружающей среде.

Внешний вид сенсорных узлов приведен на рис. 3.5.

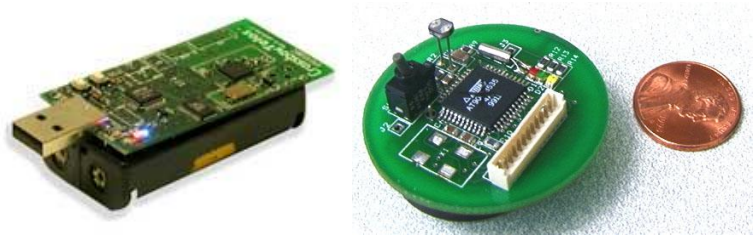


Рис. 3.5 – Внешний вид сенсорных узлов

Для выполнения функций на каждый сенсорный узел устанавливается специализированная операционная система (ОС). Примером широко известной операционной системы для сенсорных узлов является разработанная в Университете Беркли система с открытым кодом TinyOS – это управляемая событиями операционная система реального времени, рассчитанная на работу в условиях ограниченных вычислительных ресурсов. Эта ОС позволяет сенсорам автоматически устанавливать связи с соседями и формировать сенсорную сеть заданной топологии.

В качестве примера в табл. 3.1 приведены параметры сенсорных узлов ML-Node-Z (компании MeshLogic, Россия) и ZigBit (компании Atmel, США). Следует отметить, что интегрированных сенсорных датчиков на этих платах нет.

Таблица 3.1 Характеристики сенсорных узлов

Параметры	**Тип сенсорного узла:**	
	ML-Node-Z	**ZigBit**
Микроконтроллер		
Процессор	Texas Instruments	ATmega1281

	MSP430	
Тактовая частота	От 32,768 кГц до 8 МГц	4 МГц
Оперативная память, Кбайт	10	8
Flash-память, Кбайт	48	128
Приемопередатчик		
Тип	IEEE 802.15.4	IEEE 802.15.4
Диапазон частот, МГц	2400 - 2483,5	2400 - 2483,5
Скорость передачи данных, Кбит/с	250	250
Выходная мощность, дБм	От –24 до 0	От –28 до 3
Чувствительность, дБм	–95	–101
Антенна	Чип	1 или 2 чипа
Внешние интерфейсы		
АЦП	12-разрядный, 7 каналов	10-разрядный, 3 канала
Цифровые интерфейсы	I2C/SPI/UART/USB	I2C/SPI/UART/IRQ/JTAG
Другие параметры		
Напряжение питания, В	От 0,9 до 6,5	От 1,8 до 3,6
Размеры, мм	44x33x10	19x14x3
Температурный диапазон, °С	От –40 до 85	От 0 до 85

Поскольку одной из важнейших функций сенсоров является автоматический выбор схемы организации сети и маршрутов передачи данных, беспроводные сенсорные сети по существу являются самонастраиваемыми. Чаще всего сенсорный узел должен иметь возможность самостоятельно определить свое местоположение, по крайней мере, по отношению к тому другому сенсору, которому он будет передавать данные. То есть сначала происходит идентификация всех сенсоров, а затем уже формируется схема маршрутизации.

Сенсорные узлы могут закрепляться стационарно, а также иметь относительную мобильность, то есть произвольно перемещаться друг относительно друга в некотором пространстве, не нарушая при этом логической связанности сети. В последнем случае сенсорная сеть не имеет фиксированной постоянной топологии, и ее структура динамически меняется с течением времени.

3.4 Способы передачи данных в БСС

В сенсорной сети узлы обычно общаются посредством беспроводной связи. Связь может осуществляться посредством радио, инфракрасного излучения (ИК-порта) или оптических сигналов. Одним из наиболее распространенных вариантов радиосвязи является

использование полос частот для промышленных, научных и медицинских целей ISM (Industrial, Scientific and Medical), которые определены Сектором радиосвязи Международного союза электросвязи ITU-R и доступны без лицензий в большинстве стран (табл. 3.2).

Некоторые из этих частот уже используются в беспроводных локальных сетях (WLAN). Для сенсорных сетей малого размера и низкой стоимости усилитель сигнала не требуется. Аппаратные ограничения и нахождения компромисса между эффективностью антенны и потреблением энергии накладывают определенные ограничения на выбор частоты передачи в диапазоне сверхвысоких частот. Чаще всего используются следующие частоты ISM - 433 МГц в Европе и 915 МГц в Северной Америке. Основными преимуществами использования радиочастот ISM является широкий спектр частот и доступность по всему миру. Они не привязаны к конкретному стандарту, тем самым дают большую свободу для реализации энергосберегающих стратегий в сенсорных сетях.

Таблица 3.2 – Полосы частот ISM, определенные ITU-R

Диапазон частот		**Полоса**	**Центральная частота**	**Область применения**
6.765 МГц	6.795 МГц	30 КГц	6.780 МГц	Локальное применение
13.553 МГц	13.567 МГц	14 КГц	13.560 МГц	
26.957 МГц	27.283 МГц	326 КГц	27.120 МГц	
40.660 МГц	40.700 МГц	40 КГц	40.680 МГц	
433.050 МГц	434.790 МГц	1.84 МГц	433.920 МГц	Европа, Африка, Ближний Восток, Россия
902 МГц	928 МГц	26 МГц	915 МГц	Северная и Южная Америка
2.4 ГГц	2.5 ГГц	100 МГц	2.45 ГГц	
5.725 ГГц	5.875 ГГц	150 МГц	5.8 ГГц	
24 ГГц	24.25 ГГц	250 МГц	24.125 ГГц	
61 ГГц	61.5 ГГц	500 МГц	61.25 ГГц	Локальное применение
122 ГГц	123 ГГц	1 ГГц	122.5 ГГц	Локальное применение
244 ГГц	246 ГГц	2 ГГц	245 ГГц	Локальное применение

В России на основании Решения Государственной комиссии по радиочастотам (ГКРЧ) № 08-24-01-001 от 28.04.2008 и № 07-20-03-001 от 07.05 2007 в качестве ISM выделены частотные диапазоны LPD (англ. Low Power Device) 433,075 – 434,750 МГц, PMR (англ. Private Mobile Radio) 446,00625 – 446,09375 и 868,7 – 869,2 МГц. Эти радиочастоты могут использоваться без оформления специального разрешения ГКРЧ и совершенно бесплатно при условии соблюдения требований по ширине полосы, излучаемой мощности (до 10 мВт в районе частоты 434 МГц, до 500 мВт в районе частоты 446 МГц и до 25 мВт в районе частоты 868 МГц) и назначению радиопередающего изделия.

Другим возможным способом связи в сенсорных сетях является использование ИК-портов. ИК-связь доступна без лицензии и защищена от помех электрических приборов. ИК-передатчики дешевле и проще в производстве. Многие из сегодняшних ноутбуков, КПК и мобильных телефонов используют ИК-интерфейс для передачи данных. Основным недостатком такой связи является требование прямой видимости между отправителем и

получателем. Это делает ИК-связь нежелательной для использования в сенсорных сетях из-за среды передачи.

Имеются также узлы БСС, которые используют для передачи оптическую среду. Применяются две схемы передачи - пассивная с использованием светоотражателя CCR (Corner-Cube Retroreflector) и активная с использованием лазерного диода и управляемых зеркал. В первом случае не требуется интегрированный источник света, для передачи сигнала используется конфигурации из трех зеркал CCR. Активный метод использует лазерный диод и систему активной лазерной связи для отправки световых лучей приемнику.

Особые требования к применению сенсорных сетей делают выбор среды передачи сложной задачей. Например, морские приложения требуют использования водной среды передачи. Здесь нужно использовать длинноволновые излучения, которые могут проникать сквозь поверхность воды. В труднодоступной местности или на поле боя могут возникнуть ошибки и большие помехи. Кроме того может оказаться, что антенны узлов не обладают нужной высотой и мощностью излучения для связи с другими устройствами. Следовательно, выбор передающей среды должен сопровождаться надежными схемами модуляции и кодирования, что зависит от характеристик передающего канала.

3.5 Протоколы и технологии передачи данных в БСС

По размерам физической зоны размещения БСС относятся к классу беспроводных персональных вычислительных сетей WPAN (Wireless Personal Area Networks). Важнейшим фактором при работе беспроводных сенсорных сетей является ограниченная емкость батарей, устанавливаемых на сенсорные узлы. Следует учитывать, что заменить батареи чаще всего невозможно. В связи с этим необходимо выполнять на сенсорах только простейшую первичную обработку, ориентированную на уменьшение объема передаваемой информации, и, что самое главное, минимизировать число циклов приема и передачи данных. Для решения этой задачи разработаны специальные коммуникационные протоколы.

Наиболее известными из протоколов БСС являются протоколы альянса ZigBee. Для выработки стандарта стека протоколов для беспроводных сенсорных сетей альянс ZigBee использовал разработанный ранее стандарт IEEE 802.15.4, который описывает физический уровень и уровень доступа к среде для беспроводных сетей передачи данных на небольшие расстояния (до 75 м) с низким энергопотреблением, но с высокой степенью надежности. Стандарт IEEE 802.15.4 является базовой основой не только для протоколов ZigBee, но и других более высокоуровневых протоколов (6loWPAN, DigiMesh и др.), и позволяет строить с помощью программных надстроек на сетевом уровне и выше любую топологию сети (см. разд. 3.7).

На данный момент альянс ZigBee разработал единственный в этой области стандарт, который подкреплен наличием производства полностью совместимых аппаратных и программных продуктов. Протоколы ZigBee позволяют создавать самоорганизующиеся и самовосстанавливающиеся сенсорные сети. Устройства ZigBee сети благодаря встроенному программному обеспечению обладают способностью при включении питания сами находить друг друга и формировать сеть, а в случае выхода из строя какого-либо из узлов могут устанавливать новые маршруты для передачи сообщений. Протоколы ZigBee позволяют устройствам находиться в спящем режиме большую часть времени, что значительно продлевает срок службы батареи. Дальность уверенной передачи радиосигнала узлов ZigBee сети зависит от многих параметров (в первую очередь – от чувствительности приемника и мощности передатчика), но в среднем расстояние между узлами сети Zigbee на открытом пространстве составляет сотни, а в помещении – десятки метров.

Самоорганизующиеся сенсорные сети могут быть реализованы также на основе беспроводной технологии *Bluetooth*. Такие сети состоят из ведущих и ведомых устройств (эти роли могут совмещаться), способных передавать данные как в синхронном, так и в

асинхронном режимах. Синхронный режим передачи предполагает прямую связь между ведущим и ведомым устройствами с закрепленным каналом и временными слотами доступа. Данный режим используется в случае ограниченных по времени передач. Асинхронный режим предполагает обмен данными между ведущим и несколькими ведомыми устройствами с использованием пакетной передачи данных. Одно устройство (как ведущее, так и ведомое) может поддерживать до 3-х синхронных соединений.

Специально для реализации БСС имеется версия спецификации ядра беспроводной технологии Bluetooth v.4.0, получившая название Bluetooth с низким энергопотреблением (Bluetooth low energy или Bluetooth LE или BLE). Устройства, использующие BLE, могут работать более года на одной миниатюрной батарейке типа таблетка без подзарядки. Таким образом, можно иметь, например, небольшие датчики, работающие непрерывно (например, датчик температуры), общающиеся с другими устройствами, такими как сотовый телефон или КПК. Эта версия спецификации Bluetooth даёт возможность поддержки широкого диапазона приложений и уменьшает размер конечного устройства для удобного использования в области здравоохранения, физкультуры и спорта, охранных систем и домашних развлечений.

Для реализации БСС может быть использован также набор стандартов связи IEEE 802.11 (более известен под торговой маркой *WiFi*). Беспроводные сети WiFi изначально были задуманы как способ замены проводных вычислительных сетей. Однако, относительно высокие скорости передачи (до 108 Мбит/с) делают перспективным возможное применение в тех самоорганизующихся сенсорных сетях, в которых необходимо передавать большие объемы информации в реальном времени (например, видеосигнала). Для организации иерархических беспроводных ad-hoc сетей с мобильными и статическими узлами (mesh-сети) разрабатывается протокол IEEE 802.11s. В нем предложен новый протокол MAC уровня для беспроводных mesh-сетей и определяет, помимо всего прочего, протоколы выбора пути и пересылки сообщений. В отличие от традиционных сетей WiFi, в которых существует только два типа устройств – «точка доступа» и «терминал», стандарт 802.11s предполагает наличие так называемых «узлов сети» и «порталов сети». Узлы могут взаимодействовать друг с другом и поддерживать различные службы. Узлы могут быть совмещены с точками доступа, порталы же служат для соединения с внешними сетями. На основе уже существующих стандартов IEEE 802.11 можно строить MANET-сети (мобильные самоорганизующиеся сети), отличительной чертой которых можно назвать большую зону покрытия (несколько квадратных километров). Сравнение характеристик БСС приведено в табл. 3.3.

Таблица 3.3 – Характеристики радиотехнологий БСС

Технология (стандарт)	ZigBee (IEEE 802.15.4)	WiFi (IEEE 802.11b)	Bluetooth (IEEE 802.15.1)
Частотный диапазон	2.4-2,483 ГГц	2.4-2,483 ГГц	2.4-2,483 ГГц
Пропускная способность, кбит/с	250	11000	7131,1
Размер стека протоколов, кбайт	32-64	более 1000	более 250
Время непрерывной автономной	100-1000	0,5-5	1-10

работы от батареи, дни			
Максимальное число узлов в сети	65536	10	7
Диапазон действия, м	10-100	20-300	10-100
Области применения	Удаленный мониторинг и управление	Передача мультиме-дийной информации	Замещение проводного соединения

БСС могут быть реализованы также на базе беспроводной технологии связи на малых расстояниях при низких затратах энергии UWB (Ultra-Wide Band, сверхширокая полоса), использующей в качестве несущей сверхширокополосные сигналы с крайне низкой спектральной плотностью мощности. Для безлицензионного использования сверхширокополосных сигналов в Российской Федерации решением ГКРЧ от 15 декабря 2009 г. № 09-05-02 выделен диапазон 2,85...10 ГГц. При этом спектральная плотность мощности СШП приемопередатчика при работе в помещении не должна превышать −47...−45 дБм/МГц . Использование сверхширокой полосы частот (не менее 500 МГц) позволяет UWB достичь скорости передачи до 480 Мбит/с на расстоянии до 3 м. На дистанциях до 10 м технология позволяет достичь лишь 110 Мбит/с. Более подробно эти и другие протоколы, используемые в БСС, рассмотрены в главе 5.

3.6 Типы узлов БСС

Типовая архитектура БСС включает три типа узлов (рис. 3.6):

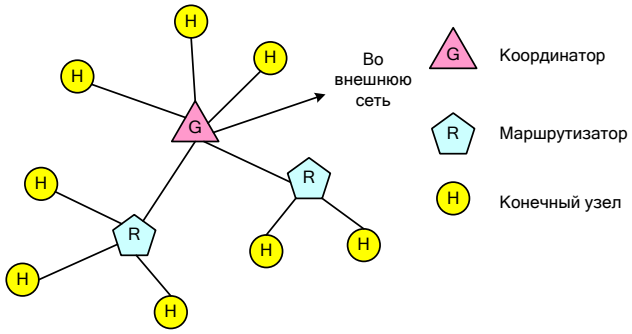


Рис. 3.6 – Типы узлов БСС

1. *Координатор* – осуществляет глобальную координацию, организацию и установку параметров сети, является наиболее сложным устройством БСС, требует наибольший объём памяти и наибольшую мощность источника питания. В одной сети должен присутствовать только один координатор. Из координатора осуществляется выход во внешнюю сеть (он реализует функцию шлюза - gateway). Часто координатор называют базовой станцией (БС).

Координатор выполняет следующие функции:

– определяет незадействованные каналы из перечня каналов, доступных для организации сети и определяемых разработчиком и организует сеть;

– передает сетевые сигнальные пакеты с информацией о существующей сети;

– управляет сетевыми подчиненными устройствами, устанавливает параметры сети - определяет максимальную глубину вложенных подсетей, число сетевых маршрутизаторов и число подчиненных устройств;

– обеспечивает маршрутизацию информации между подчиненными устройствами;

– большую часть времени находится в режиме приема;

– обеспечивает организацию таблиц маршрутизации;

– позволяет маршрутизаторам и конечным устройствам входить в сеть.

2. *Маршрутизатор* – принимает, буферизирует и передает данные от других узлов БСС, а также определяет направление передачи.

Маршрутизатор выполняет следующие функции:

– определяет активные каналы, подключается к сети и позволяет оконечным устройствам входить в сеть – использует дополнительные, определенные приложением, списки активных каналов;

– ретранслирует сигнальные сетевые пакеты с параметрами сети от координатора;

– администрирует сетевые адреса подключенных к маршрутизатору подчиненных устройств;

– поддерживает следующие классы устройств маршрутизации: устройство с таблицей маршрутизации и с функцией древовидной маршрутизации, устройство только с функцией древовидной маршрутизации, поддержка функции аварийной древовидной маршрутизации;

– поддерживает два режима работы устройств: без перехода в «спящий режим» и с переходом в «спящий» режим в периоды, определяемые координатором сети и параметрами сетевой синхронизации;

– поддерживает функции маршрутизации многоячейковых сетей: создает таблицы соседних сетевых узлов с параметром качества связи с каждым из них, создает таблицы сетевой маршрутизации, ретранслирует пакеты запроса и подтверждения определения маршрутов между устройствами;

– поддерживает функции маршрутизации по древовидному принципу – транслирует сообщения вверх и вниз по иерархической древовидной структуре ветви в зависимости от адреса получателя сообщения.

3. *Конечное (оконечное) устройство (сенсорный узел)* – выполняет только прикладные действия (сбор информации и управление удаленным объектом) и не осуществляет ретрансляцию данных.

Сенсорный узел имеет следующие особенности:

– всегда ищет и пытается войти в существующую сеть – использует дополнительные, определенные приложением, списки активных каналов и сигнальные пакеты синхронизации существующей сети для определения параметров сети и маршрутизатора для входа в сеть;

– питается от автономного источника (батареи);

– из пакетов синхронизации определяет наличие данных от координатора;

– запрашивает данные от координатора;

– способен находиться длительное время в «спящем» режиме (до 99,99% от всего времени работы).

По выполняемым наборам функций все узлы БСС можно отнести к двум видам:

1. *Устройство с полным набором функций FFD (Fully Function Device)*:

– поддержка стандарта IEEE 802.15.4;

– дополнительная память и энергопотребление позволяют выполнять роль координатора сети;

– поддержка всех типов топологий («точка-точка», «звезда», «дерево», «ячеистая сеть»);

– способность выполнять роль координатора сети;
– способность обращаться к другим устройствам в сети.

2. *Устройство с ограниченным набором функций RFD (Reduced Function Device)*:
– поддерживает ограниченный набор функций стандарта IEEE 802.15.4;
– поддержка топологий «точка-точка», «звезда»;
– не выполняет функции координатора;
– обращается к координатору сети и маршрутизатору.

Координаторы и маршрутизаторы всегда относятся к устройствами FFD, оконечные устройства могут быть FFD или RFD.

3.7 Типовые архитектуры и топологии БСС

Выделяют два типа архитектуры беспроводных сенсорных сетей: однородные (одноранговые) и иерархические (кластерные). Однородность сети подразумевает, что все узлы выполняют одинаковые функции при сборе, обработке и передаче информации. Этот подход позволяет добиться оптимальной маршрутизации. Пересылка данных происходит по самым эффективным по некоторым критериям маршрутам, что позволяет добиться экономии таких важных ресурсов, как энергия (передача идёт по маршруту с самым высоким запасом энергии) и время (передача происходит по самому короткому маршруту). Для критически важных данных может быть организована передача по наиболее надёжному пути. Агрегирование данных, если необходимо, происходит по мере следования сообщений к координатору. Однако при такой организации сети формирование связей между узлами происходит спонтанно, что ведёт к столкновениям пакетов и возникновению задержек, связанным с выходом из спящего режима узлов, находящихся на выбранном пути передачи.

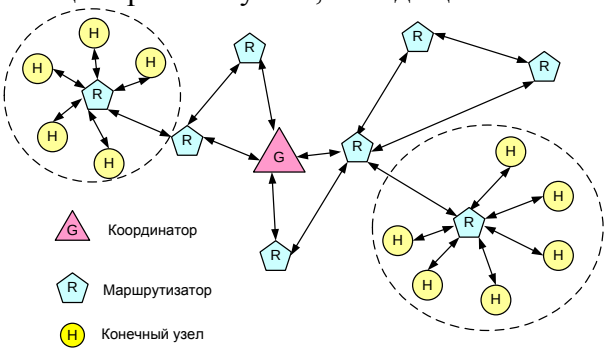


Рис. 3.7 – Кластерная структура БСС

Альтернативным подходом является иерархическая (древовидная) маршрутизация. Она основана на делении сети на области, называемые кластерами. Кластер образуют маршрутизатор и конечные узлы, у которых он запрашивает сенсорные данные (рис. 3.7). Внутри каждого кластера маршрутизатор отвечает за сбор информации со всего кластера, её обработку и дальнейшую передачу. Остальные узлы кластера осуществляют только сбор данных и передачу их маршрутизатору. Таким образом, узлы в иерархической сети не равноправны. Во-первых, агрегирование данных происходит на маршрутизаторах, и, во-вторых, пересылка агрегированных данных далее может производиться только маршрутизаторами. Таким образом, минимизируются задержки передачи, поскольку маршрутизаторы доступны всегда. Столкновения пакетов исключены благодаря централизованному методу создания ссылок. Однако такая маршрутизация не предоставляет оптимальных путей передачи данных. К тому же сенсорный узел, выполняющий функции маршрутизатора, тратит значительно больше энергии, что приводит к быстрому истощению его батарей. Существуют архитектуры, предполагающие использование в качестве маршрутизаторов физически выделенных сенсоров, обладающих большими запасами

энергии и вычислительными мощностями, однако этот подход применим только для узкого ряда приложений. Маршрутизаторы кластеров ретранслируют данные друг другу и, в конечном счете, данные передаются координатору. Координатор обычно имеет связь с IP-сетью, куда и направляются данные для окончательной обработки. В каждой сети должно быть, по меньшей мере, одно полнофункциональное устройство FFD для работы в качестве координатора.

Возможно также построение одноранговых ячеистых сетей (рис. 3.8). В таких сетях функциональные возможности каждого сенсорного узла одинаковы. Возможность самоорганизации и самовосстановления сетей ячеистой топологии позволяет в случае выхода части сенсоров из строя спонтанно формировать новую структуру сети. Правда, в любом случае необходим центральный функциональный узел-координатор, принимающий и обрабатывающий все данные, или шлюз для передачи данных на обработку внешнему узлу. Спонтанно создаваемые сети часто называют латинским термином Ad Hoc, что означает «для конкретного случая».

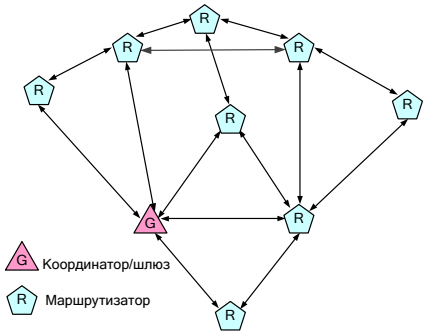


Рис. 3.8 – Ячеистая структура БСС

Возможные топологии сенсорной сети приведены на рис. 3.9. Одноранговые сети могут формировать произвольные топологические структуры (точка-точка, звезда), ограниченные только дистанцией между каждой парой узлов. Ячеистая топология (Mesh Topology) – базовая полносвязная топология, в которой каждый маршрутизатор сети соединяется с несколькими другими маршрутизаторами этой же сети. Характеризуется высокой отказоустойчивостью, но и более сложной настройкой.

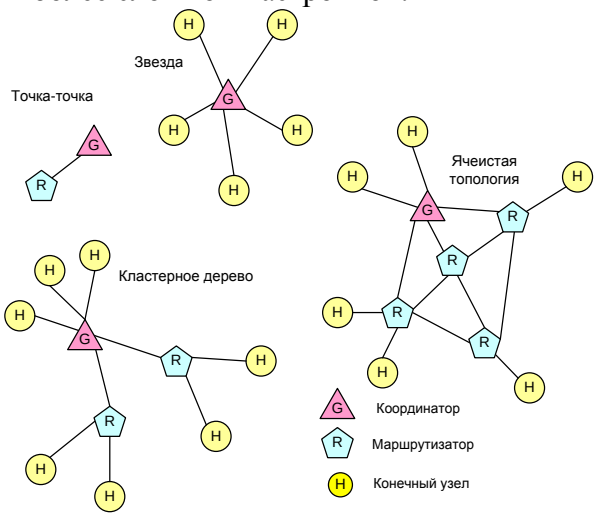


Рис. 3.9 – Возможные топологии сенсорной сети

Примером одноранговой или пиринговой сети (от англ. peer-to-peer, P2P – равный к равному) является кластерное дерево. Сеть типа кластерное дерево является частным случаем сети P2P, в которой большинство устройств являются FFD. Устройства RFD подключаются к кластеру в качестве конечных узлов. Для присоединения к сети удалённых

от координатора новых сетевых устройств могут использоваться уже присоединённые к сети FFD в режиме координатора. В этом режиме они, как и изначально координатор PAN, «зазывают» маяками в сеть новые сетевые устройства. В результате формируется кластер из сетевых устройств, которые «слышат» своего координатора. Тем не менее, вся информация о кластере доступна координатору PAN. Подобным образом могут формироваться мультикластеры из сетевых устройств.

3.8 Режимы работы БСС

Самой энергозатратной операцией для сенсорных узлов является передача данных в беспроводное окружение. Потому энергосберегающие формы передачи являются ключевым фактором для продления срока службы сенсоров, так как он практически целиком зависит от срока службы батарей.

Сбор данных беспроводной сенсорной сетью может производиться различными способами в зависимости от целевого назначения конкретной сети. Принимая во внимание различные способы использования сетевых ресурсов, беспроводные сенсорные сети можно разделить на классы в зависимости от вида их функционирования и типа целевого приложения:

1. *Проактивные сети*. Узлы такой сети периодически включают свои сенсоры и передатчики, снимают показания и передают их на базовую станцию. Таким образом, они делают "моментальную фотографию" своего окружения с некоторой периодичностью и используются обычно для приложений, требующих регулярного мониторинга некоторых значений.

2. *Реактивные сети*. Узлы реактивных сетей с некоторой периодичностью снимают показания, однако не передают их, если полученные данные попадают в определенную область нормальных показаний. В то же время сведения о неожиданных и резких изменениях в показаниях датчиков или их выходе за диапазон нормальных значений незамедлительно передаются на базовую станцию. Этот вид сети предназначен для работы с приложениями реального времени.

3. *Гибридные сети*. Это комбинация двух вышеперечисленных типов, где сенсорные узлы не только периодически отправляют снятые данные, но и реагируют на резкие изменения в значениях.

3.9 Протоколы маршрутизации в БСС

Для определения маршрута передачи информации в БСС от конечного узла до узла-координатора, а также между оконечными узлами, используются специальные протоколы маршрутизации. Протоколы маршрутизации в БСС решают следующие задачи:

1. Самоорганизация узлов сети (самоконфигурирование, самовосстановление и самооптимизация).
2. Маршрутизация пакетов данных и адресация узлов.
3. Минимизация энергопотребления узлов сети и увеличение общего времени жизни всей сети.
4. Сбор и агрегация данных.
5. Регулирование скорости передачи и обработки данных в сети.
6. Максимизация зоны покрытия сети.
7. Обеспечение заданного качества обслуживания (QoS).
8. Защита от несанкционированного доступа.

При выборе пути передачи информации в сети в качестве метрик в них могут быть использованы следующие параметры:

– длина пути (количество участков переприема информации);
– надежность;

– задержка;
– пропускная способность;
– загрузка;
– стоимость передачи трафика и др.

Протоколы маршрутизации БСС отвечают за поддержку маршрутов в сети и должны гарантировать надежную связь даже в жестких неблагоприятных условиях. Многие протоколы маршрутизации, управления электропитанием, распространения данных, были специально разработаны для БСС, где энергосбережение является существенной проблемой, на решение которой направлен протокол. Другие же были разработаны для общего применения в беспроводных сетях, но нашли свое применение и в БСС.

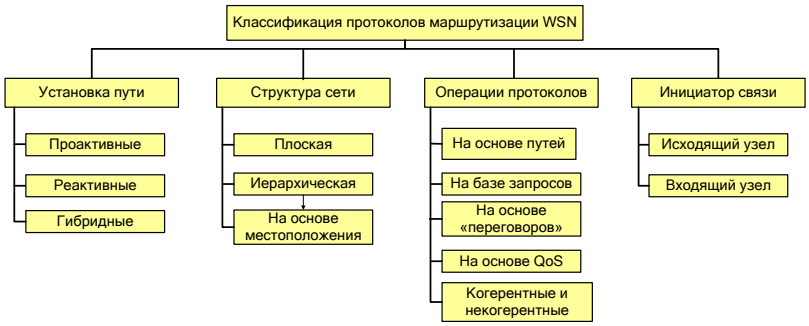


Рис. 3.10 – Классификация протоколов маршрутизации БСС

Существует большое количество протоколов маршрутизации для БСС, классифицировать их можно по разным признакам (рис. 3.10). В зависимости от используемого режима работы сети, обуславливающего необходимость передачи информации от узлов, все протоколы маршрутизации можно разделить на проактивные (все пути определяются заранее, до того как они будут нужны), реактивные (пути определяются по требованию) и гибридные (комбинация первых двух).

Протоколы, учитывающие структуры сети, делятся на:

1) протоколы *одноуровневой (плоской) (flat-based)* маршрутизации - все узлы БСС имеют одинаковую функциональность, примеры: SPIN (Sensor Protocols for Information via Negotiation), Direct Diffusion, Rumor Routing;

2) протоколы *иерархической (hierarchical-based)* маршрутизации – узлы сети выполняют разные функции, они могут быть и физически разными, примеры: LEACH (Low-Energy Adaptive Clustering Hierarchy), PEGASIS (Power-Efficient GAthering in Sensor Information Systems), TEEN и APTEEN (Threshold-sensitive Energy Efficient Protocols), SOP (Self-Organization Protocol);

3) протоколы маршрутизации на основе *информация о местонахождении узла (location-based)*, примеры протоколов: GAF (Geographic Adaptive Fidelity), GEAR (Geographic and Energy Aware Routing).

Работа протокола маршрутизации может основываться на различных принципах:

1) протоколы маршрутизации со *многими маршрутами (multipath routing)* – используются несколько маршрутов от источника до точки назначения, что повышает надежность соединения, но увеличивает накладные расходы и энергозатраты;

2) протоколы маршрутизации *«по запросу» (query-based)* – узел посылает запрос на данные в сеть и другой узел, который имеет запрашиваемые данные, отвечает на запрос;

3) протоколы маршрутизации, основанные на *«переговорах» (negotiation routing)* между узлами;

4) протоколы, учитывающие *качество обслуживания (QoS-based)*, что позволяет обеспечить определенный уровень услуг в сети.

В протоколах, направленных на агрегацию данных, промежуточные узлы, располагающиеся между источниками информации и базовой станцией (БС), могут осуществлять агрегацию данных и посылать БС уже сведенные данные. Этот процесс позволяет сенсорным узлам экономить энергию.

Все протоколы маршрутизации также можно разделить на два вида – в одних инициатором соединения является источник информации, а в других – получатель. Классификация протоколов маршрутизации БСС на основе типов узлов показана на рис. 3.11.

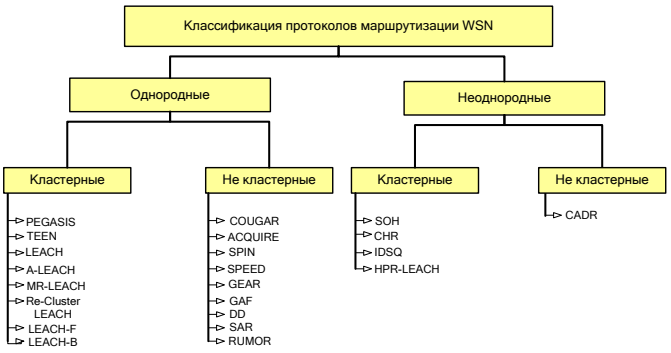


Рис. 3.11 – Классификация протоколов маршрутизации БСС на основе типов узлов

3.10 Мобильные БСС

В последние годы активно внедряются беспроводные децентрализованные самоорганизующиеся сети, состоящие из мобильных устройств MANET (Mobile Ad hoc NETwork). Каждое устройство такой сети может независимо передвигаться в любых направлениях, и, как следствие, часто разрывать и устанавливать соединения с соседями.

Самоорганизующиеся сети MANET обладают следующими преимуществами над беспроводными сетями традиционной архитектуры:

– возможность передачи данных на большие расстояния без увеличения мощности передатчика;

– устойчивость к изменениям в инфраструктуре сети;

– возможность быстрой реконфигурации в условиях неблагоприятной помеховой обстановки;

– простота и высокая скорость развертывания сети.

Однако мобильность узлов ведет к дополнительному повышению динамичности топологии сети и, следовательно, к возможности обрыва связи из-за помех или включения/выключения узла добавляется вероятность его перемещения.

Для маршрутизации на сетевом уровне в MANET используются специальные протоколы, ориентированные на динамические сети (например, поддерживать маршрут, если уехал промежуточный узел, и маршрут разрушился):

1) *реактивные* - находят маршрут в том случае, когда нужно передать пакет и для него нет известного пути и пытаются изменить этот путь, если произошла ошибка, примеры: специализированный протокол вектора расстояния по запросу AODV (Ad hoc On-Demand Distance Vector), протокол динамической маршрутизации источника DSR (Dynamic Source Routing) и др.;

2) проактивные *(превентивные)* - находят маршрут заранее для всех возможных пар источник-приемник и периодически обновляют информацию о маршрутизации для поддержки путей, примеры: протокол оптимизированной маршрутизации состояния соединения OLSR (Optimized Link-State Routing) и др.

Предпочтение одному или другому виду протоколов может быть отдано только с учетом обстановки и скоростей движения абонентов. К примеру, для автомобильной версии MANET имеет смысл использовать реактивные протоколы.

Сети MANET включают Ad hoc сети для транспортных средств VANET (Vehicular Ad hoc Network), в которых каждый участвующий автомобиль превращается в беспроводной маршрутизатор или узел, позволяющий автомобилям подключаться друг к другу на расстоянии и создавать мобильную сеть. Стандарт для сетей VANET разрабатывается в рамках рабочей группы IEEE 802.11p. Технические средства стандарта IEEE 802.11p должны функционировать на скорости до 200 км/час и на расстояния до 1 км. Физический уровень и MAC подуровень базируются на стандарте IEEE 802.11a. Частотный диапазон для США включает спектр от 5,859 до 5,925 ГГц, для Европы рекомендуется использование двух поддиапазонов шириной по 10 МГц каждый: 5,865 — 5,875 ГГц и 5,885 — 5,895 ГГц.

Возможности по взаимодействию транспортных средств между собой и с сетью связи общего пользование в ближайшие годы могут привести к образованию нового, очень масштабного сегмента Интернета вещей. Уже сейчас современный автомобиль интегрирует в себя GPS/GLONASS приемник, различные сенсоры, бортовой компьютер. Однако задача, которая ставится при создании VANET, несколько иная. Архитектура сети VANET предполагает взаимодействие автомобиля, как с другими автомобилями, так и с придорожной сетью. При этом выделяется три группы услуг:

1. Обеспечение безопасности - помощь водителю (навигация, предотвращение столкновений и смена полос), информирование (об ограничении скорости или о зоне ремонтных работ), предупреждение (послеаварийные, о препятствиях или состоянии дороги).
2. Повышение эффективности управления автомобильным трафиком - сокращение длительности поездки, потребления топлива.
3. Повышение уровня комфорта пассажиров и водителей - информация о местоположении автомобиля, о текущем трафике на дорогах, о погоде, возможность осуществления P2P соединений, в том числе с собственным домом через придорожную сеть, а также информация от придорожной сети об отелях, станциях заправки, меню в ресторанах и так далее.

3.11 Сопряжение БСС с сетями общего пользования

В настоящее время для сопряжения БСС с сетями связи общего пользования (ССОП) обычно используется протокол беспроводных персональных сетей на базе сетевого протокола IPv6 с низким энергопотреблением 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks), предложенный IETF, который позволяет интегрировать сенсорные сети в существующее семейство сетей стека протоколов TCP/IP. Данный протокол позволяет передавать IP-пакеты поверх стандарта IEEE 802.15.4 способом, удовлетворяющим открытым стандартам (протокол IPv6). При этом обеспечивается взаимодействие с другими IP-каналами и устройствами. Протокол 6LoWPAN создан для маломощных беспроводных персональных сетей (LoWPANs) и описан в документах RFC4919 и RFC4944. В архитектуре сети 6LoWPAN (рис. 3.12) определены три типа логических устройств (оконечный узел, маршрутизатор и шлюз), а также три вида сетей: «Простая LoWPAN», «Расширенная LoWPAN» и «Ad hoc LoWPAN». Как видно из рисунка, «Ad hoc LoWPAN» не подключена к ССОП, «Простая LoWPAN» подключена к ССОП через один шлюз, а «Расширенная LoWPAN» включает в себя несколько шлюзов, связанных с ССОП и друг с другом посредством магистральной линии связи.

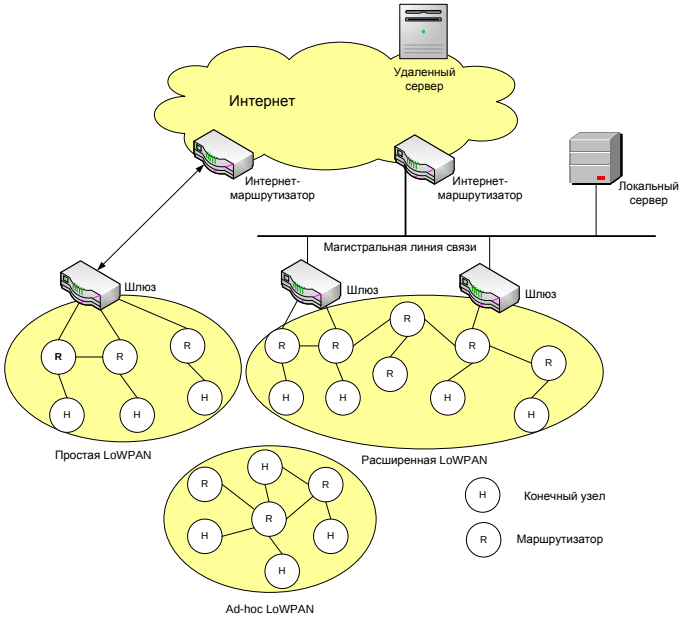


Рис. 3.12 - Архитектура сети 6LoWPAN

3.12 Проблемы реализации БСС

При практической реализации беспроводных сенсорных сетей существует ряд проблем:

1. Проблема энергопотребления.

Ограничение по энергопотреблению связанно с тем, что сенсоры работают от источника питания с ограниченным лимитом энергии (обычно батарейка). Чем реже они будут заменяться или заряжаться, тем более низкую стоимость будет иметь их обслуживание. Также энергопотребление является важным ограничением при использовании сенсоров, доступ к которым осложнен, следовательно, источник питания не может быть заменен или подзаряжен. Для уменьшения энергопотребления обычно предусматривается отключение передатчиков сенсорных узлов, когда нет необходимости передачи информации. На сетевом уровне используются оптимальные пути передачи информации от сенсорного узла до координатора (базовой станции), учитывая число промежуточных узлов, требуемую энергию и доступную энергию. Кроме сетевого протокола на потребление энергии влияет конструкция узлов (например, маленький размер памяти, эффективность переключений между заданиями), программное обеспечение, механизмы защиты и даже рабочие приложения.

2. Проблема самоуправления.

Сенсорные сети часто должны работать в удаленных областях и в жестких условиях, без возможности их обслуживания и ремонта. Поэтому, сенсорные узлы должны конфигурироваться самостоятельно, взаимодействовать с другими узлами, адаптироваться к поломкам изменениям окружающей среды без вмешательства человека.

3. Проблема беспроводного соединения.

Выбор беспроводного соединения налагает ряд ограничений на реализацию сенсорных сетей. Например, затухание сигнала ограничивает расстояние передачи информации. Так связь между мощностями сигналов переданной и принятой информацией описывается законом обратного квадрата расстояния:

Pпр ~ Pпрд / D^2,

где Pпр - мощность принятого сигнала;

Pпрд - мощность переданного сигнала;

D – расстояние между передатчиком и приемником.

Следовательно, увеличение расстояния между сенсорным узлом и маршрутизатором/координатором приводит к увеличению мощности передаваемого сигнала. Поэтому более эффективно, с точки зрения затрат энергии, разделить большие расстояния передачи информации в сенсорных сетях на несколько небольших.

4. Проблема децентрализованного управления.

Алгоритмы построения многих сенсорных сетей строятся по централизованному принципу. При децентрализованном управлении сенсорные узлы должны обмениваться информацией с соседними узлами, чтобы сгенерировать решении о коммутации узлов, без глобальной информации обо всей сети. Вследствие этого децентрализованные алгоритмы могут быть неоптимальными, но более эффективными в отношении энергии, чем централизованные. Например, при централизованном управлении базовая станция может опрашивать все сенсорные узлы, принимать от них информацию, сообщать каждому узлу свой маршрут передачи информации. При частом изменении сети потери будут значительны. Децентрализованный подход позволяет каждому узлу делать собственное решение при наличии небольшой информации (список соседних устройств, включающий информацию о расстоянии до базовой станции). В данном случае потери на управление будут значительно уменьшены.

5. Проблема конструкции.

Главной целью беспроводных сенсорных сетей является создание маленьких, дешевых и эффективных устройств. Из-за требования к низкому потреблению энергии типичный сенсорный узел имеет небольшие скорости выполнения операций и объемы хранимой информации. Также из-за этого нежелательно использование некоторых устройств, таких как GPS-приемники. Ограничения по размерам влияет на структуру протоколов и алгоритмов, реализованных в беспроводных сенсорных сетях. Например, таблица всех маршрутов в сети может быть слушком большой и не поместиться в памяти узла. Поэтому только небольшая часть информации (например, список соседних узлов) может храниться в памяти узла.

6. Проблема безопасности.

Удаленное расположение сенсоров и их автоматическая работа увеличивает их незащищенность к сторонним вторжениям и атакам. При беспроводном соединении достаточно легко для нарушителя перехватить пакеты, передаваемые сенсорным узлом. Например, наиболее большая угроза осуществления атаки «отказа в обслуживании» (denial-of-service), цель данной атаки нарушить корректное функционирование сенсорной сети. Это может быть достигнуто при помощи различных способов, например, при подаче мощного сигнала, который мешает сенсорным узлам обмениваться информацией («белый шум» или jamming attack). Есть различные варианты защиты систем от злоумышленников, но для многих из них необходимы высокие требования к аппаратным ресурсам, что труднодостижимо на жестко ограниченных по многим требованиям сенсорных узлах. Следовательно, сенсорные беспроводные сети требуют новых решений для создания ключей, их распространения, идентификации и защиты узлов.

3.13 Электропитание узлов БСС от внешней среды

Одним из основных требований, предъявляемых к узлам сенсорной сети, является длительное время их автономной работы. Задача уменьшения энергопотребления может решаться за счет оптимизации конструкции и режимов работы аналоговых и цифровых схем узлов, а также за счет извлечения энергии, необходимой для работы этих схем, из окружающей среды. В настоящее время во всем мире ведется активный поиск новых

экологичных и неограниченных ресурсов энергии, которые позволят сетевым устройствам избавиться от батарей или проводов и разработать автономные беспроводные сенсорные сети с теоретически неограниченным сроком службы.

В окружающей среде существуют четыре основных источника энергии: механическая энергия (вибрации, деформации), тепловая энергия (температурные перепады или изменения), энергия излучения (солнце, инфракрасные лучи, радиочастоты) и химическая энергия (химия, биохимия). Эти источники характеризуются различными плотностями мощности (рис. 3.13).

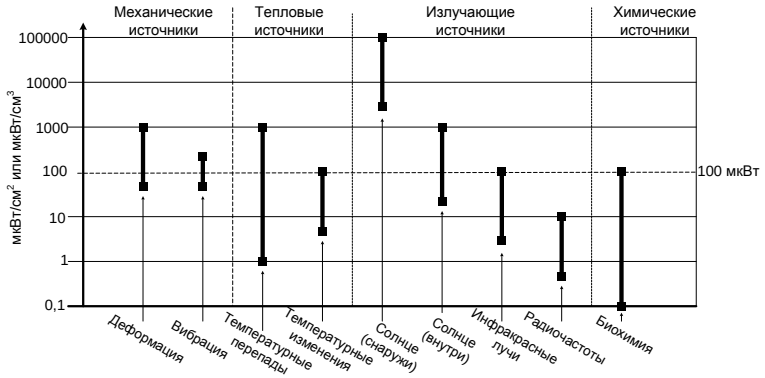


Рис. 3.13 - Плотность мощности (до преобразования) для различных типов источников энергии из внешней среды

Рисунок показывает, что значение выходной мощности 10-100 мкВт является приемлемым при размерах источника в 1 см^2 или 1 см^3. Получение энергии от солнца считается наиболее мощным (даже если значения, приведенные на рис. 3.14, должны быть умножены на весовые коэффициенты для перевода КПД, редко превышающих 20% в фотоэлементах). К сожалению, получение солнечной энергии невозможно в темных участках (например, в помещениях). Аналогично невозможно получать энергию от температурных перепадов, если этих перепадов нет или от несуществующих вибраций. Как следствие, источник внешней энергии должен быть выбран в соответствии с местной средой, окружающей узел беспроводной сенсорной сети, т.е. не существует универсального источника энергии из внешней среды.

Для питания узлов сенсорной сети от окружающей энергии необходимо снизить потребления энергии датчиками (сенсорами/актуаторами), микроконтроллером и радио-передатчиком. В последние годы значительный прогресс в этом направлении был достигнут производителями микроконтроллеров и радиочастотных чипов (Atmel, Microchip, Texas Instruments и др.) как для рабочего, так и для холостого режима. Пример типичного потребления энергии узлом беспроводных сенсорных сетей приведен на рис. 3.14.

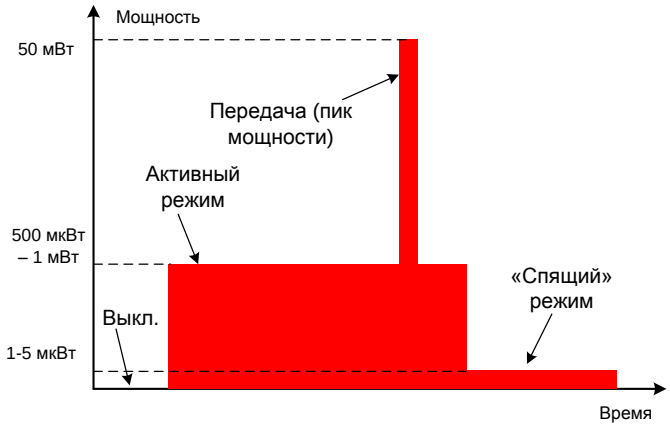


Рис. 3.14 - График потребления энергии узлом БСС

Можно выделить три типичных значения потребляемой мощности:

1) 1-5 мкВт: потребление энергии в «спящем» режиме;
2) 500 мкВт – 1 мВт: потребление энергии в активном режиме;
3) 50 мВт: пик передачи энергии.

Анализ приведенной диаграммы позволяет сделать следующие выводы. Во-первых, минимальная мощность источника энергии из внешней среды для построения жизнеспособных беспроводных узлов должна быть порядка 1-5 мкВт, что соответствует достаточной величине для холостого режима микропроцессора и радиочастотного чипа.

Во-вторых, современные источники энергии из внешней среды не могут обеспечивать беспроводные сенсорные сети энергией, достаточной для активного режима (потребление энергии в 500 мкВт - 1 мВт против 10-100 мкВт для выходной мощности таких источников). Однако, благодаря ультранизкому потреблению энергии в спящем режиме, беспроводные сенсорные сети, питаемые от внешней среды, могут использовать прерывистый рабочий цикл, изображенный на рис. 3.15. Энергия хранится в буфере (а) (конденсаторы, батареи) и используется для выполнения измерительного цикла, как только энергии в буфере становится достаточно (б и в). Далее система опять возвращается к спящему режиму (г), ожидая нового измерительного цикла.

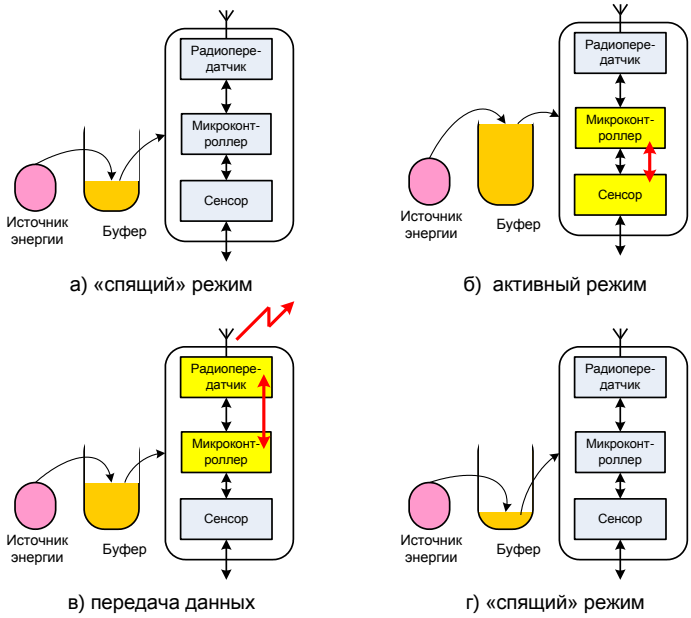


Рис. 3.15 – Рабочий цикл в беспроводной сенсорной сети

Таким образом, используя энергию из внешней среды возможно питание любых приложений, даже самых неэкономных. Основной проблемой является адаптация частоты измерительного цикла к непрерывно вырабатываемой энергии. Среднее энергопотребление сенсорных узлов (P) соответствует общему количеству энергии, необходимой для одного измерительного цикла (W), умноженному на частоту этого действия (f):

$$P = W \times f.$$

Эта простая связь между P, W и f проиллюстрирована на рис. 3.16. Используя логарифмические масштабы по оси абсцисс (энергия в Джоулях) и по оси ординат (частота измерений), среднее энергопотребление 100 мкВт показано прямой линией с коэффициентом наклона -1. Например, выполнение полного цикла работы сенсорного узла (измерение + преобразование + передача) требует 250-500 мкДж. Следовательно, непрерывно получая 100 мкВт мощности, можно выполнять полный цикл работы узла сенсорной сети каждые 1-10

секунд (0,1-1 Гц). Это подходит многим промышленным нуждам, особенно тем, где обслуживание предсказуемо.

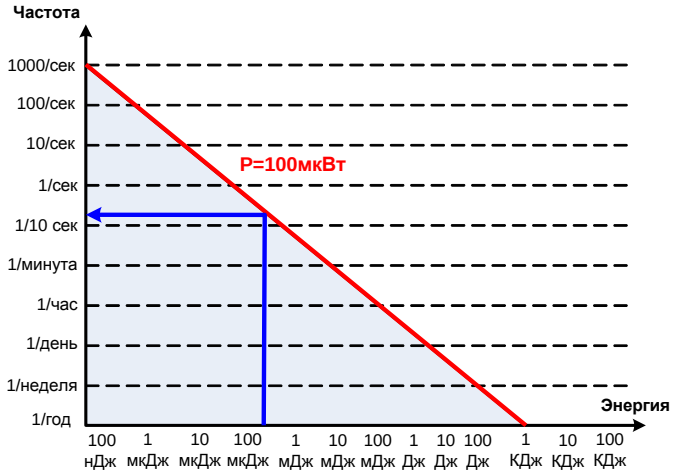


Рис. 3.16 – Связь мощности, энергии и частоты

В целом получение энергии из внешней среды – за исключением фотоэлемента – только развивающаяся отрасль, еще не приспособленная для промышленного применения. Тем не менее, улучшение существующих технологий может привести в перспективе к жизнеспособным решениям электропитания автономных беспроводных сенсорных сетей.

3.14 БСС и Интернет вещей

Благодаря таким характеристикам БСС, как миниатюрность узлов, низкое энергопотребление, встроенный радиоинтерфейс, достаточная вычислительная мощность, сравнительно невысокая стоимость, стало возможным их широкое использование во многих сферах человеческой деятельности с целью автоматизации процессов сбора информации, мониторинга и контроля характеристик разнообразных технических и природных объектов.

БСС целесообразно применять в следующих предметных областях Интернета вещей:

- мониторинг телекоммуникационной инфраструктуры сетей;
- мониторинг транспортных магистралей (железных дорог, метрополитена и др.), нефте- и газопроводов, инженерных сетей энерго- и теплоснабжения;
- контроль и анализ транспортных грузопотоков;
- экологический, биологический и медицинский мониторинг;
- автоматизация систем жизнеобеспечения в системах класса “Умный дом”;
- выявление и предупреждение чрезвычайных ситуаций (мониторинг сейсмической активности и вулканической деятельности, анализ атмосферы и прогноз погоды для своевременного предупреждения о наступлении стихийных бедствий) и другие.

Контрольные вопросы по главе 3

1. Что такое сенсорная сеть? Из каких элементов она состоит?
2. В чем особенность самоорганизующейся (ad hoc) сети связи?
3. Какие компоненты входят в состав базовой архитектуры сенсорной сети?
4. Из каких подсистем состоит аппаратная часть узла беспроводной сенсорной сети?
5. Какие ограничения существуют для узлов БСС?
6. Какие способы передачи данных используются в БСС?
7. Какие частотные диапазоны разрешены в России для построения БСС?

8. Какие протоколы и технологии передачи данных используются в БСС?
9. Укажите отличия основных типов узлов БСС.
10. Какие основные архитектуры применяются для построения БСС?
11. Какие типовые топологии используются в БСС? В чем их отличие?
12. В каких режимах может работать БСС?
13. Какие задачи решают протоколы маршрутизации в БСС?
14. Поясните принципы классификации протоколов маршрутизации в БСС.
15. Укажите особенности реализации беспроводных самоорганизующихся сетей мобильных устройств MANET.
16. Как сопрягаются БСС с сетями общего пользования?
17. Перечислите основные проблемы практической реализации БСС.
18. Сравните по плотности мощности (до преобразования) различные типы источников энергии из внешней среды.
19. Укажите режимы работы узла БСС и величины потребляемой при этом мощности.
20. Поясните, как можно использовать энергию из внешней среды для электропитания узлов БСС.
21. Приведите примеры использования БСС для реализации концепции Интернета вещей.

ГЛАВА 4 МЕЖМАШИННЫЕ КОММУНИКАЦИИ M2M

4.1 Общие принципы M2M

Межмашинное взаимодействие (машинно-машинное взаимодействие, англ. Machine-to-Machine, M2M) – общее название технологий, которые позволяют машинам обмениваться информацией друг с другом, или же передавать её в одностороннем порядке в автоматическом режиме между устройствами без участия человека. При всём своём практическом многообразии, идея машино-машинного взаимодействия может быть сведена к простой схеме из трёх элементов. Представьте себе цифровое устройство (машину) A, занятое сбором любой информации. Собранные сведения передаются через канал связи B (проводный или беспроводный) на устройство (машину) C, находящееся от устройства A на некотором удалении, производящее анализ полученных данных и хранение результатов, а при необходимости и генерацию управляющих команд для устройства A (рис. 4.1). Работает такая схема без участия человека (машина общается с машиной), откуда и название: M2M. Хотя правильнее было бы использовать более точное сокращение – M2(CN2)M (Machine-to-(Communication-Network-to-) Machine), что однозначно указывает на обязательное наличие в межмашинных коммуникациях некоторой телекоммуникационной сети.

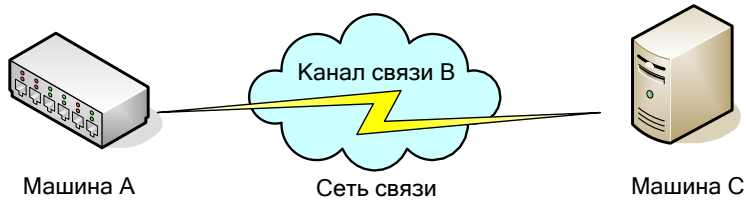


Рис. 4.1 – Идея связи «машина – машина» M2M

Многие рассматривают M2M как частный случай IoT, а некоторые наоборот – Интернет вещей как вариант реализации межмашинных коммуникаций. Авторы придерживаются первого подхода, так как Интернет Вещей – термин намного более широкий, подразумевающий не только взаимодействие с устройствами, людьми и вещами, но и обеспечение этого взаимодействия дополнительными контекстами, такими как географические, временные координаты и т.п.

Точную дату появления систем M2M назвать достаточно сложно. Одной из первых разработок M2M, интегрированных с беспроводными решениями, считается OmniTRACS – решение американской компании Qualcomm, созданное в 1989 году для отслеживания коммерческого транспорта.

Исключение человека из электронных коммуникаций машин, сведение его роли к пассивной роли наблюдателя – принципиально важный момент. Человек ненадёжен – он медлителен, склонен ошибаться, быстро утомляется, поэтому исключение человека из информационной системы позволяет построить намного более эффективные электронные комплексы. Однако вплоть до конца XX века именно человек оставался главным генератором и главным потребителем информации на Земле. И только за последнее время ситуация существенно изменилась – M2M-функциональность появилась в миллионах устройств.

Концепция M2M объединяет телекоммуникационные и информационные технологии для автоматизации различных технологических и бизнес процессов. M2M технологии применяются в самых различных сферах – в энергетике, логистике, грузоперевозках, финансах, торговле, безопасности, менеджменте, здравоохранении, образовании и др. В транспортной сфере технологии M2M используются, например, для диагностики двигателей, мониторинга транспорта, спутникового слежение за автотранспортом, ГЛОНАСС/GPS контроля водителей и грузов и др. Характерными примерами использования M2M в быту

являются измерение и передача показателей счетчиков расхода энергоресурсов (электроэнергии, воды, газа и т.п.), обеспечение безопасности дома (охранная и пожарная сигнализации, контроль протечек воды).

Для реализации межмашинных коммуникаций используются все возможные среды передачи данных: электрические линии, волоконно-оптические линии, радиолинии. Одним из широко используемых подклассов M2M является межмашинное взаимодействие с использованием мобильных решений, для него также может использоваться аббревиатура M2M (англ. Mobile-to-Mobile или Mobile-to-Machine). Использование беспроводных M2M-коммуникаций дает очевидные преимущества. Во-первых, возможность мониторинга и управления удаленными объектами, до которых невыгодно прокладывать проводную связь. Во-вторых, возможность оперативно и достаточно просто подключать новые устройства без дополнительных затрат. Ну и наконец, это управление объектами там, где использование проводов невозможно в принципе (например, для мониторинга и управления подвижными объектами).

4.2 Стандартизация M2M

Межмашинные коммуникации являются важнейшей составляющей Интернета вещей. В настоящее время можно выделить более 140 организаций, прямо или косвенно участвующих в процессах стандартизации M2M.

В 2007 г. технический комитет ETSI подготовил ряд документов, определяющих случаи применения M2M для электронного здравоохранения e-Health, интеллектуальных счетчиков, для потребителей, а также термины и определения, требования к услугам M2M и функциональную архитектуру сети M2M. По версии ETSI, machine-to-machine (или mobile-to-machine) – это симбиоз телеком- и информационных технологий для автоматизации бизнес-процессов и создания услуг с добавленной стоимостью VAS (Value Added Service), направленных на управление информационными и технологическими процессами в различных областях жизнедеятельности общества.

Функциональная архитектура M2M представлена в стандарте ETSI TS 102 690. Она разделена на два домена: домен устройств и шлюзов M2M и сетевой домен (рис. 4.2).

Домен устройств и шлюзов M2M включает в себя следующие элементы:

1. *Устройство M2M* – поддерживает M2M приложения и использует сервисные возможности M2M. Устройства M2M подключаются к сетевому домену следующими способами:

а) прямое соединение – устройство M2M подключается к сетевому домену через сеть доступа, при этом устройству M2M доступны такие процедуры, как регистрация, аутентификация, авторизация, управление и инициализация в пределах сетевого домена. M2M устройство может предоставлять сервисы другим устройствам, скрытым от сетевого домена;

б) шлюз в качестве сетевого прокси-сервера – устройство M2M подключается к сетевому домену через шлюз M2M. К шлюзу устройства M2M подключаются через доступную сеть устройств M2M. В этом случае шлюз играет роль прокси-сервера. Через прокси-сервер доступны такие процедуры, как аутентификация, авторизация, управление и инициализация.

В общем случае устройство M2M может подключаться к сетевому домену через различные шлюзы M2M.

2. *Сеть доступа M2M* – обеспечивает связь между устройствами M2M и шлюзами M2M. Примерами сетей M2M могут служить персональные сети (PAN), такие как IEEE 802.15.1, ZigBee, Bluetooth, IETF ROLL, ISA100.11a или локальные сети, такие как PLC, M-BUS, Wireless M-BUS и KNX.

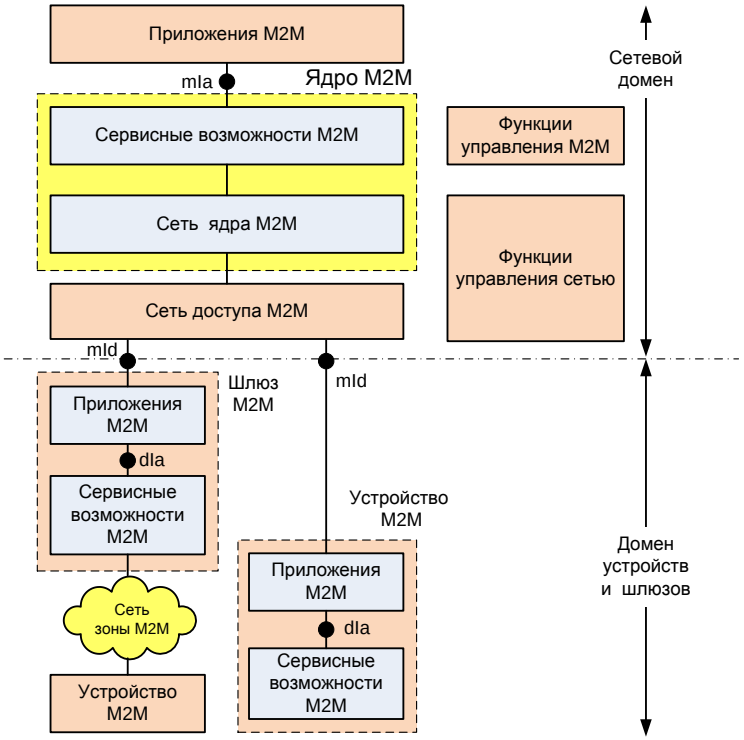


Рис. 4.2 - Высокоуровневая архитектура ETSI M2M (источник: ETSI)

3. *Шлюз M2M* – поддерживает приложения M2M и использует сервисные возможности M2M. Шлюз выступает в качестве прокси-сервера между устройством M2M и сетевым доменом. Шлюз M2M может предоставлять сервисы другим устройствам, скрытым от сетевого домена.

Сетевой домен состоит из следующих элементов:

1. *Сеть доступа M2M* – позволяет устройствам M2M и шлюзам M2M взаимодействовать с транспортной сетью. Сеть доступа M2M использует xDSL, HFC, спутниковые сети, GERAN, UTRAN, eUTRAN, W-LAN, WiMAX и другие технологии.

2. *Транспортная сеть M2M* обеспечивает:

– IP-соединения и возможно другие способы коммуникаций;
– функции управления услугами и сетью;
– взаимодействие с другими сетями;
– роуминг услуг;
– предоставление различных наборов услуг;

Транспортная сеть M2M может быть реализована, например, на базе таких стандартов, как 3GPP, ETSI TISPAN, 3GPP2 и др.

3. *Сервисные возможности M2M* обеспечивают:

–предоставление функций M2M, которые могут использоваться различными приложениями;
–расширение функций через набор открытых интерфейсов;
–использование функциональности ядра сети;
–упрощение и оптимизация разработки и внедрения приложений.

4. *Приложения M2M* – реализуют логику услуг и используют сервисные возможности M2M услуг через открытые интерфейсы.

5. *Функции управления сетью* – включают функции, требуемые для управления сетями доступа и транспортной сетью, включая инициализацию, администрирование, управление сбоями и др.

6. *Функции управления M2M* – состоят из функций, требуемых для управления сервисными возможностями M2M в сетевом домене. Управление устройствами M2M и шлюзами включает в себя специфические сервисные возможности M2M:

−набор функций управления M2M включает функцию загрузки услуг M2M (Service Bootstrap, MSBF), реализованной на соответствующем сервере. Роль MSBF заключается в упрощении начальной загрузки постоянных учетных данных по безопасности на M2M устройство (или M2M шлюз) и использовании сервисных возможностей M2M в сетевом домене;

−постоянные учетные данные безопасности, загруженные при помощи MSBF, хранятся в безопасном месте, которое называется сервером аутентификации M2M (M2M Authentication Server, MAS). В роли такого сервера может выступать AAA сервер. Функция MSBF может быть реализована на MAS сервере или на другом устройстве, взаимодействующем при этом с MAS при помощи соответствующего протокола (например, Diameter в случае использования AAA сервера).

Стандарт TS 102-690 определяет три интерфейсных точки в функциональной архитектуре M2M (рис 4.3):

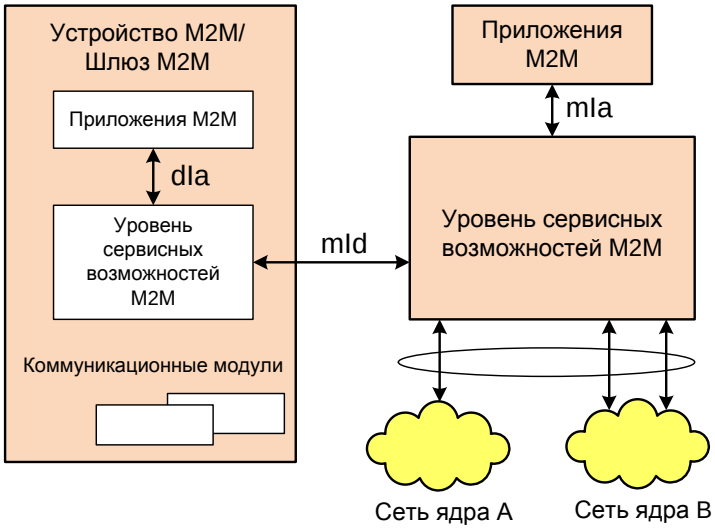


Рис. 4.3 – Интерфейсные точки функциональной архитектуры M2M (источник: ETSI)

1. Точка (интерфейс) mIa - между сетевым приложением NA (Network Application) и сервисными возможностями сетевого домена и приложений M2M. Она обеспечивает примитивы регистрации и авторизации для NA, управления сервисными сессиями (отчетность о событиях или потоковых сессиях) и примитивы чтения/записи /выполнения/подписки/уведомления для объектов или групп объектов, расположенных непосредственно в устройствах M2M или шлюзах, а также для групп объектов, управляемых сетевым доменом.

2. Точка (интерфейс) dIa между:

а) приложением устройства DA (Device Application) и сервисными возможностями M2M в том же устройстве M2M или в шлюзе M2M;

б) приложением шлюза GA (Gateway Application) и сервисными возможностями M2M в том же шлюзе M2M.

Интерфейс dIa выполняет функции регистрации и авторизации для приложений DA и GA в устройстве/шлюзе, управление сервисными сессиями (отчет о событии или потоковые сессии) и примитивы чтения/записи/выполнения/подписки/уведомления для объектов или групп объектов расположенных непосредственно в устройствах M2M или шлюзах, а также для групп объектов, управляемых с помощью устройства/шлюза.

3. Интерфейс mId между устройством M2M или шлюзом и сервисными возможностями M2M в сетевом домене и приложений. mId выполняет функции регистрации и авторизации для приложений DA и GA в ядре M2M, управление сервисными сессиями (отчет о событии или потоковые сессии) и примитивы чтения/записи/выполнения/ подписки/уведомления для объектов или групп объектов расположенных непосредственно в устройствах M2M или шлюзах, а также для групп объектов, управляемых с помощью устройств, шлюзов или возможностей ядра сети.

В 2012 году был создан Глобальный партнерский проект oneM2M, способствующий формированию общедоступных и общепризнанных технических спецификаций и технических отчетов, относящихся, прежде всего, к уровню услуг M2M (M2M Service Layer). В рамках проекта oneM2M созданы четыре рабочих группы по следующим направлениям разработки: технические требования; архитектура; безопасность; управление, общее описания объектов и их семантика. Результаты работы данных групп пока носят предварительный характер и разрабатываемые документы находятся на стадиях согласования. Инициатива oneM2M предусматривает в идеале формирование единого стандарта услуг M2M. Также предусматривается формирование единых подходов к взаимодействию с участниками рынка услуг передачи информации, вертикальными рынками и разработчиками программных архитектур.

4.3 Коммуникации малого радиуса действия NFC

Технология связи на малых расстояниях NFC (Near Field Communication) – совместная разработка компаний NXP Semiconductor и Sony – представляет собой комбинацию нескольких существующих бесконтактных технологий радиочастотной (РЧ) идентификации и связи. Эта технология – простое расширение стандарта бесконтактных карт, которая объединяет интерфейс смарткарты и считывателя в единое устройство. Устройство NFC может поддерживать связь и с существующими смарткартами и считывателями стандарта ISO 14443, и с другими устройствами NFC, и таким образом совместимо с существующей инфраструктурой бесконтактных карт, уже использующейся в общественном транспорте и платежных системах. NFC нацелена, прежде всего, на использование в мобильных телефонах. Технология NFC позволяет обмениваться различной информацией, например, номерами телефонов, картинками, музыкальными файлами или ключами цифровой авторизации между двумя расположенными близко друг к другу устройствами с поддержкой NFC. Это могут быть любые портативные устройства, а также смарт-карты или считывающие устройства RFID. Данная технология может использоваться в качестве ключа доступа к данным или сервисам, таким как безналичная оплата или электронный замок.

Модель предоставления услуг с использованием технологии NFC целесообразно рассматривать в контексте развития технологий сетей связи. Сегодня ориентиром развития может служить концепция сетей следующего поколения NGN/IMS/4G/5G. Она предполагает уровневую архитектуру с делением на слои (Stratum) – транспортный, услуг связи и приложений. Первые два слоя реализуются средствами сетей связи. Слой приложений представляет собой совокупность всех прикладных услуг, формируемых и предоставляемых пользователям раз личными поставщиками.

Приложения, формирующие контент для услуг на основе NFC, находятся в слое приложений и взаимодействуют с функцией поддержки специфики этих приложений (middleware) в слое услуг. Последняя добавляет к базовой функциональности услуги свою функциональность, необходимую для доставки услуги сетевому пользователю.

Услуги с использованием технологии NFC (как, впрочем, и многие другие в мобильной связи и в сети Интернет) предполагают наличие в аппарате пользователя некоторых специальных функций, относящихся только к этой группе услуг. Иными словами, приложения не могут быть реализованы обычными средствами сетей связи, а требуют присутствия в терминале пользователя специальной программы (мидлета), которая, с одной

стороны, осуществляет взаимодействие по интерфейсу NFC, а с другой – использует функцию поддержки приложений в сетевом оборудовании. За счет этого уровневая структура, представленная в рекомендациях МСЭ-Т и ETSI, расширяется (рис. 4.4).

Интерфейс NFC стандартизован на нижних уровнях. Интерфейсы UNI (User-Network Interface) и ANI (Application Network Interface) представляют эталонные точки, в которых может присутствовать тот или иной физический интерфейс в соответствии с конкретной реализацией. Чтобы сделать систему открытой, необходимо стандартизовать высокоуровневые решения на интерфейсе NFC и в эталонных точках UNI и ANI, т.е. стандартизация должна касаться процедур взаимодействия и форматов сообщений на уровне приложений.

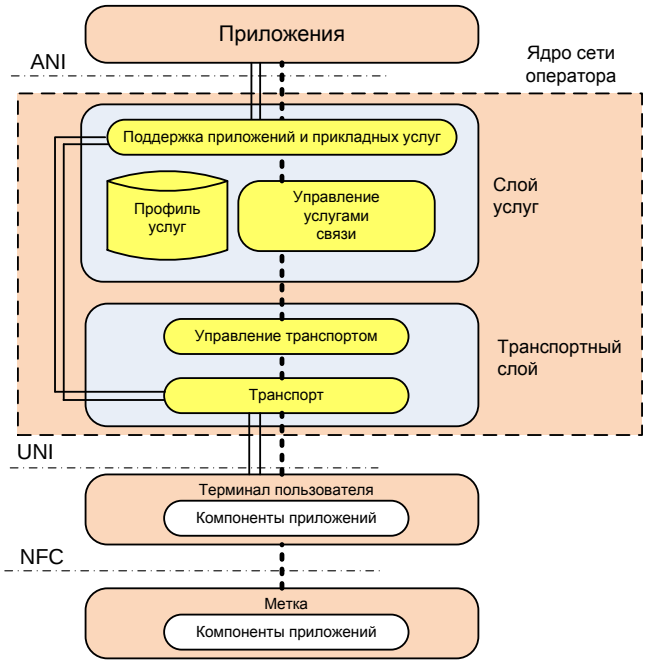


Рис. 4.4 - Место технологии NFC в архитектуре сети NGN

Частота работы системы NFC – 13,56 МГц, скорость передачи – 106 кбит/с (возможны 212 кбит/с и 424 кбит/с) на расстоянии примерно 10 см. В отличие от существующих технологий бесконтактной связи на данном диапазоне частот, которые позволяют передавать информацию только от активного устройства пассивному, NFC обеспечивает обмен между двумя активными (равноправными) устройствами. Таким образом, NFC можно использовать для доступа к устройствам радиочастотной идентификации RFID.

В основе технологии NFC лежит индуктивная связь (рис. 4.5). Сигнал подвергается амплитудной манипуляции OOK (On-Off Keying) с глубиной 100% или 10% и фазовой манипуляции BPSK. При передаче информации пассивному устройству используется амплитудная манипуляция ASK (Amplitude Shift Keying). При обмене с активным устройством оба устройства равноправны и выступают в качестве поллинговых. Каждое устройство имеет собственный источник питания, поэтому сигнал несущей отключается сразу после окончания передачи.

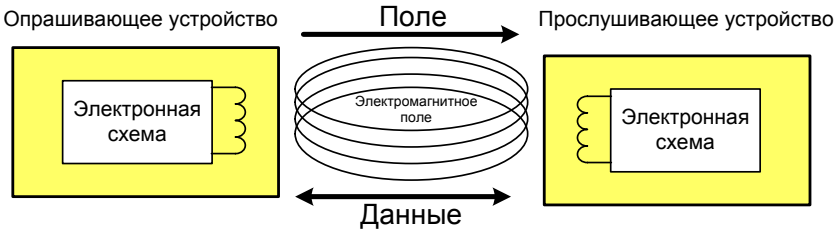


Рис. 4.5 - Принцип обмена данными по технологии NFC

За счет индуктивной связи между опрашивающим и прослушивающим устройствами пассивное устройство влияет на активное. Изменение импеданса прослушивающего устройства вызывает изменение амплитуды или фазы напряжения на антенне опрашивающего устройства, которое он обнаруживает. Этот механизм называется модуляцией нагрузки. Она выполняется в режиме прослушивания с применением вспомогательной несущей 848 кГц. В зависимости от стандарта применяется амплитудная (ASK для 14443 A) или фазовая манипуляция (BPSK для 14443 B). Еще один пассивный режим, совместимый с FeliCa, осуществляется без вспомогательной поднесущей с манипуляцией ASK на частоте 13,56 МГц.

В NFC определено три основных режима работы:

1. *Пассивный* (эмуляция смарт-карты). Пассивное устройство ведет себя как бесконтактная карта одного из существующих стандартов. Такой режим экономит батарейное питание и позволяет использовать NFC даже при выключенном питании. NFC можно использовать для всех тех применений, для которых используются бесконтактные карты, а совместимость с карточными стандартами, позволяет использовать уже существующую инфраструктуру.

2. *Передача между равноправными устройствами* (режим P2P – Person to Person). Производится обмен между двумя устройствами, при этом за счет собственного источника питания у прослушивающего устройства можно использовать NFC даже при выключенном питании опрашивающего устройства

3. *Активный режим* (чтение или запись).

В каждом режиме может применяться один из трех способов передачи: NFC-A, NFC-B, NFC-F. Для распознавания способа передачи инициирующее устройство посылает запрос. Характеристики режимов кодирования и модуляции приведены в табл. 4.1.

Таблица 4.1 Характеристики режимов NFC

Стандарт	**Тип устройства**	**Кодирование**	**Модуляция**	**Скорость передачи кбит/с**	**Несущая, МГц**
NFC-A	Опрашивающее	Модифицированный код Миллера	ASK 100%	106	13,56
	Прослушивающее	Манчестер	Модуляция нагрузки (ASK)	106	13,56 ± 848 кГц
NFC-B	Опрашивающее	NRZ-L	ASK 10%	106	13,56
	Прослуши-	NRZ-L	Модуляция нагрузки	106	13,56± 848 кГц

	вающее		(BPSK)		
NFC-F	Опраши-вающее	Манчестер	ASK 10%	212/424	13,56
	Прослу ши-вающее	Манчестер	Модуляция нагрузки (ASK)	212/424	13,56 (без поднес у-щей)

В пассивном режиме используются метки NFC – пассивные устройства, предназначенные для обмена с активными NFC-устройствами. Как и метки RFID, метки NFC применяются для хранения небольшого количества данных. Всего определено 4 типа меток NFC (табл. 4.2).

Таблица 4.2 Типы меток NFC

Тип метки	1	2	3	4
Стандарт	14443 A	14443 B	JIS 6319-4	14443 A/B
Совместимый продукт	Innovision Topaz	NXP Mifare	Sony FeliCa	NXP DESFire, SmartMX-JCOP, др.
Скорость передачи, кбит/с	106	106	212, 424	106, 212, 424
Объем памяти	96 байт, расширение до 2 кбайт	48 байт, расширение до 2 кбайт	До 1 Мбайта	До 32 кбайт
Защита от коллизий	Нет	Есть	Есть	Есть

Для использования сервиса NFC необходим встроенный в мобильный телефон специальный модуль или дополнительные устройства, такие как NFC-стикеры и модули. Стикеры можно прикрепить к корпусу телефона. Стикеры бывают пассивные и активные. Пассивные не могут осуществлять обмен данными с мобильным телефоном и, следовательно, не дают возможности записи информации в NFC-устройство по каналам связи мобильного оператора (через SMS или через мобильный Интернет). Активные используют канал связи Wi-Fi или Bluetooth для связи с телефоном: это либо повышенное энергопотребление, либо необходимость подзарядки модуля отдельно. Общий недостаток внешних модулей - это наличие крепления.

В модуле NFC есть микропроцессор (рис. 4.6), который обеспечивает надежное хранение сервисных приложений, криптографическую защиту и поддерживает три основных канала связи:

– NFC для бесконтактных транзакций;

– информационный поток с TSM («Trusted Service Manager») через сеть мобильного оператора;

– обмен данными с пользователем через пользовательский интерфейс – мобильное приложение телефона.

Сервисные приложения - программные модули (платежные, транспортные, карт лояльности и другие) хранятся в элементе безопасности, защищенные ключами от несанкционированного доступа.

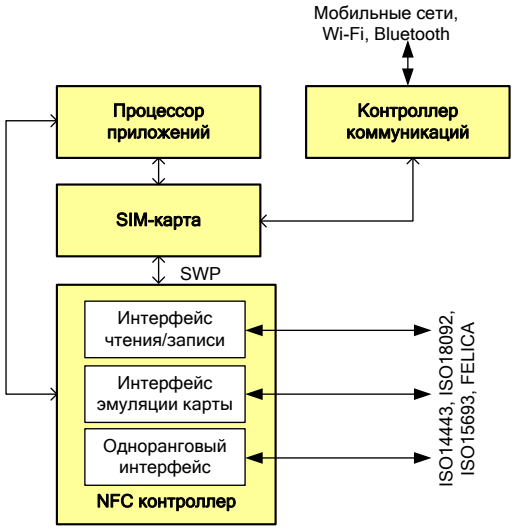


Рис. 4.6 – Структурная схема мобильного телефона с модулем NFC

Технология NFC предназначена в первую очередь для портативных устройств. Она является логическим продолжением и развитием технологии RFID. Несомненное преимущество NFC – простота использования. Для обмена информацией необходимо поднести устройства близко друг к другу. Существенное преимущество NFC над технологией Bluetooth - более короткое время установки соединения.

Особенно обширна область приложений, которые можно получить благодаря совмещению технологии NFC с возможностями мобильной связи. Это и различные схемы электронной коммерции (включая продажу и контроль билетов на транспорте, на зрелищных мероприятиях и т.п.), и разнообразные платные и бесплатные справочно-информационные услуги, реклама, дистанционные системы контроля, электронные деньги, удостоверения личности, мобильная торговля, электронные ключи и т.п. Мобильные телефоны могут использоваться для получения по сети сотовой подвижной связи (СПС) некоего контента, который затем передается через интерфейс NFC на стационарные терминалы, снабженные соответствующим интерфейсом, например текст – на принтер, видеоклипы – на телевизор и т.д. Некоторые стандартные сферы использования технологии приведены в табл. 4.3.

Таблица 4.3 Применение технологии NFC

Область применения	**Примеры**
Оплата с помощью мобильного телефона	• Покупка билетов или оплата такси • Работа с бесконтактными терминалами продаж (платежные системы) • Хранение чеков в памяти телефона
Телефон как электронный ключ	• Для прохода в здание (контроль доступа) • Для доступа к ПК • Для автомобиля • Для создания офиса дома
Передача данных	• Обмен электронными визитками • Печать фотографий напрямую с фотоаппарата
Электронная блокировка	• Доступ к глобальным сетям или Bluetooth
Доступ к данным	• Загрузка расписаний с электронного табло на телефон • Загрузка карт на телефон • Считывание навигационных координат
Хранение электронных билетов на мобильном телефоне	• В театр, на аттракцион или на какое-либо мероприятие

Потребительская суть технологии NFC применительно к мобильной коммерции, привлекающей сегодня наибольшее внимание специалистов, состоит в возможности

размещения поставщиком товаров/услуг/информации множества сравнительно простых и дешевых устройств с интерфейсом NFC (меток) в местах, удобных для бизнеса поставщика. Метки могут использоваться самостоятельно либо как дополнение к платежному терминалу или другому устройству. При поднесении телефона, снабженного интерфейсом NFC, к метке активируется обмен информацией между меткой и телефоном, в результате чего программное приложение (мидлет), записанное в телефонном аппарате, без участия абонента взаимодействует с информационной системой поставщика.

Все многообразие возможных услуг NFC через оператора мобильной связи укладывается в рамки следующих основных сценариев:

– запрос и получение бесплатной информации любым пользователем;

– запрос и получение бесплатной информации авторизованным пользователем;

– запрос платной услуги с отсроченным ее получением (например, покупка электронного билета);

– запрос и немедленное получение платной услуги (проход через турникет);

– получение заказанной ранее и оплаченной услуги (использование электронного билета).

В качестве примера на рис. 4.7 показан сценарий запроса и немедленного получения платной услуги с использованием мобильного телефона с функцией NFC.

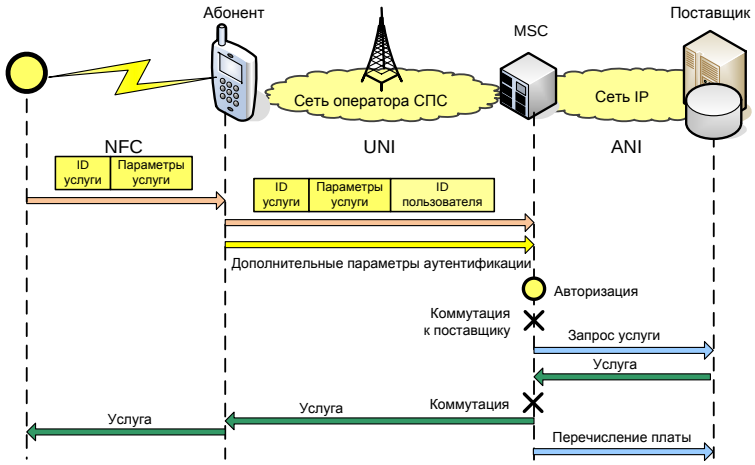


Рис. 4.7 - Сценарий запроса и немедленного получения платной услуги с помощью NFC

Интерфейс NFC на уровне приложений должен как минимум обеспечивать передачу идентификатора услуги и, если потребуется, параметров услуги. В телефонном мидлете информация, полученная от метки, передается в центр коммутации мобильной связи (MSC), где должна быть проверена допустимость запрошенной услуги для данного абонента. На основе идентификатора (ID) услуги определяется адрес, по которому передается запрос поставщику услуги. В ответ поставщик отправляет соответствующий контент, который после выполнения в MSC контрольных процедур направляется абоненту.

4.4 Промышленные сети для реализации M2M

Промышленной сетью называют комплекс оборудования и программного обеспечения, которые обеспечивают обмен информацией (коммуникацию) между несколькими устройствами (различные датчики, исполнительные механизмы, промышленные контроллеры) в рамках промышленной автоматизированной системы. Промышленная сеть является основой для построения распределенных систем сбора данных и управления на промышленных предприятиях. За рубежом для обозначения промышленных сетей часто используется термин Fieldbus, дословно – «полевая шина». Термин употребляется

преимущественно в автоматизированной системе управления технологическими процессами (АСУ ТП).

Промышленные сети используются для:

– передачи данных между датчиками, контроллерами и исполнительными механизмами;

– диагностики и удалённого конфигурирования датчиков и исполнительных механизмов;

– калибрования датчиков;

– питания датчиков и исполнительных механизмов;

– связи между датчиками, исполнительными механизмами, ПЛК и АСУ ТП верхнего уровня.

Промышленные сети могут взаимодействовать с обычными компьютерными сетями, в частности использовать глобальную сеть интернет.

Промышленные сети отличаются от традиционных локальных вычислительных сетей (ЛВС), размещаемых в организациях и учреждениях, следующими свойствами:

– специальным конструктивным исполнением, обеспечивающим защиту от пыли, влаги, вибрации, ударов;

– широким температурным диапазоном (обычно $-40 \div +70\ ^0C$);

– повышенной прочностью кабеля, изоляции, разъемов, элементов крепления;

– повышенной устойчивостью к воздействию электромагнитных помех;

– возможностью резервирования для повышения надежности;

– повышенной надежностью передачи данных;

– возможностью самовосстановления после сбоя;

– детерминированностью (определенностью) времени доставки сообщений;

– возможностью работы в реальном времени (с малой, постоянной и известной величиной задержки);

– работой с длинными линиями связи (от сотен метров до нескольких километров).

Промышленные сети обычно не выходят за пределы одного предприятия. Однако с появлением Ethernet и интернет для промышленных сетей стали применять ту же классификацию, что и для ЛВС: LAN, MAN, WAN.

В настоящее время насчитывается более 50 типов промышленных сетей. Однако широко распространенными является только часть из них. В России подавляющее большинство АСУ ТП используют сети Modbus и Profibus. В последние годы возрос интерес к сетям на основе CANopen и DeviceNet. Распространенность в России той или иной промышленной сети связана, в первую очередь, с предпочтениями и активностью Российских фирм, продающих импортное оборудование.

Поскольку в промышленной автоматизации сетевые интерфейсы могут быть неотъемлемой частью соединяемых устройств, а сетевое программное обеспечение прикладного уровня модели OSI исполняется на основном процессоре промышленного контроллера, то отделить сетевую часть от устройств, объединяемых в сеть, иногда физически невозможно. С другой стороны, смену одной сети на другую часто можно выполнить с помощью замены сетевого ПО и сетевого адаптера или введением преобразователя интерфейса, поэтому часто один и тот же тип программируемого логического контроллера (ПЛК) может использоваться в сетях различных типов.

Соединение промышленной сети с ее компонентами (устройствами, узлами сети) выполняется с помощью *интерфейсов*. Наиболее важными параметрами интерфейса являются пропускная способность и максимальная длина подключаемого кабеля. Промышленные интерфейсы обычно обеспечивают гальваническую развязку между соединяемыми устройствами. Наиболее распространены в промышленной автоматизации последовательные интерфейсы RS-485, RS-232, RS-422, Ethernet, CAN, HART, AS-интерфейс.

Для обмена информацией взаимодействующие устройства должны иметь одинаковый *протокол обмена*. Для большинства промышленных сетей стек протоколов реализован с помощью специализированных сетевых микросхем или встроен в универсальный микропроцессор.

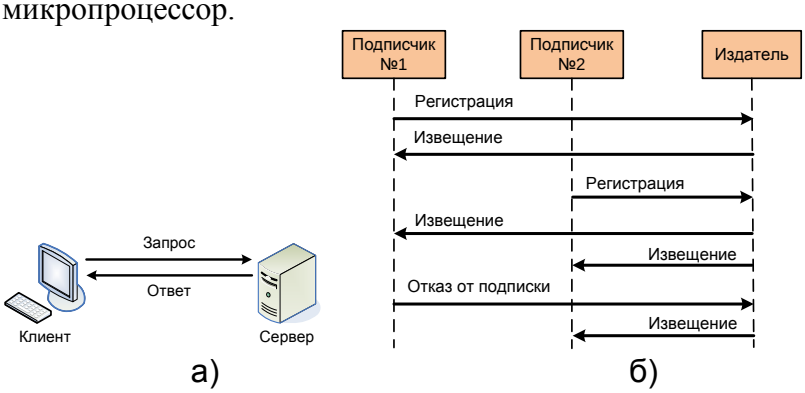


Рис 4.8 – Схемы взаимодействия устройств в промышленных сетях: а) клиент-сервер; б) издатель-подписчик

Взаимодействие устройств в промышленных сетях выполняется в соответствии с моделями *клиент-сервер* или *издатель-подписчик* (производитель-потребитель) (рис. 4.8). В модели клиент-сервер взаимодействуют два объекта (рис. 4.8а). Сервером является объект, который предоставляет сервис, т. е. который выполняет некоторые действия по запросу клиента. Сеть может содержать несколько серверов и несколько клиентов. Каждый клиент может посылать запросы нескольким серверам, а каждый сервер может отвечать на запросы нескольких клиентов. Эта модель удобна для передачи данных, которые появляются периодически или в заранее известное время, как, например, значения температуры в периодическом технологическом процессе. Однако эта модель неудобна для передачи случайно возникающий событий, например, события, состоящего в случайном срабатывании датчика уровня, поскольку для получения этого события клиент должен периодически, с высокой частотой, запрашивать состояние датчика и анализировать его, перегружая сеть бесполезным трафиком.

В модели взаимодействия издатель-подписчик имеется один издатель и множество подписчиков (рис. 4.8б). Подписчики при регистрации сообщают издателю список меток (тегов), значения которых они хотят получать по определенному расписанию или по мере появления новых данных. Каждый клиент может подписаться на свой набор тегов. В соответствии с установленным расписанием издатель рассылает подписчикам извещения с запрошенной информацией.

В любой модели взаимодействия можно выделить устройство, которое управляет другим (подчиненным) устройством. Устройство, проявившее инициативу в обмене, называют *ведущим* или *главным* (master). Устройство, которое отвечает на запросы мастера, называют ведомым или подчиненным (slave). Ведомое устройство никогда не начинает коммуникацию первым. Оно ждет запроса от ведущего и только отвечает на запросы. Например, в модели клиент-сервер клиент является ведущим, сервер - подчиненным. В модели издатель-подписчик на этапе подписки ведущим является клиент, а на этапе рассылки публикаций – сервер.

В сети может быть одно или несколько ведущих устройств. Такие сети называется, соответственно, *одномастерными* или *многомастерными*. В многомастерной сети возникает проблема разрешения конфликтов между устройствами, пытающимися одновременно получить доступ к среде передачи информации. Конфликты могут быть разрешены методом передачи маркера, как, например, в сети Profibus, методом побитного сравнения идентификатора (используется в CAN), методом прослушивания сети (используется в Ethernet) и методом предотвращения коллизий (используется в беспроводных сетях).

Во всех сетях применяется *широковещательная рассылка* без определенного адреса, т.е. всем участникам сети. Такой режим используется обычно для синхронизации процессов в сети, например, для одновременного запуска процесса ввода данных всеми устройствами ввода или для синхронизации часов.

Некоторые сети используют *многоабонентский режим*, когда одно и то же сообщение посылается нескольким устройствам одновременно.

Сети могут иметь топологию звезды, кольца, шины или смешанную. *Звезда* в промышленной автоматизации используется редко. *Кольцо* используется в основном для передачи маркера в многомастерных сетях. *Шинная топология* является общепринятой, что является одной из причин применения термина «промышленная шина» вместо «промышленная сеть». К общей шине в разных местах может быть подключено произвольное количество устройств. Характеристики наиболее распространенных типов промышленных сетей приведены в табл. 4.4.

Табл. 4.4 - Характеристики промышленных сетей

Прото-кол	Кол-во веду-щих узлов	Топо-логия	Макс. длина сегмента	Макс. скоро-сть	Кол-во прово-дов	Макс. кол-во стан-ций	Макс. блок дан-ных	Стан-дарт
ASI	один	шина/дерево	100 м	167 кбит/с	2	32	4 бита	EN50295
CAN	много	шина	500 м/125 кбит/с; 40 м / 1 Мбит/с	1 Мбит/с	2	64	8 байт	ISO 11898 ISO 11519
DeviceNet	много	шина	500 м/125 кбит/с; 100 м/500 кбит/с	500 кбит/с	4	64	8 байт	Откр ыт. спец ифик ации
Foun-dation Fieldbus	много	шина	2000 м, 9,5 км - общая	31,25 кбит/с	2	240	246 байт	Откр ыт. спец ифик ации
HART	два	шина	100 м	1200 бит/с	2	15	25 байт	Откр ыт. спец ифик ации
Profibus PA	один	шина	1,9 км	93,75 кбит/с	2	32	246 байт	EN50170
Profibus DP	много	шина	1 км/12 Мбит/с (4 повторит)	12 Мбит/с	2	127	246 байт	EN50170
Modbus+	много	шина	1,8 км	1 Мбит/с	2	32	32 байта	Фирм ен-ный

4.5 Современное состояние и перспективы применения M2M

Оценки и прогнозы развития рынка M2M-оборудования крайне оптимистичны, а потенциал развивающейся M2M-индустрии очень большой. На данном этапе технология M2M продолжает активно развиваться, системы стали более высокоинтеллектуальными, а

сфера их применения практически безгранично расширилась. Возросли возможности практической реализации различных M2M-решений также благодаря снижению стоимости на устройства беспроводной связи, повышению их производительности и функциональности. Способность управлять удаленными устройствами с помощью беспроводного сигнала позволила свести к минимуму зависимость от местонахождения и времени. Последнее поколение M2M-модулей обеспечивает поддержку таких базовых технологий, как GSM/GPRS, GPS, Bluetooth, ZigBee и др.

Сегодня M2M-оборудование очень широко используется в противоугонных и охранных системах, оно стало неотъемлемой частью многих правоохранительных структур. Внедрение данной технологии позволяет обеспечить максимально быструю реакцию спецслужб при попытке угона автомобиля или взлома квартиры. Сигнал о происшествии передается по сети GSM на диспетчерский пульт дежурному оператору в виде SMS-сообщения или голосового сигнала, одновременно возможно оповещение владельца. Особенно ощутима поддержка M2M систем в плохо телефонизированных районах.

Кроме мониторинга стационарных объектов применение M2M возможно в системах мобильного позиционирования. Таксопарки, грузоперевозчики и многие другие компании могут отслеживать перемещения своих автомобилей в реальном масштабе времени, получать информацию об их техническом состоянии, корректировать маршруты, тем самым, ускоряя доставку груза. Кроме того при возникновении аварии автоматическое сообщение с указанием места происшествия мгновенно направляется в службу спасения (например, системы экстренного реагирования при авариях: отечественная – ЭРА-ГЛОНАСС, американская – E911, европейская – eCall).

Мобильные системы M2M давно и успешно используются в банковском секторе. К примеру, банкоматы или платёжные терминалы могут автоматически передавать необходимую информацию по GSM-сетям, а если у них, а также если закончилась чековая бумага или наличность, или же наоборот, что наличности слишком много и требуется приезд инкассаторов. Применять M2M можно и в аграрном комплексе, датчики мониторинга влажности почвы позволят сделать расход воды максимально экономичным и эффективным. А система «умный дом» давно превратилась из мечты в реальность, ее многочисленные преимущества может оценить каждый желающий. Модулями связи снабжают множество различных датчиков контроля температуры, уровня освещенности, механического напряжения мостов, давления в трубопроводах, датчиков огня и дыма и т.д.

В системах M2M используются различные беспроводные технологии связи. Чаще всего применяются публичные сетевые коммуникации (сотовые, спутниковые, Ethernet и WiFi), в то время как технологии, оптимизированные для индивидуальных устройств – например, ZigBee и Bluetooth – все еще используются сравнительно редко (рис. 4.9).

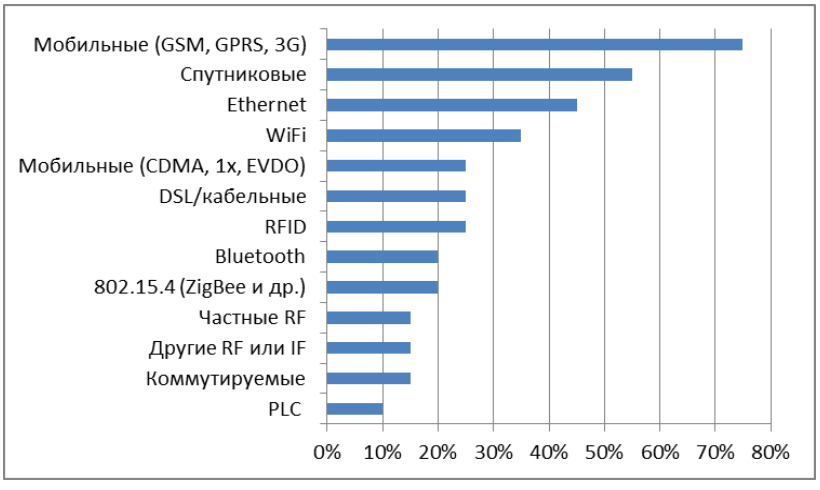


Рис. 4.9 – Доля беспроводных технологий, используемых в системах M2M (источник: Duke-Wooley, 2012)

Контрольные вопросы по главе 4

1. В чем заключается основная особенность межмашинного взаимодействия M2M?
2. Что включает функциональная архитектура M2M стандарта ETSI?
3. Какие интерфейсные точки стандартизированы в функциональной архитектуре M2M?
4. В чем особенность технологии связи на малых расстояниях NFC?
5. Каков принцип обмена данными по технологии NFC?
6. Укажите три основных режима работы технологии NFC.
7. Какие бывают типы меток NFC? В чем их отличие?
8. В чем особенность промышленных сетей для реализации M2M?
9. Какие модели взаимодействия устройств применяются в промышленных сетях?
10. Какие режимы и топологии используются в промышленных сетях?
11. Приведите примеры применения технологий M2M.

ГЛАВА 5 СТАНДАРТЫ И ПРОТОКОЛЫ ПЕРЕДАЧИ ДАННЫХ В IoT

5.1 Классификация технологий передачи данных в IoT

Одним из главных вопросов организации Интернета вещей является реализация взаимодействия между:

–интернет-вещами,

–пользователями и интернет-вещами,

–удалённым сервером и интернет-вещами.

IoT использует большое количество вариантов сетей связи для передачи данных, начиная от сети на теле человека BAN (Body Area Network), которая работает на расстоянии в несколько десятков сантиметров, вплоть до всемирной сети интернет. Коммуникации малой дальности используют такие технологии, как RFID, NFC, Bluetooth, Wi-Fi и др. Коммуникации большого радиуса действия реализуются на базе различных сотовых сетей (2G/3G/4G), сетей беспроводного широкополосного доступа WiMAX, сетей позиционирования GPS/ГЛОНАСС и др.

По территории охвата телекоммуникационные сети, используемые в Интернете вещей, можно разделить на 4 основных типа (рис. 5.1):

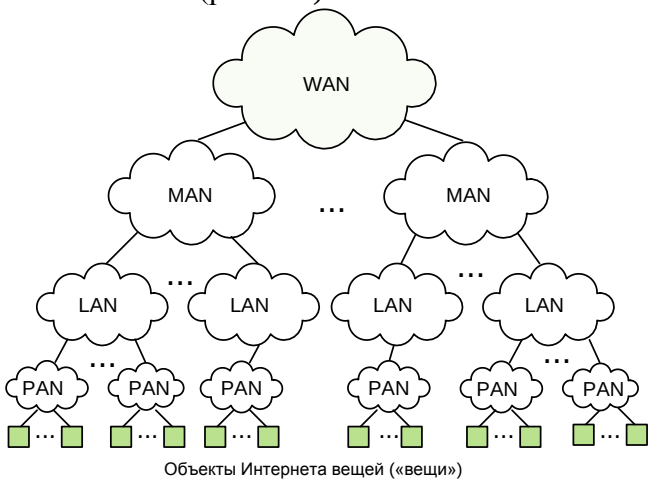


Рис. 5.1 – Иерархия сетевых технологий, используемых в IoT

1. *Персональная сеть PAN (Personal Area Network)* – это сеть, построенная «вокруг» человека. Данные сети призваны объединять все персональные устройства пользователя (телефоны, смартфоны, карманные персональные компьютеры, ноутбуки, гарнитуры и др.). Применительно к IoT такая сеть строится «вокруг» устройства («вещи»).

2. *Локальная сеть LAN (Local Area Network)* – сеть, покрывающая обычно относительно небольшую территорию или небольшую группу зданий (дом, офис, фирму). К локальным сетям можно отнести и *сеть контроллеров CAN (Controller Area Network)* – промышленную сеть, ориентированную, прежде всего, на объединение в единую сеть различных исполнительных устройств и датчиков в рамках отдельного предприятия.

3. *Городская сеть MAN (Metropolitan Area Network)* – объединяет отдельных пользователей и локальные сети в пределах города, представляет собой сеть по размерам большую, чем LAN, но меньшую, чем WAN.

4. *Глобальная сеть WAN (Wide Area Network)* – связывает пользователей и сети, рассредоточенные на расстоянии сотен и тысяч километров.

Интернет вещей практически не выдвигает особых требований к технологиям LAN, MAN и WAN, кроме того они достаточно хорошо освещены в технической литературе. Поэтому в данной главе рассмотрены только стандарты и протоколы сетей малого и среднего радиуса действия, которые широко используются в IoT.

Все технологии передачи данных в Интернете вещей в зависимости от используемой среды передачи можно разделить на два больших класса: проводные и беспроводные.

Проводные технологии передачи данных в IoT могут использовать металлический (медный) кабель связи, электропроводку (технология PLC – Power Line Communication) или волоконно-оптический кабель. Однако ввиду сложностей физической реализации линий связи проводные технологии для коммуникаций интернет-вещей применяются в меньшей степени, чем беспроводные.

Беспроводные сети малого радиуса действия, используемые в IoT, можно разделить на три вида:

1. *Беспроводные персональные сети WPAN (Wireless Personal Area Network).*

Применяются для связи различных устройств, включая компьютерную, бытовую и оргтехнику, средства связи и т.д. Физический и канальный уровни регламентируются стандартом IEEE 802.15.4. Радиус действия WPAN составляет от нескольких метров до нескольких десятков сантиметров. Такие сети используются как для объединения отдельных устройств между собой, так и для связи их с сетями более высокого уровня, например, глобальной сетью интернет. WPAN может быть развёрнута с использованием различных сетевых технологий, например, Bluetooth, ZigBee, 6LoWPAN и других, рассмотренных далее в данной главе.

2. *Беспроводные сенсорные сети WSN (Wireless Sensor Network).*

Распределённые, самоорганизующиеся сети множества датчиков (сенсоров) исполнительных устройств, объединенных между собой посредством радиоканала. Область покрытия подобных сетей может составлять от нескольких метров до нескольких километров за счёт способности ретрансляции сообщений от одного элемента к другому.

3. *Малые локальные сети TAN (Tiny Area Network).*

Вычислительные сети, развертываемые в пределах небольшого офиса или отдельного жилища. Их часто называют домашними сетями, так как они объединяют компьютеры, бытовую электронику и приборы сигнализации, принадлежащие одной семье. Наиболее часто такие сети строятся на базе технологии Wi-Fi.

Таблица 5.1 – Стандарты и протоколы IoT

Стандарт	Частота, МГц	Скорость, кбит/с	Уровни протокола						Шифрование
			PHY	MAC	NWK	TRP	APS	ACL	
IEEE 802.15.4	868/915/2400	20/40/250	+	+	-	-	-	+	+
ZigBee	2400	250	-	-	+	+	+	+	+
6LoWPAN	-	50-200	-	-	+	-	-	+	+
WirelessHART	2400	250	+	+	+	+	+	+	+
ISA100.11a	2400	250	+	+	+	+	+	+	+
Z-Wave	865/915/869	9,6/40	+	+	+	-	+	-	-
Bluetooth LE	2400	1000	+	+	+	+	+	+	+
DECT ULE	1880-1900	1000	+	+	+	-	-	+	+

Для взаимодействия огромного количества разнообразных устройств в IoT требуются стандартизированные интерфейсы, форматы данных и коммуникационные протоколы. В табл. 5.1 приведен перечень некоторых стандартов и протоколов IoT с указанием рабочей частоты, скорости передачи данных, поддержки уровней OSI (физического PHY, доступа к среде MAC, сетевого NWK, транспортного TRP), а также реализации подуровня поддержки приложений APS (Application Support Sublayer), поддержки списков управления доступом ACL (Access Control List) и 128-битного стандарта шифрования AES (Advanced Encryption Standart).

5.2 Стандарт IEEE Std 802.15.4

Стандарт IEEE Std 802.15.4 предназначен для реализации беспроводных персональных сетей WPAN большой емкости с низким энергопотреблением и низкой скоростью передачи данных. Он реализует только два нижних уровня стека протоколов – физический уровень (PHY) и уровень доступа к среде (MAC). Стандарт 802.15.14 является базовой основой для более высокоуровневых протоколов, таких как ZigBee, WirelessHART и MiWi. Он может быть также использован совместно со стандартом 6LoWPAN и стандартными протоколами Интернета для построения беспроводных сенсорных сетей (рис. 5.2).

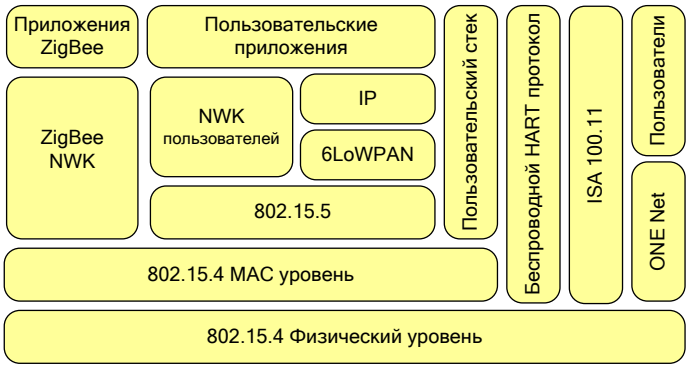


Рис. 5.2 - Стек протоколов для стандарта IEEE Std 802.15.4

Физический уровень 802.15.14 PHY определяет способ передачи данных, интерфейс организации связи, аппаратные особенности и параметры, необходимые для построения сети. На практике физический уровень управляет работой трансивера, выполняет выбор каналов, сигналов управления и уровня мощности передачи.

В стандарте 802.15.4 на физическом уровне под обмен данными зарезервированы 27 каналов в трёх частотных диапазонах: 868 МГц, 910 МГц и 2.4 ГГц, что позволяет использовать стандарт в нелицензируемом в большинстве стран мира диапазоне для промышленных, научных и медицинских целей ISM (Industrial Scientific Medical). На территории Российской Федерации доступен к использованию только диапазон 2.4 ГГц. В данном диапазоне определены 16 каналов шириной 5 МГц с несущими частотами, вычисляемыми в соответствие с выражением:

$Fc = 2405 + 5(k - 1)$, МГц, где $k = 1, \ldots, 16$.

Первая версия стандарта 802.15.4 определяла два физических уровня с широкополосной модуляцией с прямым расширением спектра DSSS (Direct Sequence Spread Spectrum): первый – в полосе 868/915 МГц со скоростью передачи соответственно 20 и 40 кбит/с, а второй – в полосе 2450 МГц со скоростью 250 кбит/с. В 2006 году допустимые скорости передачи данных на частотах 868/915 МГц были увеличены до 100 и 250 кбит/с. Кроме того были определены четыре спецификации физического уровня в зависимости от метода модуляции: при сохранении широкополосной модуляции DSSS возможно

использовании в диапазоне 868/915 МГц как двоичной, так и квадратурной фазовой манипуляции QPSK (Quadrature Phase Shift Keying). С 2007 года в версию стандарта IEEE 802.15.4a число физических уровней было увеличено до шести за счёт включения уровня с сверхширокополосной радиотехнологией UWB (Ultra WideBand) для высокоскоростной передачи данных, а также спецификации уровня с радиотехнологией CSS (Chirp Spread Spectrum), основанной на расширении частотного спектра методом линейной частотной модуляции. Физический уровень UWB определён выделенными частотами в трёх диапазонах: ниже 1 ГГц, 3-5 ГГц и 6-10 ГГц, а для CSS выделен спектр в полосе 2450 МГц нелицензируемого диапазона ISM. В 2009 году в версиях стандартов IEEE 802.15.4c и IEEE 802.15.4d были расширены доступные частотные диапазоны. Данные спецификации определяют возможность использования на физическом уровне приёмо-передающие устройства с квадратурной фазовой манипуляцией QPSK или с фазовой манипуляцией более высоких порядков на частоте 780 МГц, а на частоте 950 МГц – гауссовскую частотную манипуляцию GFSK (Gaussian Frequency-Shift Keying) или двоичную фазовую манипуляцию BPSK (Binary Phase-Shift Keying).

На канальном уровне спецификация IEEE 802.15.4 определяет механизмы взаимодействия элементов сети на физическом уровне для обеспечения формирования фрагментов данных (кадров), проверки и исправления ошибок, отправки кадров на сетевой уровень. При этом подуровень MAC канального уровня регулирует множественный доступ к физической среде с разделением по времени, управляет связями трансиверов и обеспечивает безопасность.

Стандарт IEEE Std 802.15.4 обеспечивает двустороннюю полудуплексную передачу данных, поддерживая при этом шифрование AES 128. Доступ к каналу основан на принципе Carrier Sense Multiple Access With Collision Avoidance (CSMA/CA) – многостанционный доступ с контролем несущей и предотвращением конфликтов. CSMA/CA – это сетевой протокол, в котором используется принцип прослушивания несущей частоты. Устройство, которое готово к передаче данных посылает jam signal (сигнал затора) и прослушивает эфир. Если обнаруживается "чужой" jam signal, то передатчик "засыпает" на случайный промежуток времени, а затем снова пробует начать передачу фрейма. Таким образом, передача может исходить только от одного устройства, что повышает производительность сети. При этом данные передаются относительно небольшими пакетами, что характерно для трафика сигналов управления и мониторинга в БСС. Важной особенностью стандарта является обязательное подтверждение доставки сообщений.

Особенностью устройств, объединённых в сеть по стандарту IEEE Std 802.15.4, является низкое энергопотребление за счёт перехода трансивера в режим «засыпания» при отсутствии данных для пересылки и сохранении подключения в этом режиме. При разработке стандарта основной акцент делался на быстроту процессов конфигурирования и реконфигурирования. В частности, переход приемника в активное состояние длится порядка 10-15 мс, а подключение к сети новых устройств – от 30 мс. При этом длительность реконфигурации и подключения устройств зависит от постоянства «прослушивания» маршрутизаторами сети.

Стандарт определяет два типа узлов сети:

1) *полнофункциональное устройство FFD (Fully Function Device)*, которое может реализовать как функцию координации работы и установки параметров сети, так и работать в режиме типового узла;

2) *устройство с ограниченным набором функций RFD (Reduced Function Device)*, обладающее только возможностью поддержания связи с полнофункциональными устройствами.

В любой сети должен быть, по крайней мере, один FFD, реализующий функцию координатора. Каждое устройство имеет 64-битный идентификатор, но в некоторых случаях для ограниченной области может использоваться краткий 16-битный для соединений в персональной сети PAN.

На канальном уровне стандарте IEEE Std 802.15.4 приведены общие рекомендации к построению топологии сети. Сети могут быть одноранговыми *P2P (peer-to-peer, point-to-point)*, либо иметь топологию «звезда». На основе структуры P2P могут формироваться произвольные структуры соединений, ограниченные лишь дальностью связи между парами узлов. С учётом этого возможны различные варианты топологической структуры БСС, в частности «дерево» кластеров – структура, в которой RFD, являясь «листьями дерева», связаны только с одним FFD, а большинство узлов в сети являются FFD. Возможна также ячеистая топология сети, сформированная на основе кластерных «деревьев» с локальным координатором для каждого кластера и содержащая глобальный сетевой координатор (рис. 5.3).

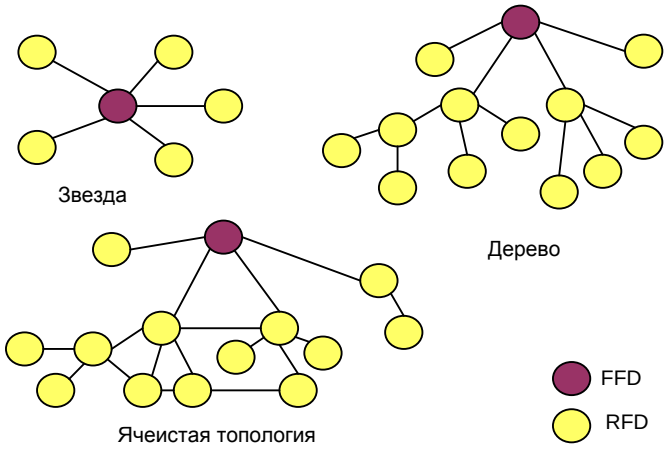


Рис.5.3 - Варианты топологии сетей стандарта IEEE Std 802.15.4

5.3 Стандарт ZigBee

Как было указано выше, стандарт IEEE Std 802.15.4 описывает два нижних уровня сетевой модели OSI, не определяя требований к верхним уровням и условий их совместимости. Решения этих задач потребовало разработки специальных коммуникационных протоколов. Наиболее известными являются протоколы альянса ZigBee, которой был создан крупнейшими мировыми компаниями, специализирующимися в области разработки программно-аппаратных средств для инфокоммуникационных систем. В числе более чем двухсот членов альянса ZigBee, координирующих работы по продвижению технологий и производству технических средств для беспроводных сенсорных сетей - Texas Instruments, Motorola, Philips, IBM, Ember, Samsung, NEC, Freescale Semiconductor, LG, OKI и многие другие. Альянс разработал и ратифицировал в 2004 году стандарт ZigBee, включающий полный стек протоколов для беспроводных сенсорных сетей. Название спецификации ZigBee произошло от Zig-zag – зигзаг и Bee – пчела. Подразумевалось, что топология сети будет напоминать зигзагообразную траекторию полета пчелы от цветка к цветку.

Спецификация ZigBee ориентирована на приложения, требующие гарантированной безопасной передачи данных при относительно небольших скоростях и возможности длительной работы сетевых устройств от автономных источников питания (батарей). Она обеспечивает невысокое потребление энергии и передачу данных со скоростью до 250 Кбит/с на расстояние до 75 метров в условиях прямой видимости. Характеристики ZigBee приведены в табл. 5.2.

Таблица 5.2 –Характеристики технологии ZigBee

Параметр	**Значение**
Частотный диапазон, МГц	868/915/2400
Битовая скорость, кбит/с	20/40/250
Тип модуляции сигнала	BPSK/BPSK/O-QPSK

Метод расширения спектра	DSSS
Чувствительность приемника, дБм	-92 или лучше для 868/915 МГц; -85 или лучше для 2400 МГц
Выходная мощность передатчика, дБм	-32...0
Размер данных пакета, байт	До 127
Адресация	16- и 64-бит MAC, 16-бит идентификатор сети
Типовые требования к реализации стека протоколов	45...128 кбайт ПЗУ; 2,7...12 кбайт ОЗУ

ZigBee базируется на стандарте IEEE Std 802.15.4, который описывает только физический уровень и уровень доступа к среде MAC для беспроводных сетей передачи данных с низким энергопотреблением (рис. 6.4). Стандарт ZigBee включает описание сетевых процессов управления, совместимости и профилей устройств, а также информационной безопасности. На сетевом уровне в ZigBee определены механизмы маршрутизации и формирования логической топологии сети.

Рис. 5.4 - Конфигурация стеков протоколов 802.15.4 и ZigBee

Основная особенность технологии ZigBee заключается в том, что она при малом энергопотреблении поддерживает не только простые топологии сети («точка-точка», «дерево» и «звезда»), но и самоорганизующуюся и самовосстанавливающуюся ячеистую (mesh) топологию с ретрансляцией и маршрутизацией сообщений. Кроме того, спецификация ZigBee содержит возможность выбора алгоритма маршрутизации, в зависимости от требований приложения и состояния сети, механизм стандартизации приложений — профили приложений, библиотека стандартных кластеров, конечные точки, привязки, гибкий механизм безопасности, а также обеспечивает простоту развертывания, обслуживания и модернизации. Применение сетей ZigBee в Российской Федерации в частотном диапазоне 2,405-2,485 ГГц не требует получения частотных разрешений и дополнительных согласований (Решение ГКРЧ при Мининформсвязи России от 07.05.2007 № 07-20-03-001).

В области технологий беспроводных сенсорных сетей ZigBee является стандартом, в наибольшей степени подкреплённым представленными на рынке полностью совместимыми аппаратными и программными средствами. Кроме того протоколы ZigBee позволяют сетевым устройствам находиться в спящем режиме бо́льшую часть времени, что существенно увеличивает ресурс работы узлов при питании от батарейных источников. В

БСС на основе ZigBee поддерживается режим «профилей устройств» или профилей для различных датчиков, которые совместимы на уровне стека протокола и могут объединяться в сеть, передавать, принимать и ретранслировать информацию. В то же время «понимать» эту информацию будет только то устройство, для которого она предназначена.

Все устройства стандарта ZigBee в зависимости от уровня сложности подразделяются на три класса, высший из которых – *координатор* – управляет процессом формирования сети, хранит данные о её топологии и служит шлюзом для передачи данных собираемых от всех сенсоров БСС для их дальнейшей обработки. В сети, как правило, используется только один PAN-координатор. Среднее по сложности устройство – *маршрутизатор* – способно ретранслировать сообщения, поддерживать все топологии сети, а также выполнять функции координатора кластера. И, наконец, самое простой узел – *оконечное устройство* – способен лишь передавать данные ближайшему маршрутизатору (рис. 5.5).

Таким образом, стандарт ZigBee поддерживает сеть с кластерной архитектурой, сформированной из обычных узлов, объединённых в кластеры посредством маршрутизаторов. Маршрутизаторы кластеров запрашивают сенсорные данные от устройств и, ретранслируя их друг другу, передают координатору, который обычно имеет связь с внешней IP-сетью, куда и отправляет информацию для накопления и окончательной обработки.

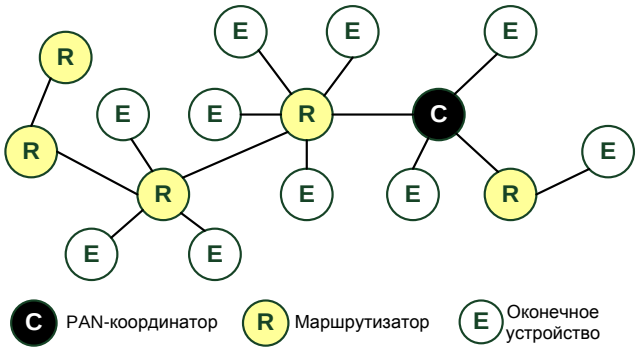


Рис. 5.5 - Типовая топология сети ZigBee

Сеть ZigBee является самоорганизующейся, то есть все узлы способны самостоятельно определять и корректировать маршруты доставки данных. Данные передаются с помощью радиопередатчиков от одних узлов к другим по цепочке, и в итоге ближайшие к шлюзу узлы сбрасывают всю аккумулированную информацию на шлюз. Эта информация включает данные, считываемые с сенсорных датчиков, а также данные о состоянии устройств и результатах процесса передачи информации. В случае выхода части устройств из строя, работа сенсорной сети после реконфигурации должна продолжиться. Беспроводные узлы функционируют под управлением специального приложения. Обычно все узлы сенсорной сети используют одну и ту же управляющую программу, обеспечивающую их функциональность и выполнение сетевых протоколов.

Концерн RF4CE (Radio Frequency for Consumer Electronics) совместно с альянсом ZigBee разработал стандартизированную спецификацию ZigBee RF4CE, предназначенную для использования в бытовых дистанционно управляемых аудио/видео устройствах, таких как телевизоры, телеприставки и игровые консоли. Она имеет ряд преимуществ по сравнению с существующими техническими решениями для дистанционного управления, включая управление работой в зоне непрямой видимости, функциональность манипулятора типа "мышь" и клавиатуры, управление с распознаванием жестов и сенсорным вводом, двусторонняя связь, более длительное время работы от аккумулятора.

5.4 Стандарт 6LoWPAN

6LoWPAN (IPv6 Low-Power Wireless Personal Area Network) – стандарт, обеспечивающий взаимодействие малых беспроводных сетей с сетями IP по протоколу IPv6 с малым энергопотреблением. Стандарт разработан группой IETF и описан в RFC 4944 и RFC 4919. Технология используется в основном для организации сетей датчиков и автоматизации жилого и офисного помещения с возможностью управления через интернет, однако может использоваться и автономно для реализации простых беспроводных сетей датчиков. Передача данных в стандарте 6LoWPAN подразумевает использование субгигагерцового диапазона и обеспечивает скорость передачи от 50 до 200 Кбит/с на расстояние до 800 метров.

Архитектура сетей 6LoWPAN несколько отличается от традиционных архитектур IP-сетей (наличие специализированного коммутационного оборудования, маршрутизаторов, медиа-конверторов) и от сложившихся архитектур беспроводных сетей сбора данных. Ближе всего к ней находится архитектура WiFi-сетей, хотя и от нее есть ряд отличий.

Прежде всего, сети 6LoWPAN являются подсетями IPv6-сетей, т.е. они могут взаимодействовать с другими сетями и узлами IP-сети, но не являются транзитными для ее сетевого трафика. Сети 6LoWPAN состоят из узлов, которые могут также исполнять роль маршрутизаторов (host и router), кроме этого в сети может присутствовать один или более так называемых граничных маршрутизаторов (edge routers). Участие в маршрутизации не является обязательным требованием для узла сети и он может играть роль, аналогичную роли конечного устройства в сетях ZigBee или устройства с ограниченной функциональностью для сетей 802.15.4, в терминологии 6LoWPAN – *«хост-узел» H* (host). Узел, способный выполнять маршрутизацию в пределах сети 6LoWPAN, называется *роутером* или *маршрутизатором R* (router). Граничный маршрутизатор отвечает за взаимодействие подсети 6LoWPAN с сетью IPv6, участвует в процедуре инициализации и маршрутизации в подсети 6LoWPAN, осуществляет компрессию/декомпрессию заголовков IPv6 при обмене с внешней сетью, в случае подключения к сети IPv4 может играть роль шлюза IPv6↔IPv4. Узлы подсети разделяют 64-битный префикс IPv6, который также является частью сетевого адреса граничного маршрутизатора. Для адресации внутри сети можно пользоваться оставшимися 64 битами (MAC-адрес сетевого интерфейса) или использовать сжатие адреса и укороченную 16-битную схему адресации (младшие два байта MAC-адреса). Предполагается, что сетевой адрес напрямую включает адрес сетевого интерфейса, это исключает необходимость применения протокола определения сетевых адресов ARP (Address Resolution Protocol).

Выделяют три типа сетей 6LoWPAN (рис. 5.6):

- ad-hoc (самоорганизующаяся, динамическая);
- простая 6LoWPAN-сеть;
- расширенная 6LoWPAN-сеть.

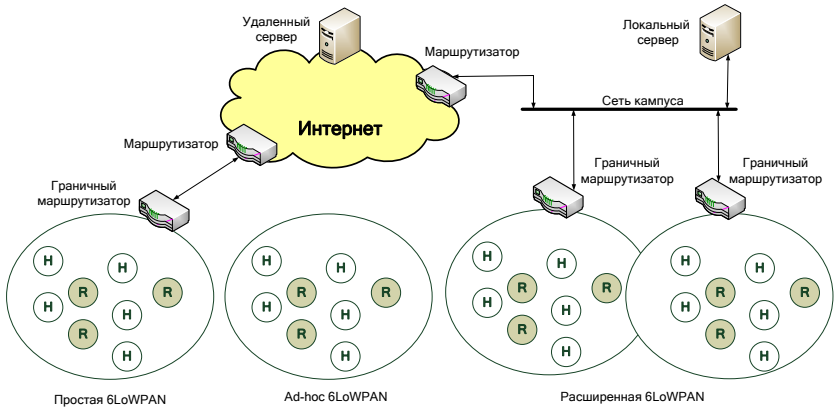


Рис. 5.6 - Типы сетей 6LoWPAN (R- маршрутизатор, H – хост)

Ad-hoc-сеть не имеет подключения к внешней IP-сети, не имеет граничного маршрутизатора. Является самоорганизующейся сетью, использующей стек протоколов 6loWPAN для организации работы и передачи данных между узлами.

Простая 6LoWPAN-сеть подключена к другой IP-сети при помощи одного граничного маршрутизатора. Граничный маршрутизатор может быть подключен к внешней IP-сети напрямую (подключение типа «точка-точка», например, GPRS/3G-модем) или может входить в состав кампусной сети (например, сети организации).

Расширенная 6LoWPAN-сеть состоит из одной или нескольких подсетей, подключенных к внешней IP-сети через несколько граничных маршрутизаторов, подключенных к одной сети (например, локальная сеть организации). При этом граничные маршрутизаторы в расширенной сети разделяют один и тот же сетевой префикс. Узлы расширенной сети могут свободно перемещаться в пределах сети и осуществлять обмен с внешней сетью через любой граничный маршрутизатор (обычно выбирается маршрут с наилучшими показателями качества сигнала – уровень ошибок, уровень сигнала).

Взаимодействие между узлами в сети 6LoWPAN, а также взаимодействие с внешними узлами осуществляется так же, как и в обычной IP-сети. Каждый узел имеет свой уникальный IPv6-адрес и может принимать и передавать пакеты IPv6. Упрощенная структура стека протоколов 6LoWPAN в сравнении со стеками TCP/IP и ZigBee представлена на рис. 5.7. Обычно узлы имеют поддержку протокола ICMPv6 и UDP. Прикладные протоколы чаще всего используют бинарный формат данных при работе по UDP-протоколу в сетях 6LoWPAN. В отличие от TCP/IP-стека, в 6LoWPAN нет поддержки протокола транспортного уровня TCP – из-за больших накладных расходов на формирование пакетов и из-за особенностей работы протокола, которые существенно затрудняют его применение в сенсорных беспроводных сетях (подтверждение пакетов и установление/разрыв соединения требуют частой работы приемопередатчика узла, и, как следствие, повышенного потребления энергии).

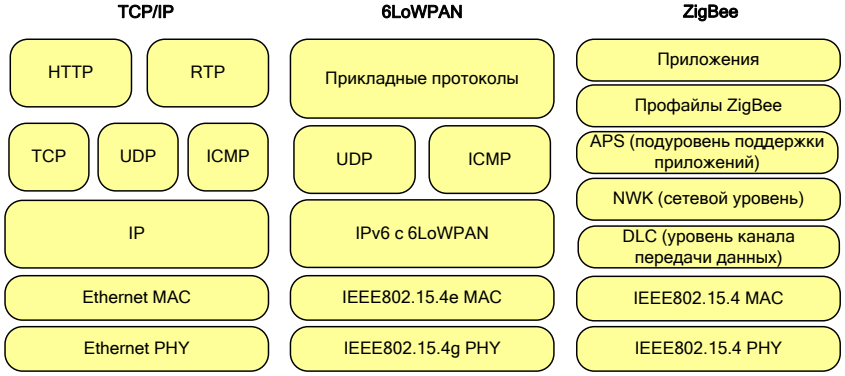


Рис. 5.7 - Сравнение стеков протоколов TCP/IP, 6LoWAPN и ZigBee

Так же как и сети ZigBee, сети 6LoWPAN являются самоорганизующимися. Для этого используется стандартная техника сетей IPv6. На базе заданных параметров стека автоматически устанавливается оптимальная топология связей между узлами в сети. Оптимальные маршруты определяются на основе метрик.

В отличие от стандартов ZigBee, 6LoWPAN расширяет стандартизацию до уровня прикладных задач, параллельно решая проблемы с интеграцией небольших беспроводных узлов в IP-сети.

Целевые приложения стека 6LoWPAN включают в себя достаточно большие масштабируемые сети с подключением к IP-сетям (интернет, интранет или экстранет). Несмотря на хорошую масштабируемость, потенциально прозрачное управление и легкий

доступ к узлам, 6LoWPAN подходит не для всех применений. В частности, текущая версия стандарта стека протоколов требует постоянной активности маршрутизаторов для корректной передачи данных, что затруднительно в сенсорных беспроводных сетях. Тем не менее, эта особенность позволяет минимизировать занимаемый стеком 6LoWPAN объем flash-памяти в конечном устройстве и, следовательно, минимизировать стоимость сетевого процессора.

Основные области применения стандарта 6LoWPAN:

−интеллектуальные системы учета;

−управление уличным освещением;

−промышленная автоматика;

−логистические системы, отслеживание товаров или объектов инвентаризации;

−коммерческие охранные системы, системы контроля и управления доступом;

−некоторые военные приложения.

Некоторые области применений 6LoWPAN перекликаются с рядом стандартов ZigBee, однако в данном случае конкуренция отсутствует, скорее – взаимодействие и дополнение друг друга, особенно в плане интеграции сервисов, расширения зон действия сети. Характеристики технологии 6LoWPAN представлены в табл. 5.3.

Таблица 5.3 –Характеристики технологии 6LoWPAN

Параметр	**Значение**
Адресация	16- и 64-бит MAC, 128-бит адрес IPv6
Требования к реализации стека протоколов	~24 кбайт ПЗУ; ~3,6 кбайт ОЗУ

5.5 Стандарты WirelessHART и ISA100.11a

Стандарты промышленных беспроводных сетей WirelessHART (IEC 62591) и ISA100.11a, как и рассмотренные ранее технологии ZigBee и 6LoWPAN, являются надстройками над физическим уровнем стандарта IEEE 802.15.4. Оба стандарта имеют общий принцип работы и конкурируют между собой. Конвергенцию WirelessHART и ISA100.11a планировалось осуществить в едином стандарте ISA100.12, однако после пяти лет работы в конце 2012 года работа над новым стандартом в рамках Международной ассоциации автоматизации (ISA) была прекращена, так как не удалось решить вопрос о совместимости этих стандартов для беспроводных сетей промышленной автоматики.

WirelessHART – протокол передачи данных по беспроводной линии связи, разработанный фондом HART Communication Foundation для передачи данных в виде HART-сообщений в беспроводной среде. Исходный протокол обмена данными HART в проводных сетях был предназначен для взаимодействия с полевыми датчиками на основе расширяемого набора простых команд «запрос-ответ», передаваемых в цифровом виде по двухпроводной линии с током 4-20 мА (рис. 5.8). Его беспроводный вариант WirelessHART обеспечивает передачу данных со скоростью до 250 кбит/с на расстояние до 200 м (в пределах прямой видимости) при частоте передачи данных в диапазоне 2.4 ГГц. WirelessHART одобрен международной электротехнической комиссией (МЭК) в качестве первого международного стандарта беспроводной связи промышленной автоматизации под номером IEC 62591.

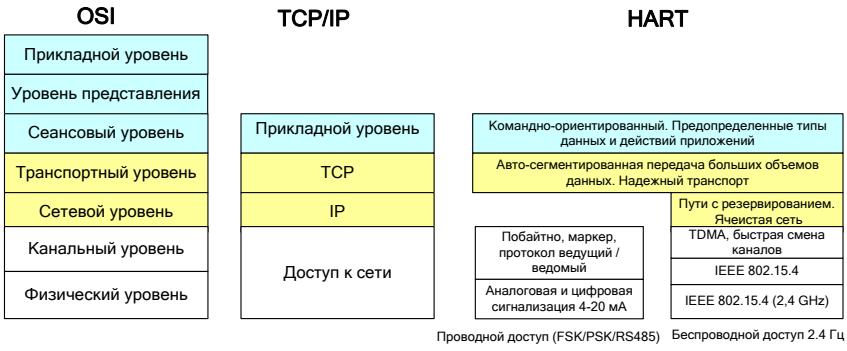


Рис. 5.8 - Сравнение стеков протоколов OSI, TCP/IP и HART

Беспроводная сеть WirelessHART состоит из трех основных элементов (рис. 5.9):

1. Беспроводные полевые устройства, подсоединенные к промышленному оборудованию. Это может быть устройство со встроенной проводной технологией WirelessHART или уже имеющееся установленное проводное HART-устройство с адаптером WirelessHART.

2. *Шлюзы* – обеспечивают обмен данными между полевыми устройствами и хост-приложениями, подсоединенными к высокоскоростной магистральной или другой имеющейся на предприятии коммуникационной сети.

3. *Администратор сети/менеджер безопасности* – отвечает за конфигурирование сети, планирование обмена данными между устройствами, маршрутизацию сообщений и мониторинг состояния сети. Администратор сети может быть встроен в шлюз, хост-приложение или контроллер автоматизации технологического процесса.

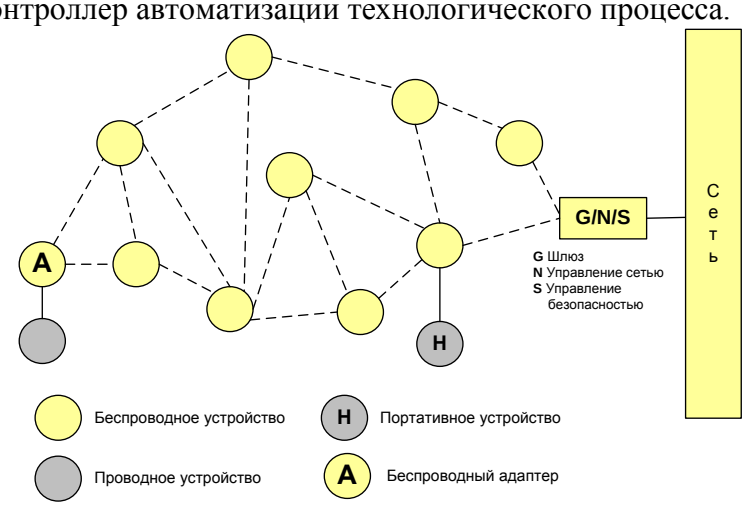


Рис. 5.9 – Архитектура сети WirelessHART

Сеть WirelessHART основана на совместимых с IEEE 802.15.4 радиопередатчиках, работающих в ISM диапазоне 2,4 ГГц. В них используется технология широкополосного сигнала с прямой последовательностью и переключением каналов для обеспечения коммуникационной безопасности и надежности, а также технология синхронизированного многостанционного доступа с временным разделением каналов (TDMA) и контролируемой задержкой для связи между устройствами в сети.

Каждое устройство в сети может служить в качестве маршрутизатора для сообщений от других устройств. Иными словами, устройство не имеет необходимости обращаться напрямую к шлюзу; оно просто передает свое сообщение на ближайшее соседнее устройство. Это расширяет масштаб сети и обеспечивает избыточные каналы передачи данных для повышения надежности.

Администратор сети определяет избыточные каналы на основе времени задержки, эффективности и надежности передачи. Чтобы обеспечить открытость и свободность избыточных каналов, передача сообщений попеременно осуществляется по каждому из них.

Схема сети WirelessHART также позволяет легко добавлять и перемещать устройства. Устройство всегда остается на связи, когда оно находится в зоне действия других устройств в сети.

Для обеспечения гибкости при разных условиях применения стандарт WirelessHART поддерживает несколько режимов передачи данных, включая однонаправленную публикацию значений параметров технологического процесса и управления, мгновенное уведомление по исключению, специальный запрос/отклик и передача больших наборов данных с автоматическим сегментированием. Эти возможности позволяют настраивать передачу данных в соответствии с производственными требованиями, что снижает энергопотребление и непроизводительные издержки.

ISA100.11a – стандарт организации промышленных сенсорных сетей, сетей датчиков и приводов. Стандарт разработан Международным обществом по автоматике ISA (International Society of Automation) и одобрен МЭК в качестве общедоступной спецификации. В настоящее время идет процесс одобрения спецификации в качестве стандарта. Для передачи промышленных данных используется низкоскоростная беспроводная связь с использованием элементов с низким энергопотреблением. Обмен данными осуществляется на частоте в районе 2,4 ГГц и скорости порядка 250 кбит/с. В основе архитектуры ISA100.11a, как и в протоколе WirelessHART, лежит стандарт IEEE 802.15.4-2006 (рис. 5.10).

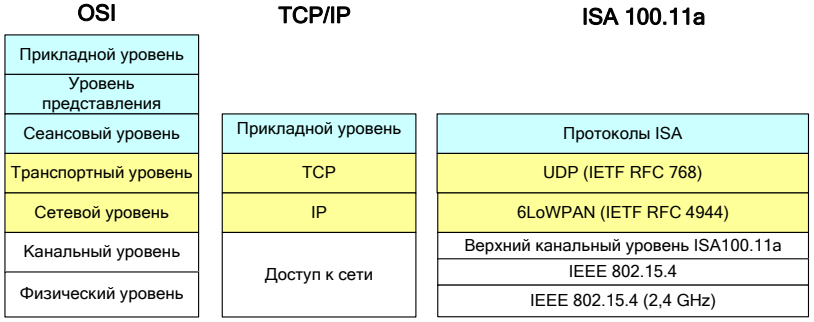


Рис. 5.10 - Сравнение стеков протоколов OSI, TCP/IP и ISA100.11a

Беспроводная сеть стандарта ISA100.11a содержит следующие компоненты (рис. 5.11):

- полевое устройство с функцией маршрутизатора;
- полевое устройство без функции маршрутизатора;
- магистральный маршрутизатор;
- шлюз;
- системный менеджер;
- менеджер безопасности.

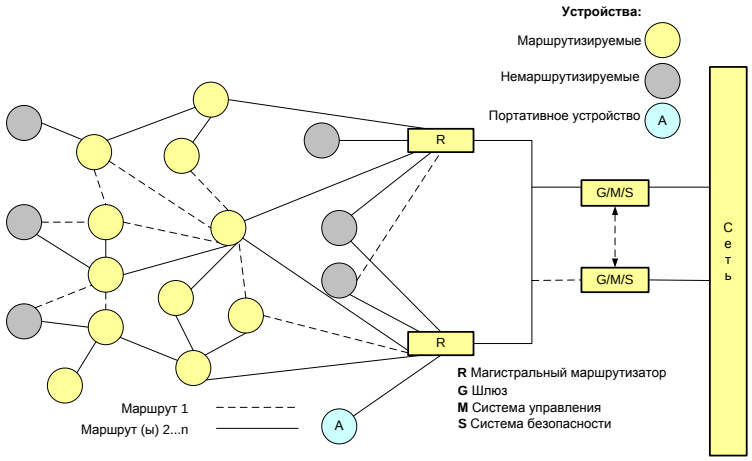


Рис. 5.11 - Архитектура беспроводной сети по стандарту SP100.11a

ISA100.11a поддерживает протоколы Fieldbus Foundation, Profibus-PA и HART, работающие на уровне приложений. Фактически, он способен поддерживать несколько кластеров устройств, работающих с указанными протоколами. Он также может поддерживать различные типы датчиков (HART, Profibus и др.) в одном кластере.

Стандарт ISA100.11a использует топологию сетей датчиков типа «ячеистая сеть» или «звезда». Сети с топологией типа «ячеистая сеть», выполняющие множество переключений, используют больше заряда батарей, чем сети с топологией типа «звезда», но являются более безопасными. Таким образом, у пользователя есть выбор и он может отдать предпочтение тому или иному способу построения сетей, в зависимости от решаемых задач.

Протоколы WirelessHART и ISA100.11a имеют много общего, т.к. за основу взят стандарт IEEE 802.15.4-2006. С целью повышения надежности беспроводных систем для предприятий в обоих случаях на физическом уровне используется технология псевдослучайной перестройки рабочей частоты FHSS (Frequency Hopping Spread Spectrum), а на канальном уровне метод кодового разделения CDMA заменен на метод временного разделения TDMA (рис. 5.12).

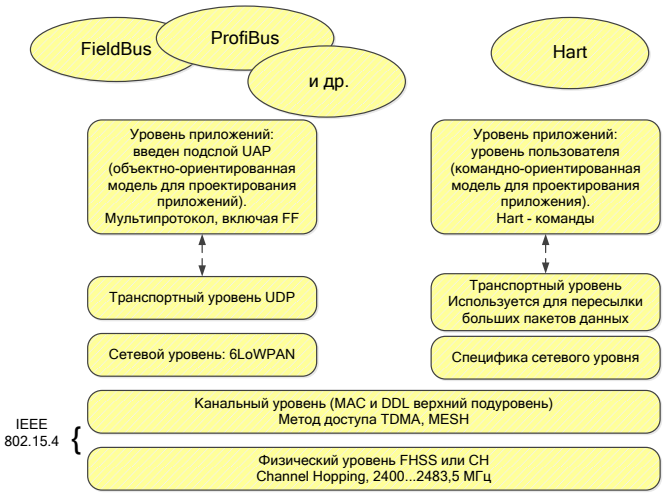


Рис. 5.12 – Сравнение стеков протоколов стандартов ISA 100.11a и WirelessHart

Оба стандарта в последних версиях поддерживают язык описания электронных устройств EDDL (Electronic Device Description Language) для обеспечения совместимости полевых устройств от разных производителей.

Однако имеются и существенные отличия между этими протоколами (см. рис. 5.12 и табл. 5.4). В ISA 100.11a используется сетевой уровень модели OSI на базе протокола 6 LoWPAN (RFC4944), т.е. предусмотрена 128-битная IPv6-адресация полевых устройств, которая в основном применяется на сетевом уровне магистральных маршрутизаторов или шлюзов. Внутри беспроводной сети ISA 100.11a используется укороченный – 16-битовый адрес EUI (без инкапсуляции и компрессии IP-заголовка в рамках одной беспроводной сети и с инкапсуляцией и компрессией IP-заголовка при наличии двух или более беспроводных сетей). В то же время внутри беспроводной сети WirelessHart вообще отсутствует IP-адресация оконечных устройств. Укороченная EUI-адресация и маршрутизация полевого беспроводного оборудования осуществляется на сетевом уровне в рамках одной беспроводной сети (не предусмотрена масштабируемость сетей).

Таблица 5.4 - Основные отличия стандартов Wireless Hart и ISA100.11a

Стандарт Wireless Hart	**Стандарт ISA100.11a**
Управление осуществляется по командам протокола Hart	Универсальность управления независимо от протоколов полевых шин
Локальная беспроводная сеть, ячеистая (mesh) топология, полевые устройства с функцией маршрутизатора, топология «сеть», MAC-адресация	Множество локальных беспроводных сетей, полевые устройства с функцией маршрутизатора и с ограниченными возможностями, топология «ячеистая сеть» и «звезда», IP-адресация
Простая архитектура построения беспроводной сети, подключение к полевой шине через один шлюз	Масштабируемость в рамках предприятия и крупных производственных комплексов, подключение к полевой шине через магистральные шлюзы

На прикладном уровне модели OSI в ISA100.11a для проектирования приложений используется концепция объектно-ориентированной модели, а Wireless Hart – командно-ориентированная. В ISA100.11a на прикладном уровне хоста введен дополнительный подслой для управления UAP и между UAP, который по стандарту ISA для полевых шин IEC 61158 рассматривается отдельно от модели OSI. В Wireless Hart такое понятие отсутствует.

ISA100.11a представляет собой полноценный и перспективный стандарт с технологической точки зрения. Он основан на открытых стандартах, а не собственных технологиях. Например, он поддерживает протокол IPv6 комитета IETF в беспроводных персональных сетях низкой мощности (6LoWPAN). Адресация устройств IPv6 позволяет использовать тысячи датчиков и упростить их подключение при переходе к интернету вещей.

Хотя беспроводная система ISA100.11a полностью устраняет необходимость использования WirelessHART, на данный момент более 15-ти производителей поддерживают стандарт WirelessHART (IEC 62591), тогда как поддержка стандарта ISA100.11a ограничена

всего тремя производителями. Следует также отметить, что более дешевая технология ZigBee применима для домашней и офисной автоматизации, в то время как дорогостоящие технологии WirelessHART и ISA 100.11a предназначены для сетей промышленной автоматики.

5.6 Стандарт Z-Wave

Z-Wave – это первый открытый беспроводный стандарт домашней автоматизации (системы «умный» дом), в основе которой лежит ячеистая (mesh) сеть. Он основан на спецификации ITU G.9959 и определяет все аспекты взаимодействия устройств, поддерживающих этот протокол, а также обеспечивает их совместимость. Технология использует маломощные и миниатюрные радиочастотные модули, которые встраиваются в бытовую электронику и различные системы, такие как освещение, отопление, контроль доступа, развлекательные системы и бытовую технику. Стек протокола Z-Wave представлен на рис. 5.13.

Рис. 5.13 - Стек протокола Z-Wave

В отличие от Wi-Fi и других стандартов передачи данных IEEE 802.11, предназначенных в основном для больших потоков информации, стандарт Z-Wave работает в диапазоне частот до 1 ГГц и оптимизирован для передачи простых управляющих команд (например, включить/выключить, изменить громкость, яркость и т.д.). Выбор низкого радиочастотного диапазона для Z-Wave обуславливается малым количеством потенциальных источников помех (в отличие от загруженного диапазона 2,4 ГГц, в котором приходится прибегать к мероприятиям, уменьшающим возможные помехи от работающих различных бытовых беспроводных устройств – Wi-Fi, ZigBee, Bluetooth). В России используется частотный диапазон 869 МГц.

Также другими преимуществами стандарта можно отметить малое потребление энергии, низкую стоимость производства и встраивания модулей Z-Wave в различные бытовые устройства.

Скорость передачи данных в сети составляет 9,6 кбит/с или 40 кбит/с с полной совместимостью. Используется модуляция GFSK. Радиус действия приблизительно 30 метров в условиях прямой видимости, в помещении уменьшается в зависимости от формы и материала стен, а также от вида антенны.

В сети Z-Wave узлы делятся на три типа: контроллеры (Controllers), маршрутизирующие исполнительные механизмы (Routing Slaves) и исполнительные механизмы (Slaves). В реальной сети все типы устройств могут работать в любой комбинации.

Z-Wave использует ячеистую топологию сети с маршрутизацией сообщений от источника (англ. source routing) и имеет один основной контроллер и ноль или более вторичных контроллеров, которые управляют маршрутизацией и безопасностью. В ячеистой сети Z-Wave каждый узел или устройство может принимать и передавать управляющие

сигналы другим устройствам сети, используя промежуточные соседние узлы. Это самоорганизующаяся сеть с маршрутизацией, зависимой от внешних факторов – например, при возникновении преграды между двумя ближайшими узлами сети, сигнал пойдет через другие узлы сети, находящиеся в радиусе действия.

Таким образом, Z-Wave сеть может иметь радиус передачи гораздо больший, чем дальность передачи одного узла. Однако из-за переприемов (hops) может быть получена небольшая задержка между командой управления и желаемым результатом. Для того чтобы Z-Wave устройства имели возможность маршрутизировать данные ими не запрашиваемые, они не могут находиться в спящем режиме. Таким образом, устройства с питанием от батареек не предназначены в качестве устройств ретрансляции. Сеть Z-Wave может включать до 232 устройств с возможностью расширения сети, если требуется еще несколько устройств. Дополнительные устройства в сеть могут быть добавлены в любое время, так же как и несколько управляющих контроллеров.

Хотя технология Z-Wave является простым и дешевым решением, низкая скорость передачи данных исключает передачу изображений, звука и высокоскоростных данных. Кроме того, для решений, где требуется более 30 устройств, Z-Wave-система является более дорогой, чем кабельные системы. Из-за своих конструктивных особенностей, такие системы имеют ограниченные масштабы и радиус действия, и требуют использования повторителей или даже кабельные соединения. В мире насчитывается более 200 производителей, предлагающих товары с Z-Wave чипами или модулями. Отличительной особенностью Z-Wave является то, что все эти продукты совместимы между собой. Сравнение стека протокола Z-Wave в с другими технологиями приведено на рис. 5.14. Характеристики технологии Z-Wave представлены в табл. 5.5.

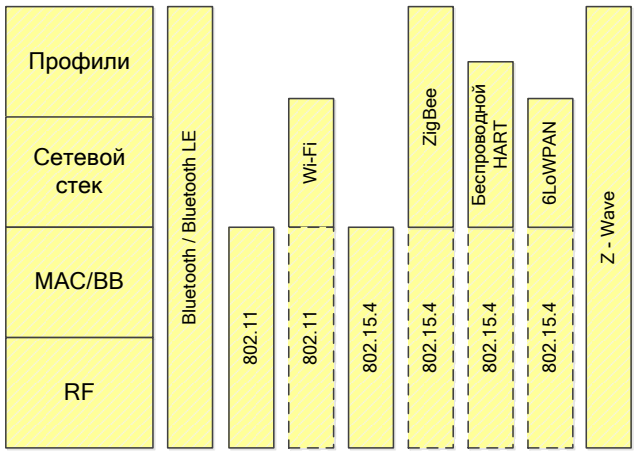


Рис. 5.14 – Сравнение стека протокола Z-Wave в с другими технологиями

Таблица 5.5 –Характеристики технологии Z-Wave

Параметр	**Значение**
Частотный диапазон, МГц	868/908, 2400
Битовая скорость, кбит/с	9.6/40, 200
Тип модуляции сигнала	BPSK
Чувствительность приемника, дБм	-101
Выходная мощность передатчика, дБм	-20...0
Размер данных пакета, байт	До 64
Адресация	32-бит -

	идентификатор дома; 8-бит - адрес узла
Типовые требования к реализации стека протоколов	32...64 кбайт ПЗУ; 2...16 кбайт ОЗУ

5.7 Стандарт Bluetooth Low Energy

Технология Bluetooth Low Energy (BLE) – Bluetooth 4.0 является технологией беспроводной связи для ближних коммуникаций, разработанной группой Bluetooth Special Interest Group (SIG). В отличие от предыдущих стандартов – Bluetooth 2.0, Bluetooth 2.1 + EDR, Bluetooth 3.0, стандарт BLE изначально ориентирован на применение в системах сбора данных, мониторинга с автономным питанием. BLE потребляет в 10-20 раз меньше энергии и способен передавать данные в 50 раз быстрее, чем классические Bluetooth-решения.

В отличие от технологий сенсорных сетей, таких как, ZigBee, 6LoWPAN или Z-Wave, ориентированных на разветвленные распределенные сети с многочисленными передачами данных между узлами сети, стандарт Bluetooth Low Energy рассчитан на топологии типа «точка-точка» и «звезда». Основными областями применения BLE являются устройства обеспечения безопасности, управления электроприборами и отображения показаний, датчики с батарейным питанием, домашние медицинские приборы, спортивные тренажеры.

Устройства BLE работают в диапазоне 2,4 ГГц. В стандарте определено 40 частотных каналов с расстоянием в 2 МГц между каналами. На физическом уровне применена GFSK-модуляция (Gaussian Frequency Shift Keying) с индексом модуляции в пределах от 0,45 до 0,55, что позволяет уменьшить пиковое потребление энергии. Скорость передачи на физическом уровне 1 Мбит/с. В стандарте BLE чувствительность приемника определена как уровень сигнала на приемнике, при котором частота битовых ошибок BER (Bit Error Rate) достигает уровня 10^{-3}. Она должна составлять -70 дБм или лучше.

Технология адаптивной скачкообразной перестройки частоты, используемая в BLE, позволяет устройствам быстро изменять рабочую частоту в широком диапазоне рабочих частот. Это не только позволяет снизить интерференцию, но и уменьшить или полностью избежать переполнения в рабочем частотном диапазоне. Наряду с широковещательным режимом, BLE предлагает способ передачи данных, ориентированный на установленное между отдельными устройствами соединение.

Как и классический стек протоколов Bluetooth, стек BLE состоит из двух основных частей: контроллера (controller) и узла сети (host) (рис. 5.15). Контроллер включает в себя физический и канальный уровень и часто реализуется в виде системы-на-кристалле с интегрированным беспроводным трансивером. Часть стека, именуемая узлом сети, реализуется программно на микроконтроллере приложений и включает в себя функциональность верхних уровней (рис. 5.15): протокол адаптации L2CAP (Logical Link Control and Adaptation Protocol), протокол атрибутов ATT (Attribute Protocol), протокол атрибутов профилей устройств GATT (Generic Attribute Profile), протокол обеспечения безопасности SMP (Security Manager Protocol), протокол обеспечения доступа к функциям профиля устройств GAP (Generic Access Profile). Взаимодействие между верхней и нижней частями стека осуществляется через интерфейс HCI (Host Controller Interface). Дополнительная функциональность прикладного уровня может быть реализована поверх уровня узла сети.

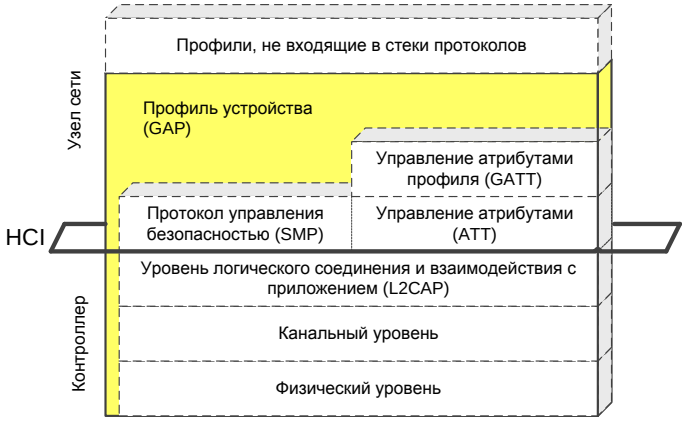


Рис. 5.15 - Структура стека протоколов Bluetooth Low Energy

Несмотря на то, что некоторые функции контроллера BLE заимствованы у классического Bluetooth, они не совместимы между собой, т.е. устройство, поддерживающее только BLE (однорежимное устройство – single-mode device) не сможет взаимодействовать с устройством, поддерживающим только Bluetooth версий 2.x/3.0. Для осуществления взаимодействия между ними хотя бы одно из устройств должно поддерживать оба стека протоколов (двухрежимное устройство - dual-mode device). Однорежимные устройства обладают наименьшим энергопотреблением и в основном представляют собой конечные исполнительные устройства. Двухрежимные устройства предполагают возможность периодического получения энергии, располагаются на различных мобильных устройствах, а также могут функционировать и как обычные Bluetooth-устройства. Характеристики BLE и Bluetooth приведены в табл. 5.6.

Таблица 5.6 – Характеристики технологий BLE и Bluetooth

Параметр	**BLE**	**Bluetooth**
Частотный диапазон, МГц	2400	2400
Битовая скорость, кбит/с	1000	<721 (v1.2), 3000(v2+EDR), <24000(v3+HS)
Тип модуляции сигнала	GFSK	GFSK(v1.2), GFSK/4-DQPSK/8DPSK (v2+EDR), 802.11 (v3+HS)
Метод расширения спектра	FHSS (ширина канала 2 МГц)	FHSS (ширина канала 1 МГц)
Чувствительность приемника, дБм	<-70 -87...93	-90
Выходная мощность передатчика, дБм	-20...10	20/4/0 (класс 1/2/3)
Размер данных пакета, байт	От 8 до 47	До 358
Адресация	48-бит открытый адрес Bluetooth или случайный	48-бит открытый адрес Bluetooth

	адрес	
Требования к реализации стека протоколов	~40 кбайт ПЗУ; ~2,5 кбайт ОЗУ	~100 кбайт ПЗУ; ~30 кбайт ОЗУ

Безусловно, большая часть областей применения Bluetooth может быть успешно заменена или дополнена устройствами BLE, что продлит срок службы устройств за счет более эффективного управления энергопотреблением. В частности, возможно применение двухрежимных устройств BLE в мобильных телефонах, планшетных компьютерах, ноутбуках. Однорежимные устройства могут применяться в качестве беспроводного интерфейса датчиков с батарейным питанием, применяющихся как отдельно, так и в составе других устройств - в часах, пульсометрах, шагомерах, домашних тонометрах, термометрах и тому подобных устройств. В составе мобильных устройств BLE может быть использован для управления домашней автоматикой, устройствами освещения или охраны, как минимум, в пределах одного помещения. Для управления устройствами в пределах всего дома возможно использование BLE в качестве шлюза между управляющим устройством и сетью домашней автоматики.

Низкое энергопотребление и более устойчивая работа в условиях большого количества аналогичных устройств в ряде случаев позволяет рассматривать BLE как альтернативу устройствам NFC, в частности RFID-меткам. Но более интересен вариант использования BLE совместно с NFC. В этом случае первые обеспечивают больший радиус устойчивой работы и большое количество совместно работающих устройств, а вторые служат для установления логического соединения между парой устройств, обеспечивая более высокий уровень безопасности за счет меньшего радиуса действия.

5.8 Семейство стандартов IEEE 802.11

IEEE 802.11 – набор стандартов связи для реализации беспроводных локальных сетей в различных частотных диапазонах. Пользователям более известен по названию Wi-Fi (от английского словосочетания Wireless Fidelity, которое можно дословно перевести как «высокая точность беспроводной передачи данных»), являющемуся торговой маркой объединения Wi-Fi Alliance. Wi-Fi – один из самых популярных групп стандартов и повсеместно используется для организации домашних и офисных сетей, публичного доступа к Интернету в гостиницах, кафе, магазинах и в других публичных местах. Получил широкое распространение благодаря использованию в мобильных устройствах, КПК и ноутбуках.

Стек протоколов стандарта IEEE 802.11 соответствует общей структуре стандартов комитета 802, то есть состоит из физического уровня и канального уровня с подуровнями управления доступом к среде MAC (Media Access Control) и логической передачи данных LLC (Logical Link Control). Как и у всех технологий семейства 802, технология 802.11 определяется двумя нижними уровнями, то есть физическим уровнем и уровнем MAC, а уровень LLC выполняет свои стандартные общие для всех технологий LAN функции. Структура стека протоколов IEEE 802.11 показана на рис. 5.16.

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.

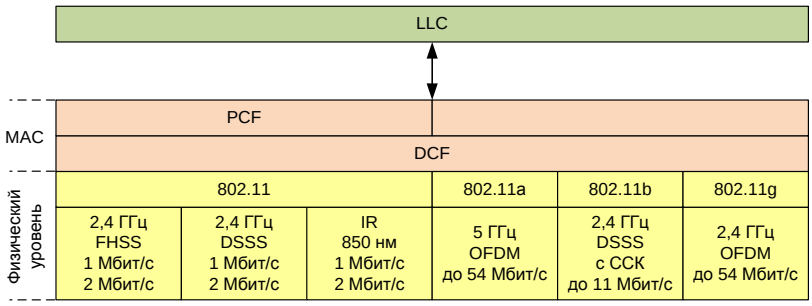


Рис. 5.16 - Стек протоколов IEEE 802.11

Уровень MAC выполняет в беспроводных сетях больше функций, чем в проводных. 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.

В сетях 802.11 уровень MAC поддерживает два режима доступа к разделяемой среде: распределенный режим DCF (Distributed Coordination Function) и централизованный режим PCF (Point Coordination Function). Режим PCF применяется в тех случаях, когда необходимо приоритезировать чувствительный к задержкам трафик.

Изначально стандарт IEEE 802.11 предполагал возможность передачи данных по радиоканалу на скорости не более 1 Мбит/с и опционально на скорости 2 Мбит/с. Один из первых высокоскоростных стандартов беспроводных сетей IEEE 802.11b использует кодирование с помощью комплементарных кодов CCK (Complementary Code Keying). Стандарт предусматривает использование нелицензируемого диапазона частот 2,4 ГГц, скорость передачи до 11 Мбит/с.

Стандарт EEE 802.11a обеспечивает суммарную скорость передачи уже до 54 Мбит/с. Рабочий диапазон стандарта – 5 ГГц. Используется мультиплексирование с ортогональным частотным разделением каналов OFDM (Orthogonal frequency-division multiplexing).

Стандарт IEEE 802.11g предусматривает использование диапазона частот 2,4 ГГц, обеспечивая скорость соединения до 54 Мбит/с. Кроме того, он гарантирует обратную совместимость со стандартом 802.11b. Обратная совместимость стандарта IEEE 802.11g может быть реализована в режиме модуляции CCK, и тогда скорость соединения будет ограничена 11 Мбит/с либо в режиме модуляции OFDM, при котором скорость может достигать 54 Мбит/с.

Стандарт IEEE 802.11n теоретически способен обеспечить скорость передачи данных до 600 Мбит/с, применяя передачу данных сразу по четырём антеннам. При работе по одной антенне – скорость до 150 Мбит/с. Устройства 802.11n работают в диапазонах 2,4-2,5 или 5,0 ГГц.

Устройства 802.11n могут работать в трёх режимах:

– *наследуемом* (Legacy), в котором обеспечивается поддержка устройств стандартов 802.11b/g и 802.11a;

– *смешанном* (Mixed), в котором поддерживаются устройства 802.11b/g, 802.11a и 802.11n;

– *чистом* – в этом режиме реализуются и повышенная скорость и увеличенная дальность передачи данных, обеспечиваемые устройствами только стандарта 802.11n.

Существует также стандарт IEEE 802.11p – технология, разработанная для беспроводной передачи информации между высокоскоростными транспортными средствами и объектами транспортной инфраструктуры с целью создания интеллектуальной транспортной системы в рамках концепции интернета вещей. Используемый частотный диапазон – 5.9 ГГц (5.85-5.925 ГГц).

С состав стандарта IEEE 802.11 входит также технология IEEE 802.11s , которая позволяет организовать иерархические беспроводные ad-hoc сети с мобильными и статическими узлами (mesh-сети), расширяет функциональность беспроводного доступа в Интернет и позволяет реализовывать точки доступа с охватом на порядок более высоким, чем у привычных хот-спотов.

Кроме этого сейчас разрабатывается стандарт IEEE 802.11ac для беспроводных локальных сетей, работающий на частотах 5-6 ГГц. Максимальная теоретическая пропускная способность в IEEE 802.11ac составляет 6933,3 Мбит/с и обеспечивается при ширине канала 160 МГц и условии использования 8 антенн MU-MIMO (Multi-User Multiple-Input/Multiple-Output), работающих в режиме пространственного мультиплексирования. Это эквивалентно разделению потока данных на несколько пространственных потоков beamforming (от англ. «формирование луча» – технология формирования адаптивной диаграммы направленности антенны) и передачи их одновременно при помощи нескольких антенн. Энергопотребление по сравнению с 802.11n снижено до 6 раз. Реализована обратная совместимость с 802.11a/b/g/n.

Еще один разрабатываемый стандарт IEEE 802.11ad (неофициально называемой WiGig) вообще не придерживается преемственности. Стандарт разрабатывается «с нуля» и предполагает работу в более высоком диапазоне частот – 60 ГГц, что определяет «комнатное» использование таких устройств – в этом диапазоне значительно меньше помех (по сравнению с диапазонами 5 и 2,4 ГГц); отсутствие препятствий на пути сигнала имеет важное значение для обеспечения нормального функционирования, а рабочие дистанции измеряются несколькими метрами (аналогично Bluetooth).

Эти два новых стандарта семейства IEEE 802.11 не являются соперниками друг для друга, занимая разные технологические и рыночные ниши. Если IEEE 802.11ac является очередным шагом на пути развития сетей WLAN, то IEEE 802.11ad, не исключено, сможет в будущем заменить технологию Bluetooth с ее невысокой скоростью передачи данных. IEEE 802.11ad вполне может «вырасти» в так называемый «беспроводный USB» и будет применяться для подключения самых разных периферийных устройств (мониторов, принтеров, дисков). Характеристики различных стандартов IEEE 802.11 приведены в табл. 5.7.

Табл. 5.7 - Характеристики стандартов IEEE 802.11

Стан-дарт IEEE	Диапазон, ГГц	Ширина канала, МГц	Вид модуляции	Антенная технология	Максимальная скорость передачи
801.11b	2,4	20	CCK	-	11 Мбит/с
801.11g	5	20	CCK, OFDM	-	54 Мбит/с
801.11a	2,4	20	OFDM	-	54 Мбит/с
801.11n	2,4; 5	20, 40	OFDM (до 64 QAM)	MIMO, MU-MIMO, до 4 потоков Beamforming	600 Мбит/с
801.11ac	5	40, 80, 160	OFDM (до 256 QAM)	MIMO, до 8 потоков Beamforming	6,93 Гбит/с
801.11ad	60	2160	SC/OFDM	Beamforming	6,76 Гбит/с

5.9 Стандарт DECT ULE

DECT ULE (Digital European Cordless Telecommunications Ultra Low Energy) – беспроводная технология с низким энергопотреблением, которая поддерживает как

традиционную телефонию, так и пакетную передачу данных на низких скоростях. DECT ULE является развитием стандартной технологии беспроводной телефонной связи DECT.

Появление дополнения DECT ULE призвано обеспечить работу различных устройств с низким энергопотреблением и низкой пропускной способностью, таких, как сенсорные устройства, умные счетчики, устройства автоматизации дома и др. DECT ULE перенял многие положительные свойства технологии DECT, добавив к ним новые возможности, включая большую дальность действия, высокую помехоустойчивость, зарезервированный во всем мире диапазон частот, низкую стоимость, низкое энергопотребление, возможность сосуществования с другими технологиями (Wi-Fi, Bluetooth и др.), возможность выхода в другие сети (ТфОП, IP) через стандартизированный протокол, зрелость технологии. Одной из главных особенностей DECT ULE является поддержка протокола IPv6, что позволяет использовать этот стандарт в Интернете вещей.

DECT ULE впервые был утвержден в 2011 г. и в этом же году появились первые продукты. Как и DECT, стандарт DECT ULE работает в диапазоне 1,88-1,90 ГГц (в Европе), поэтому он обладает большей помехоустойчивостью, чем ZigBee, Bluetooth, Wi-Fi, которые работают в диапазоне 2,4 ГГц Используются 10 радиоканалов с шириной 1,728 МГц.. Скорость передачи данных – до 1 Мбит/с. Дальность работы составляет 600 метров на открытом пространстве и около 70 метров внутри помещений. Длительность работы устройств DECT ULE от батареек измеряется годами (от 4 до 10 лет).

Архитектура стека протокола DECT ULE показана на рис. 5.17. Физический уровень работает на частотах 1880-1920 МГц с символьной скоростью 1,152 Мбит/с. Для радио доступа используются технологии FDMA/TDMA/TDD. Сети DECT ULE в основном строятся по топологии звезда с одним управляющим устройством. Уровень доступа к среде MAC поддерживает традиционный стандарт DECT и все связанные с ним возможности по поиску устройств, установлению соединений, безопасности и др. Управление данными на канальном уровне DECT ULE DLC (Data Link Control) обеспечивает мультиплексирование и сегментацию больших пакетов с верхних уровней. Также этот стандарт обеспечивает аутентификацию и шифрование данных, целостность пакетов и их последовательную доставку с наилучшим возможным качеством (best effort).

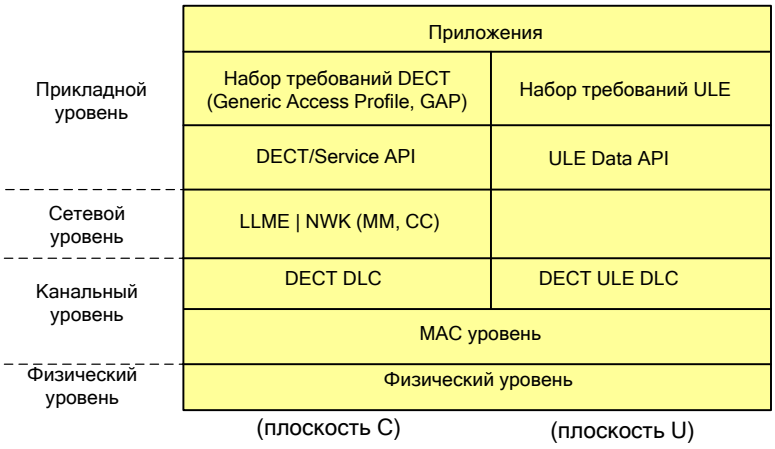


Рис. 5.17 – Стек протоколов DECT ULE

Стек DECT ULE устанавливает постоянный виртуальный канал PVC (permanent virtual circuit) для уровня приложений и обеспечивает поддержку широкого спектра различных протоколов. Одной из возможных технологий для связи между управляющим устройством и терминалом DECT ULE является 6LoWPAN.

Стек DECT ULE может быть разделен на плоскость управления (C-plane) и плоскость пользователя (U-plane). Предполагается, что уровень адаптации ULE 6LoWPAN может работать напрямую на уровне DLC плоскости пользователя.

Прикладной протокол CoAP (Constrained Application Protocol), который представляет собой двоичную версию протокола http, упрощённую под задачи транспортировки данных по линиям с ограниченной пропускной способностью, также может быть использован в DECT ULE сетях с поддержкой протокола IPv6.

5.10 Протокол MQTT

Имеющиеся протоколы для Web-услуг на базе протокола HTTP не отвечают требованиям в контексте услуг IoT и M2M и нуждаются в доработке. Кроме того, требуется разработать новую, более свободно связанную архитектуру межплатформенного ПО, которая позволит преодолеть ограничения таких моделей взаимодействия как SOA, REST, Pub/Sub. Эти проблемы должен решить протокол передачи телеметрических сообщений по очереди MQTT (Message Queuing Telemetry Transport) – лёгкий и простой протокол обмена сообщениями, реализующий модель «публикация/подписка» (publish/subscribe) и предназначенный для связи компьютеризированных устройств, подключённых к локальной или глобальной сети, между собой и различными публичными или приватными веб-сервисами. Его задача – заменить проприетарные технологии, используемые разными компаниями и стать таким же стандартом обмена данными в сети Интернет, как протокол HTTP. Протокол MQTT изначально был создан для датчиков, отслеживающих состояние труб, однако позже сфера его деятельности была расширена и он нашел свое применение во множестве встраиваемых решений, в том числе в смартфонах. Так социальная сеть Facebook применяет этот протокол для обмена сообщениями (Facebook Messenger).

В сети на базе протокола MQTT различают 3 объекта (рис. 5.18):

1) *издатель* (publisher) – MQTT-клиент, который при возникновении определенных событий передает информацию о нем в брокер;

2) *брокер* (broker) – MQTT-сервер, который принимает информацию от издателей и передает ее соответствующим подписчикам, в сложных системах может выполнять также различные операции, связанные с анализом и обработкой поступивших данных;

3) *подписчик* (subscriber) – MQTT-клиент, который после подписки у соответствующего брокера большую часть времени «слушает» его и постоянно готов к приему и обработке входящего сообщения от брокера.

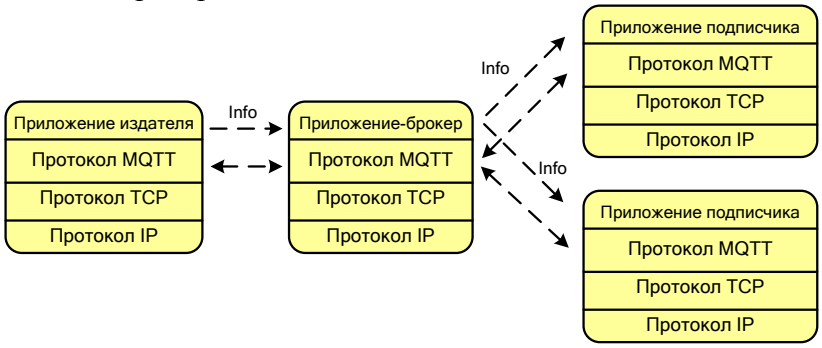


Рис. 5.18 – Сеть на базе протокола MQTT

Спецификация MQTT открыта и доступна в Интернете. В настоящее время есть два варианта спецификации MQTT: MQTT v3.1 - основная спецификация для сетей на базе TCP/IP и MQTT-S v1.2 для датчиков и встраиваемых устройств в сетях, отличных от TCP/IP, например ZigBee.

Пока что неясно, какой радиоспектр будет использоваться для нового протокола, но планируется, что само устройство должно быть достаточно экономичным, энергоэффективным, чтобы работать продолжительное время от заряда аккумулятора. MQTT уже используется в работе спутников, а также в медицине и некоторых промышленных сферах.

Основные преимущества протокола MQTT:

−небольшие накладные расходы на транспортном уровне (заголовок фиксированного размера длиной 2 байт);

−протокол обмена сведен к минимуму для уменьшения сетевого трафика;

− встроенный механизм контроля соединения.

Протокол MQTT имеет ряд достоинств, по сравнению с протоколом HTTP: меньшие накладные расходы на передачу данных и меньшая полоса пропускания (табл. 5.8). Для своей работы он не требует постоянного соединения между клиентом и сервером (как в случае HTTP). MQTT также хорошо адаптирован к работе по каналам связи с низкой пропускной способностью.

Таблица 5.8 - Сравнение характеристик протоколов HTTP и MQTT

Операция	**Протокол**		**Экономия**
	HTTP	**MQTT**	
Чтение одного блока данных с сервера	302 байт	69 байт	в 4 раза меньше
Запись одного блока данных на сервер	320 байт	47 байт	в 7 раз меньше
Чтение 100 блоков данных с сервера	12 600 байт	2445 байт	в 5 раз меньше
Запись 100 блоков данных на сервер	14 100 байт	2126 байт	в 7 раз меньше

Как было указано выше, протокол MQTT обеспечивает обмен сообщениями в режиме «публикация/подписка», который позволяет устройствам посылать и получать данные и сигналы тревог, когда возникает некоторое событие (Event-driven application). В модели с одним издателем и многими подписчиками можно отправлять информацию из одной точки многим другим устройствам или «слушателям», которые заинтересованы в получении информации. Это похоже на концепцию социальной сети, когда один человек размещает информацию, а многие абоненты одновременно просматривают ее. Встраиваемые устройства могут использовать протокол MQTT для сбора данных от нескольких устройств с ограниченной пропускной способностью и предоставления информации многим подписчикам. В результате система является относительно простой для настройки и предоставляет идеальный коммуникационный сетевой протокол для облачных решений в области IoT.

Контрольные вопросы по главе 5

1. Как классифицируются по территории охвата телекоммуникационные сети, используемые в Интернете вещей?
2. Какие беспроводные сети малого радиуса действия используются в IoT?
3. Укажите особенности стандарта IEEE Std 802.15.4.
4. Какие типы узлов сети определены в стандарте IEEE Std 802.15.4?
5. Каково назначение стандарта ZigBee? Укажите его основную особенность.
6. Какие устройства входят в состав сети на базе стандарта ZigBee?
7. Для каких целей был разработан стандарт 6LoWAPN?
8. Сравните стеки протоколов TCP/IP, 6LoWAPN и ZigBee.
9. Что общего и чем отличаются стандарты промышленных беспроводных сетей WirelessHART и ISA100.11a?
10. В чем особенность стандарта Z-Wave?
11. В чем заключается основное отличие стандарта Bluetooth Low Energy (BLE) от других технологий сенсорных сетей?
12. Какие стандарты входят в состав семейства IEEE 802.11? В чем их отличие друг от друга?
13. Для каких целей был создан стандарт DECT ULE?
14. Какие функции реализует протокол MQTT в контексте реализации услуг IoT и M2M?

ГЛАВА 6 ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ IoT

6.1 «Умная планета»

Отдельные масштабные проекты в направлении создания «умной» планеты, своего рода «Интранеты вещей», энергично развиваются в последние годы. Так, Национальное управление США по аэронавтике и исследованию космического пространства (National Aeronautics and Space Administration, NASA) при поддержке компании Cisco создает систему глобального сбора данных о Земле - «Кожу планеты» (Planetary skin). Планируется разработать онлайновую платформу для сбора и анализа данных об экологической ситуации, поступающих от космических, воздушных, морских и наземных датчиков, разбросанных по всей нашей планете. Эти данные станут достоянием широкой общественности, правительств и коммерческих организаций. Они позволят в режиме, близком к реальному времени, измерять, докладывать и проверять экологические данные, своевременно распознавать глобальные климатические изменения и адаптироваться к ним. Разработка платформы началась с серии пилотных проектов, включая проект Rainforest Skin (букв. – «кожа тропических джунглей»), в ходе которого будет исследован процесс уничтожения тропических лесов в мировом масштабе.

В рамках программы Planetary Skin разрабатываются системы поддержки принятия решений, позволяющие эффективно управлять такими природными ресурсами, как биомасса, вода, земля и энергия, климатическими изменениями и связанными с ними рисками (такими как подъем уровня мирового океана, засухи и эпидемии), а также развитием новых экологических рынков, образуемых вокруг углеводородов, воды и биологического разнообразия.

Концепцию «разумной планеты» Smart Planet пропагандирует компания IBM. Суть ее заключалась в том, что благодаря технологиям IoT можно сделать планету разумнее. Сегодня влияние этой идеи уже заметно ощущается по всему миру в различных секторах и отраслях, а также в нашей повседневной жизни. Компании, работающие в сфере энергетики и энергоснабжения, находят лучшие, более эффективные способы выработки и распределения электроэнергии. Города внедряют решения для управления дорожным движением, помогающие обществу сэкономить время и деньги и при этом повысить качество жизни. Компании, производящие потребительские товары, используют интеллектуальные технологии для создания и поставки более качественных продуктов в более короткие сроки и по более низкой цене. Системы здравоохранения используют информацию для уменьшения числа ошибок, сокращения затрат и обеспечения более индивидуализированного обслуживания.

Технологии IoT на базе сенсорных сетей широко используются в экологии, например, отслеживание движения птиц, мелких животных и насекомых, мониторинг состояния окружающей среды с целью выявления ее влияния на сельскохозяйственные культуры и скот, обнаружение лесных пожаров, наводнений, загрязнений и др.

Начинать строить «умную планету» нужно с построения «умных зданий», объединяя их затем в «умные города», и продолжать этот процесс до тех пор, пока «цифровой интеллектуальностью» не будет наделена вся планета. Эти и другие «умные» направления внедрения Интернета вещей рассмотрены далее в главе.

6.2 «Умный город»

В последние годы в городах интенсивно создаются информационные системы для автоматизации отдельных сфер городской жизни: безопасности городской среды, транспорта, энергетики и ЖКХ, здравоохранения, образования, государственного и муниципального управления и др. Принципы и технологии IoT позволяют создать полносвязное интегрированное решение, необходимое для функционирования городской

среды (рис. 6.1) и доступное всем жителям города, сотрудникам городских служб, чиновникам и управленцам разных уровней.

Следует признать, что Интернет вещей пока еще не проник глубоко в элементы городской инфраструктуры и хозяйства, но уже сформировал сферу влияния, в рамках которой играет практически революционную роль. Это в первую очередь транспорт, энергетика и коммунальные услуги, экология, контроль преступности, информационное обеспечение жителей города и интерактивное управление домохозяйством.

Интеллектуальные мобильные устройства и высокоскоростные территориально распределенные сети для доступа к ним, сенсоры, встраиваемые в городскую среду, – все это обеспечивает основу для создания *всеобъемлющих городов* (ubiquitous city), или *и-городов*, в которых объекты инфраструктуры и люди тесно связаны. Правительства нескольких стран уже приняли масштабные программы создания интеллектуальных городов U-City.

Рис. 6.1 - Основные подсистемы «умного города»

Наиболее эффективные U-системы (связанные на основе Интернета вещей) – это коммунальная, транспортная, парковочная службы, а также служба борьбы с уличной и бытовой преступностью. Это, по сути, ключевые проблемы городской жизни, которые можно решить на основе единой системы мониторинга и контроля. Так, в корейском городе Eunpyeong New Town эффективно работает U-система в сфере торговли в виде портала с информацией о магазинах, кафе и т.д., а также система контроля местоположения детей, предназначенная для родителей. С помощью сайта Яндекс.Такси в Москве можно отследить перемещения заказанной машины, обнаружить ближайших водителей на онлайн-карте. Сбор информации от автобусов, оборудованных системой GPS или ГЛОНАСС, позволяет создавать интерактивные табло, онлайн-ресурсы и приложения, которые информируют жителей о том, сколько им придется ждать автобуса. Например, в Москве на Тверской улице установлены пять первых «умных» остановок, оборудованных сенсорными панелями. Теперь пассажиры могут проложить свой путь на интерактивной карте и узнать точное время прибытия автобуса или троллейбуса. В Москве планируется также оснастить парковки интеллектуальной системой, которая позволит автомобилистам получать информацию о свободных парковочных местах в режиме реального времени.

Другой интересный пример — умные мусорные контейнеры. Сигнал о наполнении подается в централизованную систему управления, которая отслеживает на карте все мусороуборочные машины и включает наполненный контейнер в маршрут ближайшего грузовика. И это тоже уже не фантастика: именно так работает мусоросборочная система в Дублине и Барселоне.

Идея использовать в Интернете вещей такую простую, получившую повсеместное распространение технологию, как сотовая связь, находит все большее применение во всем мире. В будущем смартфоны горожан сформируют постоянно расширяющуюся сеть муниципальных датчиков. Сейчас ученые экспериментируют со встраиванием датчиков в сотовые телефоны для решения социальных проблем (например, сбора данных по

загрязнению воздуха или уровню радиации) так, чтобы свести к минимуму или даже нулю необходимость в помощи со стороны горожан.

6.3 «Умный дом»

«Умный дом» предназначен для максимально комфортной жизни людей посредством использования современных высокотехнологичных средств. Принцип работы системы «умный дом» заключается в автоматизации всего, из чего состоит жилая постройка: освещение, кондиционирование, система безопасности, электроэнергия, отопление, водоснабжение и водоотведение и так далее. К основным подсистемам «умного дома» относятся: климат-контроль, освещение, мультимедиа (аудио и видео), охранные системы, связь и другие (рис. 6.2).

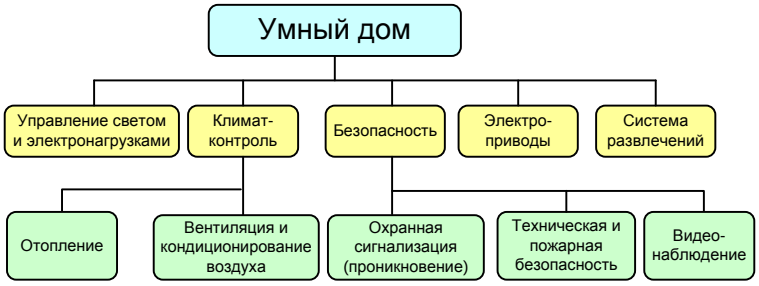


Рис. 6.2 – Основные подсистемы «умного дома»

В стандартном проекте «умного дома» можно выделить три основные подсети: сеть мультимедийных устройств, сеть электроосветительного оборудования и сенсорную сеть. В последнем случае это датчики движения, света, температуры, давления, влажности, вибрации и т.п. Таким образом, «умный дом» состоит из программного и аппаратного обеспечения, датчиков и проводной/беспроводной сети (рис. 6.3).

В общем случае, «умный дом» предоставляет его владельцу следующие преимущества:

1) снижение потребления ресурсов (газ, вода, электроэнергия);
2) высокий уровень комфорта;
3) обеспечение необходимого взаимодействия всех автоматизируемых систем объекта недвижимости, задание различных режимов работы;
4) снижение вероятности возникновения аварийных ситуаций;
5) повышение оперативности, простоты и удобства управления.

Рис. 6.3 – Основные компоненты «умного дома»

Для автоматизации дома смарт-узлы могут быть интегрированы непосредственно в бытовые приборы, например в пылесосы, микроволновые печи, холодильники и телевизоры (их описание приведено ниже). Они могут взаимодействовать друг с другом и с внешней сетью через интернет. Это позволит конечным пользователям легко управлять устройствами дома как локально, так и удаленно.

Большинство бытовых устройств из категории «умных» вещей можно поделить на две группы по типу использования интернета.

К первой группе относится техника, которая через WWW обновляет свое программное обеспечение, получает новые функции, принимает управляющие сигналы от находящегося вдали хозяина, и, соответственно, отправляет ему информацию, подтверждающую выполненные действия и свое состояние. Этот тип использования интернета бытовой техникой является наиболее разумным и способен доказать потенциальному потребителю свою полезность.

Во вторую группу входит техника, в которой интернет является как бы инородным телом. Суть решения в том, что в совершенно привычный бытовой прибор, типа микроволновки или холодильника, встраивается упрощенный компьютер и дисплей, после чего с их помощью можно получать мультимедийные развлечения там, где их раньше не было, например, на той же кухне.

Одним из самых первых примеров бытовой техники, имеющей подключение к Интернету, является обычный тостер, оснащенный интерфейсом для удаленного включения и сообщения о готовности поджаренного тоста. Так техношутка Джона Ромки, одного из первых специалистов в области TCP/IP-протокола, породила в далеком 1988 году технотренд Интернета вещей, который в наши дни воплощается в жизнь. Ниже приведены наиболее характерные примеры «умных» домашних вещей с подключением к интернет.

Интернет-холодильник (Internet refrigerator или *Smart refrigerator)* – новый класс бытовых холодильников, появившийся в начале XXI века. Как правило, он имеет встроенный компьютер с постоянным подключением к сети интернет и сенсорный экран на фронтальной панели (рис. 6.4). Такой холодильник не только хранит продукты, но и даёт возможность пользоваться интернетом, через который можно получить доступ к различным сайтам (например, с кулинарными рецептами для приготовления блюд) и даже заказывать продукты в интернет-магазинах с доставкой на дом. Кроме того, с помощью интернет-холодильника можно общаться, используя электронную и видеопочту. Интернет-холодильник может предоставлять целый ряд сервисов: доступ в Интернет, видеотелефон, e-mail, TV, MP3-музыку, базу данных по кулинарным рецептам и правилам питания, электронное перо, чтобы оставить сообщение, голосовые послания. Ряд моделей интернет-холодильников оборудованы телевизионным и радиоприёмником. Кроме того, при использовании интернет-холодильника появляется возможность вывести на экран картинку от веб-камеры внешнего видеонаблюдения. Это позволяет видеть происходящее во дворе частного дома, даже не покидая кухни, присматривать за своим малышом, находящимся в детской комнате и т.д. Некоторые устройства данного типа также могут следить за содержимым холодильника, выбирая оптимальные условия хранения и заморозки продуктов. Кроме этого, интернет-холодильник отслеживает продукты с истекающим сроком годности. Информация обо всем этом поступает на смартфон пользователя и последний, находясь в магазине, может оценить свои реальные потребности в продуктах.

Рис. 6.4 – Интернет-холодильник Digital Dios Refrigerator компании LG Electronics (фото с сайта smh.com.au).

Робот-пылесос может действовать автономно, программироваться и управляться через Интернет, для чего имеется ряд сенсоров и инфракрасная встроенная камера (рис. 6.5). Система управления работой пылесоса делает несколько снимков в секунду создавая, таким образом, карту всего дома или отдельных его комнат. Устройство также имеет возможность запоминать оптимальный путь уборки и определять своё местонахождение в доме. Аккумулятора хватает на определенное время уборки (обычно до 1,5 часов), по истечении которого робот сам отправляется на подзарядку. К пылесосу имеется беспроводный доступ Wi-Fi с помощью компьютера или смартфона. Через эти устройства можно запустить его и в режиме реального времени наблюдать за тем, что происходит в комнате. Более того, можно поговорить с людьми, которые находятся в доме через систему голосовой связи. Встроенный источник света позволяет видеть в полной темноте и проверить помещение даже ночью.

Рис. 6.5 – Робот-пылесос VC-RL87W компании Samsung (фото с сайта www.samsung.com)

Интернет микроволновая печь (рис. 6.6) имеет встроенный модем для выхода в интернет, память для хранения скачиваемой информации и пульт управления. Она выполняет следующие задачи:

- скачивание рецептов из интернета и самопрограммирование;
- связь с компаниями – производителями продуктов;
- дает доступ к системе заказа продуктов по интернету.

Рис. 6.6 – Микроволновая интернет-печь M-G270IT компании LG Electronics (фото с сайта http://www.compress.ru)

Интернет-кондиционер подключается к интернету по проводной или беспроводной сети WiFi и дает пользователю доступ к управлению кондиционером из любой точки земного шара. Владелец может дистанционно включать и выключать систему, программировать настройки, выбирать режимы, температуру, скорость вентилятора, задавать параметры, словом совершать любые манипуляции, доступные с обычного пульта. Управлять таким кондиционером можно с любого устройства (компьютер, ноутбук, планшет, смартфон), в котором установлена специальная программа и который имеет выход в интернет.

Система по уходу за домашними животными призвана обеспечить им все необходимые комфортные условия существования. Такая система используется в случае длительного отсутствия хозяев дома – это позволяет не беспокоиться о благополучии своих домашних любимцев. Основными задачами системы по уходу за домашними животными являются автоматическая подача еды и питья, а в случае возникновения непредвиденных обстоятельств - информирование хозяев о них (по телефону, с помощью SMS или по электронной почте). По желанию можно составить полный отчет о поведении домашних любимцев во время отсутствия хозяев - сколько раз и когда ели, когда ходили в туалет, пили воду и т.д. Можно даже сопроводить этот отчет фотографиями (если установлена камера слежения) и передавать их (по электронной почте, с помощью MMS) – словом, все, чтобы хозяева чувствовали себя комфортно и были уверены в том, что их любимцам ничего не угрожает.

6.4 «Умная энергия»

В настоящее время наиболее проработанным вариантом применения технологий IoT являются «умные сети» (Smart Grids) в энергетике. Работа такой сети основана на том, что поставщик и потребитель получают объективную картину по использованию энергоресурсов за счет мониторинга на всех участках сети и, как следствие, получают возможность оперативного управления. В случае аварий такие сети способны автоматически идентифицировать проблемные участки и в течение короткого времени направлять электроэнергию по резервным схемам, восстанавливая электроснабжение. Для потребителей «умные» сети означают возможности по гибкому регулированию потребления электроэнергии, как в «ручном», так и в автоматическом режиме.

Управление энергосетью производится с помощью следующих систем (рис. 6.7):

– «умной» маршрутизации энергопотоков (Smart Routing) – системы контроля нагрузки и качества, самовосстановления сетей в результате аварийных событий, хранения энергии и др.;

– «умных» измерений (Smart Metering) – современные интеллектуальные приборы учета (Smart Meter), системы интеллектуального здания (Smart Home), «умные» бытовые приборы.

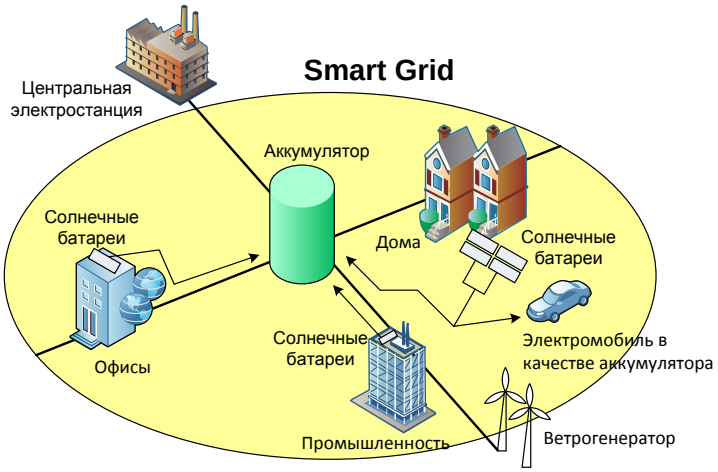


Рис. 6.7 – Схема «умной» сети Smart Grid

«Умный» (или интеллектуальный) счетчик (Smart Meter) – прибор учета энергоресурсов с расширенными возможностями, который позволяет контролировать величину потребленных энергоресурсов и периодически передавать информацию через телекоммуникационную сеть поставщику энергоресурсов или в центр учета и расчетов за жилищные и коммунальные услуги. «Умные» счетчики могут измерять расход электроэнергии, газа, воды, тепла, а также обладать дополнительными возможностями, которые рассматриваются ниже.

«Умный» прибор учета обладает следующими техническими особенностями:

1. Формирует и хранит текущие и архивные значения потребленных энергоресурсов. Объем архивных данных зависит от размера памяти контроллера прибора.

2. Имеет встроенные часы реального времени, которые требуют периодической синхронизации из единого центра.

3. Обладает возможностью взаимодействия с информационной управляющей системой для формирования баланса потребления, учета допуска прибора.

4. Имеет стандартный цифровой интерфейс для обмена данными с автоматизированной системой учета потребления энергоресурсов и (или) телекоммуникационную часть для удаленной передачи данных в центр учета и расчетов.

Основные требования, предъявляемые к «умным» сетям, следующие:

– возможность «самовосстановления» сети после замыканий, физических повреждений и пр.;

– возможность мотивирования потребителей для активного участия в регулировании сети (посредством регулирования собственного потребления);

– высокая устойчивость к вредоносным внешним воздействиям (теракты, диверсии и т.п.);

– возможность предоставления электроэнергии высокого качества (в т.ч. с заданными параметрами) и сокращение потерь;

– интеграция опций производства и хранения электроэнергии;

– высокая эффективность.

Развитие технологий «умных» сетей (Smart Grid) и «умных» счетчиков (Smart Metering) несет в себе перспективу того, что все промышленные и бытовые энергоприемники обретут способность к взаимодействию в информационной сети, станут управляемыми и будут выполнять функции измерения собственного потребления электроэнергии и мощности. Это даст реальный инструмент для энергосбережения и повышения энергоэффективности.

6.5 «Умный транспорт»

Интеллектуальные транспортные системы ITS (Intelligent Transportation System) на базе технологий IoT позволяют осуществлять автоматическое взаимодействие между объектами инфраструктуры и транспортным средством V2I (Vehicle to Infrastructure) или между различными транспортными средствами V2V (Vehicle to Vehicle). Системы V2V осуществляют обмен данными по беспроводной связи между машинами на расстоянии до нескольких сот метров. Системы V2I осуществляют обмен между транспортным средством и центрами управления дорожным движением, операторами дорог и сервисными компаниями. Данные, переданные объектами инфраструктуры, интегрируются в общую систему и передаются близлежащим транспортным средствам. Технологии обеих групп способны значительно увеличить безопасность и эффективность транспорта.

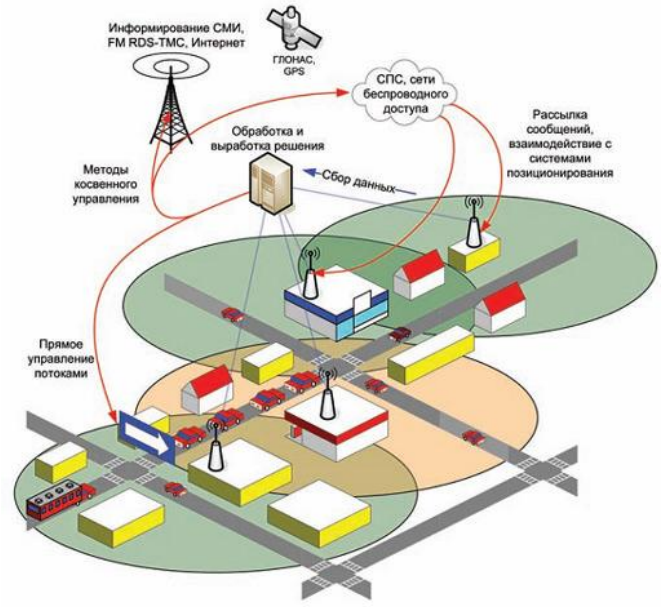


Рис. 6.8 – Система интеллектуального управления транспортом

В качестве примера использования технологий IoT в городах можно привести систему управления автомобильным трафиком (рис. 6.8), которая на основе анализа пропускной способности дорог не только самостоятельно управляет трафиком с помощью перенастройки светофоров, но и постоянно в реальном времени публикует данные о своём состоянии, которые могут быть доступны любым другим устройствам и сервисам, будь-то ГЛОНАСС/GPS-навигатор, мобильный телефон или специализированные веб-сайты. Использование технологии IoT в транспортной сфере позволяет не только отслеживать оповещения о критических ситуациях, но также перенаправлять маршруты движения в режиме реального времени и даже предупреждать пассажиров и водителей об альтернативных маршрутах, транспортных средствах, придорожном жилье и пунктах общественного питания. Кроме того, с помощью установленных на улицах датчиков можно будет обеспечить публикацию информации об их загруженности.

Среди таких «умных» транспортных систем IoT можно упомянуть:

– системы предотвращения столкновений;

– системы «боковой поддержки», указывающие водителю на пересечение дорожных полос или опасные маневры;

– системы ночного видения;

– системы автоматического управления машиной и движения в группах машин;

– системы, контролирующие состояние водителя (в частности, не позволяющие ему заснуть);

– системы превентивного реагирования на аварийную ситуацию (например, системы, осуществляющие предварительное натягивание ремней безопасности перед неизбежным столкновением).

Система информирования водителей при помощи встраиваемых в машины устройств VICS (Vehicle Information and Communication System) собирает информацию через сенсоры, установленные на объектах дорожной инфраструктуры (дорожном полотне, камерах наблюдения и пр.), с использованием «машин-зондов» (мобильных пунктов наблюдения за дорожным движением), а также путем использования уже установленных бортовых систем, позволяющих собирать информацию о скорости движения транспортного потока, погоде и состоянии дорог. Эта информация системой VICS обрабатывается и переводится в цифровой вид, а затем рассылается по бортовым навигационным системам. Пользователи системы могут получать информацию в различных видах - в виде текста, простой графики, карт. Бортовые системы динамически обрабатывают данные и предлагают водителю оптимальный маршрут.

6.6 «Умное производство»

Считается, что изобретение паровой машины в XVIII веке вызвало первую индустриальную революцию. Следующий качественный скачок произошел в промышленности в начале XX века при переходе на конвейерное производство. Затем, с 1960-х годов, процессы на предприятиях начали кардинально меняться благодаря внедрению компьютеров. И вот сейчас мы становимся свидетелями стремительно нарастающей четвертой индустриальной революции, движущей силой которой является Интернет вещей. За счет технологий IoT производственные компании смогут оптимизировать всё - от работы склада до выполнения непосредственно производственных заданий, если каждое промышленное здание, транспортное средство и даже инструмент будут снабжены сенсорами и регулярно будут отправлять отчёт о своём состоянии, местоположении и других характеристиках.

Приведем конкретный пример. Поскольку требования к качеству и безопасности автомобилей неуклонно растут, производители заинтересованы в возможности контролировать работу основных систем и деталей уже выпущенных и проданных машин. Иными словами, автозавод хочет оставаться с ними в контакте, и благодаря Всемирной сети это возможно. В будущем любой автомобиль станет частью Интернета вещей. Машина сможет связываться со своим производителем и, к примеру, сообщать ему, что нуждается в досрочном техобслуживании. Сенсоры в режиме онлайн будут оповещать, к примеру, о перегреве, вибрации, преждевременном износе определенного узла или, скажем, о непривычных звуках.

Подобные интеллектуальные цифровые системы впредь будут устанавливать на любых машинах и станках, но прежде всего на оборудовании таких системообразующих объектов, как, например, электростанции. Каждый узел станка или оборудования будет заниматься самодиагностикой и через интернет сообщать о своем состоянии в соответствующий эксплуатационный центр управления.

Такие решения будут иметь целый ряд преимуществ для самих производителей. Так, компании смогут лучше планировать выпуск и поставку запчастей, они получат возможность отслеживать, насколько часто те или иные узлы сталкиваются с определенными проблемами, и своевременно вносить необходимые инженерно-конструкторские изменения. К тому же они смогут целенаправленно информировать клиента о необходимости заменить тот или иной узел.

Наконец, производители смогут проверять, использует ли клиент качественные фирменные запчасти или прибегает к дешевым подделкам. Проблема эта весьма остро стоит сегодня перед многими компаниями и в целом машиностроительной отраслью, столкнувшейся с потоком контрафактной продукции. Для проверки подлинности запчастей в

оборудование будут, к примеру, встраивать чипы, знающие, где в интернете находится соответствующая документация производителя. При замене деталей они будут проверять «новичков» и сверять полученную информацию с родной базой данных. Таким образом, машиностроительная продукция впредь будет существовать как бы в двух ипостасях. Одна – реальная, «железная», а другая – виртуальная, в виде набора цифровых данных.

Благодаря IoT станет возможным объединение всех контрольно-измерительных приборов и датчиков на каком-либо производстве в единую информационную сеть. Помимо эффективного расходования энергии можно будет даже быстро интегрировать в систему альтернативные источники экологически чистого электричества – например, солнечные батареи и ветряные генераторы. Снижение производственных издержек, эффективный расход энергии, отказ от экономически нерентабельных активов – всё это вместе позволит существенно удешевить производство, а использование возобновляемых источников электричества улучшит экологическую обстановку.

Еще одно современное проявление Интернета вещей – связь между машинами (M2M) с помощью SMS. В Европе эту технологию уже используют в сельском хозяйстве для слежения в реальном времени за перемещениями крупного рогатого скота. Помимо слежения за перемещением скота, фермеры получают автоматические уведомления о состоянии животных. В стойлах и в поле устанавливаются снабженные SIM-картами устройства для связи M2M, а к животным прикрепляются специальные датчики, собирающие информацию и передающие ее на устройство сбора данных. Это устройство немедленно отправляет фермеру нужную информацию с помощью SMS. За данными о состоянии животных можно следить не только через SMS, но и в онлайновом режиме через канал GPRS, связывающий системы мониторинга с центром обработки данных. В Европе таким приложением уже пользуются около 4 тысяч ферм.

6.7 «Умная медицина»

«Умная медицина» на базе Интернета вещей на практике обычно реализуется в виде систем мониторинга здоровья людей с использованием разнообразных биосенсоров и датчиков и систем удаленной медицинской помощи. Возможные применения систем мониторинга на базе сенсорных сетей в медицине:

1. *Мониторинг физиологического состояния человека:* физиологические данные, собранные сенсорными сетями могут храниться в течение длительного периода времени и могут использоваться для медицинского исследования. Установленные узлы сети могут также отслеживать движения пожилых людей, инвалидов и, например, предупреждать падения. Эти узлы невелики и обеспечивают пациенту большую свободу передвижения, в то же время позволяют врачам выявить симптомы болезни заранее. Кроме того, они способствуют обеспечению более комфортной жизни для пациентов в сравнении с лечением в больнице.

2. *Мониторинг врачей и пациентов в больнице:* каждый пациент имеет небольшой и легкий узел сети. Каждый узел имеет свою конкретную задачу. Например, один может следить за сердечным ритмом, в то время как другой снимает показания кровяного давления. Врачи могут также иметь такой узел, он позволит другим врачам найти их в больнице.

3. *Мониторинг медикаментов в больницах:* сенсорные узлы могут быть присоединены к лекарствам, тогда шансы выдачи неправильного лекарства, могут быть сведены к минимуму. Так, пациенты будут иметь узлы, которые определяют их аллергию и необходимые лекарства. Компьютеризированные системы показали, что они могут помочь свести к минимуму побочные эффекты от ошибочной выдачи препаратов.

Одним из этапов совершенствования современной медицины является персонализация данных и повышение коммуникации между врачами. Легкий доступ к истории болезни, позволяет назначать своевременное эффективное лечение. Ведение медицинских карт постепенно может перейти в сеть. «Облачные» решения используются для хранения

больших объемов информации в интернете. Благодаря интернету врачи разных клиник получают доступ к данным пациента. Электронные медицинские карты дают возможность своевременно узнавать о здоровье больного, назначать эффективное лечение. Связывание оборудования медицинского учреждения в единую сеть позволит получать необходимые данные на портативные устройства врачей, на которые поступает информация о пациенте: какие лекарства прописаны, результаты анализов и т.д.

Внедрение интернет-технологий экономит время пациента и врача. Не надо добираться до поликлиники, стоит только включить компьютер и можно связаться с медицинским учреждением. Видеозвонки дают возможность не только произвести опрос, но и сделать общий осмотр, что часто достаточно для общего представление о здоровье человека. Если все-таки необходима встреча с врачом, то записаться на прием можно также через интернет.

Аппараты для измерения давления, весы и другое портативное оборудование оснащается беспроводными передатчиками, которые позволяют данные сразу переносить на компьютер и вести учет за своим здоровьем. Разрабывается «умная одежда», которая собирает данные о состоянии человека: частоту сердечного ритма, температуру тела, частоту дыхания. В такую умную одежду вшиваются еще на стадии разработки чипы, которые не только проводят измерения, но и позволяют передавать данные на мобильный телефон.

6.8 «Умная жизнь»

Уже трудно кого-то удивить доставкой продуктов на дом, но компания Electrolux решила сделать шаг еще дальше, представив свою новую разработку - робота AMMI (рис. 6.9), ходящего за покупками вместо своего владельца. AMMI - это, по сути, корзина для покупок, которая доставит продукты на дом, при этом сохраняя их свежесть с помощью термоэлектрического охлаждения. Хозяину робота нужно только сделать он-лайн заказ в магазине и потом отправить робота, чтобы он его забрал. AMMI оснастили GPS-навигатором, для того, чтобы он мог легко найти дорогу до супермаркета, а также гироскопом для безопасного перемещения по улицам города и системой беспилотного движения.

Рис. 6.9 – Робот AMMI компании Electrolux (фото с сайта www.trendhunter.com)

Компьютеризированная обувь Verb for Shoe («Команда для обуви») компании VectraSense (рис. 6.10) имеет встроенный специализированный микрокомпьютер ThinkShoe (с ультранизким расходом энергии), работающий под управлением специальной операционной системы Magellan и способный постепенно обучаться индивидуальному стилю ходьбы хозяина обуви. ThinkShoe по беспроводной связи может соединяться с карманным (мобильным) компьютером владельца. Скорость обмена данными составляет 1,5 Мбит/с, используемая радиочастота — 2,4 ГГц. Ботинки Verb могут выходить в Интернет и связываться с сервером компании-производителя для точной идентификации неисправностей и обновления собственного программного обеспечения. При встрече на улице разные туфли Verb узнают друг друга и тут же обмениваются по радио визитками хозяев — эту информацию можно посмотреть на домашнем компьютере. Работают ботинки от пары плоских батареек, которых хватает примерно на два месяца.

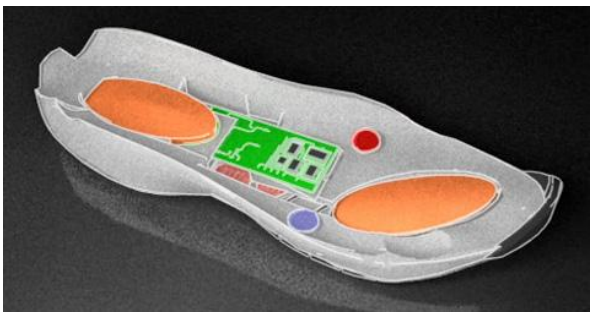


Рис. 6.10 – Компьютер, две воздушные камеры, сенсоры и радиопередатчик – начинка обуви Verb (источник: verbforshoe.com)

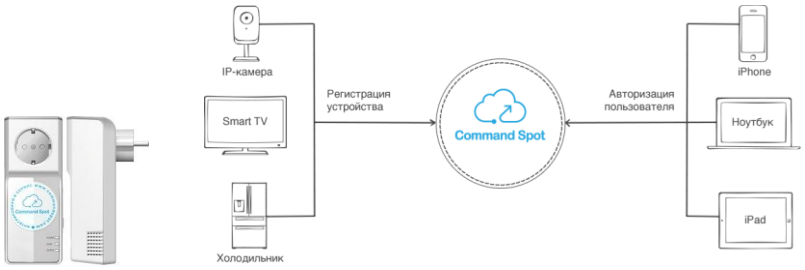
Примером умных устройств являются *очки Google Glass* компании Google (рис. 6.11). В устройстве используется прозрачный дисплей HMD (Head-Mounted Display), который крепится на голову и находится чуть выше правого глаза, и камера, способная записывать видео высокого качества. Взаимодействие Glass с пользователем осуществляется через голосовые команды, жесты, распознаваемые тачпадом, который расположен на дужке за дисплеем, и систему передачи звука с использованием костной проводимости. Концепция Google Glass реализует одновременно три отдельные функции, сведя их воедино: дополненная реальность, мобильная связь + интернет, видеодневник. Такие очки позволяют, надев их, получать информацию, дополняющую увиденное. Например, очки смогут распознать местность и подсказать пользователю, что находится поблизости.

Рис. 6.11 – Очки-компьютер Google Glass

«Умное» зеркало-гаджет Cybertecture Mirror компании James Law Cybertecture (Япония) (рис. 6.12) умеет отражать не только того, кто в данный момент в него смотрится. На поверхности зеркала, как на большом экране, можно увидеть температуру воздуха и календарь, дату и день недели, а еще - гороскоп, рост и вес пользователя, и массу дополнительной информации. Cybertecture Mirror управляется при помощи специального пульта управления, и представляет собой что-то вроде своеобразного компьютера с собственной операционной системой Android, Wi-Fi доступом и стерео-динамиками. Все необходимые настройки и параметры можно выставить в компьютере и получать на зеркало-экран сообщения с электронной почты, новости с rss-подписки, смотреть фотографии и следить за временем. В перспективе хайтек-зеркало сможет обучаться и подстраиваться под каждого члена семьи, выводя персональные напоминания, календарь и прочую информацию индивидуального характера. В будущем система сможет получать указания от семейного доктора, считывать RFID-метки и даже демонстрировать видеоролики.

Рис. 6.12 – «Умное» зеркало Cybertecture Mirror

Для включения или отключения любых бытовых, осветительных или отопительных электроприборов через интернет можно использовать дистанционно управляемую электрическую «умную розетку», включающую в себя GSM-модуль (рис. 9.25). Управление осуществляется с компьютера через интернет-браузер или с мобильных устройств через загружаемое из интернет-магазина облачное приложение.



а) б)

Рис. 6.13 – Управление электроприборами через интернет: а) «умная розетка»; б) схема управления (источник: www.commandspot.com)

Очевидно, что список подобных вещей будет пополняться всё новыми «умными» устройствами и недалек тот день, когда практически все достаточно сложные предметы нашего быта будут иметь такую возможность.

Контрольные вопросы по главе 6

1. Приведите примеры международных проектов в рамках концепции «умная планета».
2. Какие основные подсистемы входят в состав концепции «умный город»?
3. Какие функции выполняют подсистемы «умного дома»?
4. Какие преимущества дает применение на практике концепции «умная энергия»?
5. Приведите примеры реализации «умного производства».
6. Какие функции выполняют системы «умной медицины»?
7. Приведите практические примеры применения технологий IoT в повседневной жизни человека.
8. Предложите возможные перспективные направления внедрения технологий Интернета вещей в различные формы общественной деятельности и личной жизни человека.

ЗАКЛЮЧЕНИЕ

Существующий ныне Интернет людей (Internet of People, IoP) приносит реальную пользу множеству индивидуальных пользователей, компаний и целых стран. Всемирная сеть стимулирует экономический рост путем электронной коммерции и ускоряет инновационные процессы в бизнесе, развивая совместную работу. Интернет помог усовершенствовать систему образования с помощью демократизации методов доступа к информационным ресурсам. Практически вся наша повседневная жизнь (работа, образование, досуг, развлечения и многое другое) уже немыслима без Сети. Но сегодня мы вступаем в эпоху, когда новый Интернет вещей (Internet of Things, IoT) может радикально улучшить жизнь каждого жителя нашей планеты – помочь решению климатических проблем, излечить тяжелые болезни, усовершенствовать процессы ведения бизнеса и сделать каждый день нашей жизни более счастливым. А что же нам ждать в перспективе?

По мнению компании InterDigital современные технологии M2M и IoT фокусируются в основном на двух плоскостях: на коммуникациях (как одна машина передает данные другой) и на контенте (какие данные передаются между машинами). В перспективе же Интернет вещей можно будет охарактеризовать кубической моделью C^6 уже с шестью плоскостями C (рис.1):

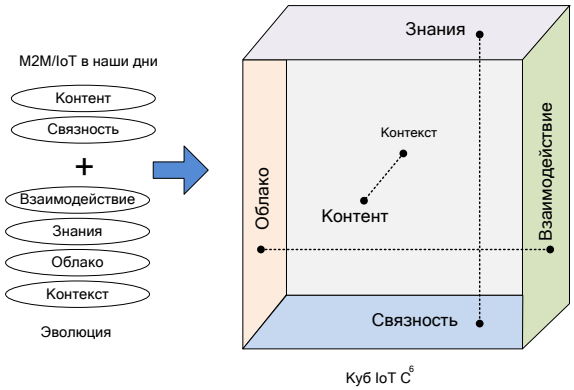


Рис. 1 – Перспективная модель C^6 Интернета вещей (источник: InterDigital)

1) **C**onnectivity – связность мобильных и фиксированных объектов;
2) **C**loud – облачные услуги и хранение контента в облаке;
3) **C**ontext – контекстно-зависимая реализация для повышения производительности;
4) **C**ontent – большие массивы данных, формируемые вещами;
5) **C**ollaboration – совместные коммуникации, объединенные вещи (интер-вещи), совместные сервисы;
6) **C**ognition – знания, полученные из массива данных, позволяющие обеспечить лучшую работу автономной системы.

По прогнозам компании Cisco мы неизбежно перейдем к «Всеохватывающему Интернету» (Internet of Everything, IoE), где всевозможные неодушевленные предметы начнут учитывать контекст и пользоваться более широкими вычислительными ресурсами и сенсорными возможностями. Cisco определяет IoE как соединение людей, процессов, данных и вещей, повышающее ценность сетевых соединений до небывалого уровня (рис. 2). IoE превращает информацию в конкретные действия, создающие новые возможности, расширяющие опыт пользователя и формирующие благоприятные условия для развития стран, компаний и пользователей.

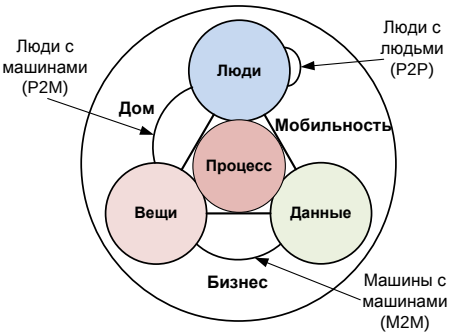


Рис. 2 – Архитектура Всеохватывающего Интернета (источник: Cisco)

Такое определение подчеркивает важный аспект IoE, отличающий его от IoT – так называемый «сетевой эффект». По мере подключения к Интернету все новых предметов, людей и данных мощь Интернета (как сети сетей) растет, согласно закону Мэткалфа, пропорционально квадрату количества пользователей. Это значит, что ценность сети выше арифметической суммы ее компонентов. В силу этого возможности Всеобщего Интернета IoE должны стать поистине безграничными. Ну что ж, поживем – увидим. Хорошо, если так и будет.

СПИСОК СОКРАЩЕНИЙ

3DES (Triple Data Encryption Standard) – тройной симметричный алгоритм шифрования
6LoWPAN (IPv6 over Low power Wireless Personal Area Networks) – стандарт взаимодействия по протоколу IPv6 поверх маломощных беспроводных персональных сетей
AAA (Authentication, Authorization, Accounting) – функции авторизации, аутентификации и расчетов
ACL (Access Control List) – список контроля доступа
AD (Autonomous Domain) – домен автономности
ADC (Analog-to-Digital Converter) – аналого-цифровой преобразователь
AES (Advanced Encryption Standart) – расширенный стандарт шифрования
AMMI (Automated Mobile Marketing Intelligence) – автоматизированная интеллектуальная корзина для покупок
ANSI (American National Standards Institute) – американский национальный институт стандартов
AODV (Ad hoc On-Demand Distance Vector) – протокол динамической маршрутизации для мобильных ad-hoc сетей
API (Application Programming Interface) – интерфейс прикладного программирования
APS (Application Support Sublayer) – подуровень поддержки приложений
ARM (Architectural Reference Model) – архитектурная эталонная модель
ARP (Address Resolution Protocol) – протокол определения адреса
AS (Actuator Sensor) – актуатор сенсора
ASI (Asynchronous Serial Interface) – асинхронный последовательный интерфейс
ASK (Amplitude Shift Keying) – амплитудная манипуляция
ATIS (Automatic Terminal Information Service) – автоматическая информационная служба терминала
ATT (ATtribute Protocol) – протокол атрибутов
ATM (Asynchronous Transfer Mode) – асинхронный режим передачи
BACnet (Building Automation and Control network) – коммуникационный протокол передачи данных для сетей систем автоматизации зданий
BAN (Body Area Network) – сеть беспроводных датчиков на теле человека
BER (Bit Error Rate) – частота битовых ошибок

BLE (Bluetooth low energy) – беспроводная технология Bluetooth с низким энергопотреблением
BOSP (Business Operation Support Platform) – платформа поддержки бизнеса
BPM (Business Process Management) – управление бизнес-процессами
BPSK (Binary Phase–Shift Keying) – двоичная фазовая манипуляция
BRM (Business Rule Management) – система управления бизнес-правилами
BSS (Business Support System) – система поддержки бизнес деятельности
CAN (Controller Area Network) – сеть контроллеров
CASAGRAS (Coordination And Support Action for Global RFID-related Activities) – проект по глобальной стандартизации RFID
CC (Cloud Computing) – облачные вычисления
CCK (Complementary Code Keying) – манипуляция дополнительным кодом
CDF (Computable Document Format) – формат вычисляемых документов
CDMA (Code Division Multiple Access) – множественный доступ с кодовым разделением
CE (Cognitive Element) – когнитивный элемент
CEP (Complex Event Processing) – обработка сложных событий
CIoT (Cognitive Internet of Things) – когнитивный Интернет вещей
CN (Cognitive Node) – когнитивный узел
CoAP (Constrained Application Protocol) – ограниченный прикладной протокол
CORBA (Common Object Request Broker Architecture) – общая архитектура брокера объектных запросов
CR (Cognitive Radio) – когнитивное радио
CRC (Cyclic Redundancy Check) – циклический избыточный код
CRN (Cognitive Radio Network) – когнитивная радиосеть
CSMA/CA (Carrier Sense Multiple Access With Collision Avoidance) – механизм множественного доступа к среде с контролем несущей и предотвращением коллизий
CSMA/CD (Carrier Sense Multiple Access with Collision Detection) – механизм множественного доступа к среде с контролем несущей и обнаружением коллизий
CSS (Chirp Spread Spectrum) – линейно-частотная модуляция
CTS (Clear to Send) – готовность к передаче
CVO (Composite VO) – композитный виртуальный объект
CA (Cognitive Agent) – когнитивный агент
DCF (Distributed Coordination Function) – функция распределенной координации
DCMI (Dublin Core Metadata Initiative) – инициатива метаданных Дублинского ядра
DDS (Data Distribution Service) – служба распространения данных
DECT ULE (Digital European Cordless Telecommunications Ultra Low Energy) – Европейская технология цифровой беспроводной телефонной связи с низким энергопотреблением
DIN (Deutsche Institute für Normung) – немецкий институт национальных стандартов
DLC (Data Link Control) – управление каналом передачи данных
DoS (Denial of Service) – отказ в обслуживании
DPA (Differential Power Analysis) – дифференциальный анализ мощности
DSL (Digital Subscriber Line) – цифровая абонентская линия
DSR (Dynamic Source Routing) – динамическая маршрутизация от источника
DSSS (Direct Sequence Spread Spectrum) – метод расширения спектра методом прямой последовательности
ECMA (European Computer Manufacturers Association) – Европейская ассоциация производителей компьютеров
EDDL (Electronic Device Description Language) – язык описания электронных устройств
EDGE (Enhanced Data rates for GSM Evolution) – повышенная скорость передачи для развития GSM
EEPROM (Electrically Erasable Programmable Read-Only Memory) – электрически стираемое перепрограммируемое постоянное запоминающее устройство

EPC (Electronic Product Code) – электронный код продукта
ERM – обеспечение электромагнитной совместимости для радиооборудования и услуг
ETSI (European Telecommunications Standards Institute) – Европейский институт по стандартизации в области телекоммуникаций
EVRC (Enhanced Variable Rate Codec) – расширенный кодек с переменной скоростью
FDDI (Fiber Distributed Data Interface) – волоконно-оптический интерфейс передачи данных
FFD (Fully Function Device) – устройство с полным набором функций
FHSS (Frequency Hopping Spread Spectrum) – псевдослучайное изменение рабочей частоты
FTP (File Transfer Protocol) – протокол передачи файлов
GAF (Geographic Adaptive Fidelity) – пространственный адаптивный протокол маршрутизации в беспроводных сетях
GAP (Generic Access Profile) – протокол обеспечения доступа к функциям профиля устройств
GATT (Generic Attribute Profile) – протокол атрибутов профилей устройств
GBR (Greedy-based Backup Routing) – «жадный» протокол маршрутизации
GEAR (Geographic and Energy Aware Routing) – пространственный энергоэффективный протокол маршрутизации
GERAN (GSM EDGE Radio Access Network) – сеть радиодоступа к GSM
GFSK (Gaussian Frequency–Shift Keying) – гауссовская частотная манипуляция
GPRS (General Packet Radio Service) – пакетная радиосвязь общего пользования
GPS (Global Positioning System) – система глобального позиционирования
GSI (Global Standards Initiative) – глобальная инициатива по стандартизации
GSM (Global System for Mobile Communications) – глобальный стандарт цифровой мобильной сотовой связи
GSMA (Global System for Mobile Communications Association) – ассоциация GSM
HANET (Home Ad hoc Network) – домашняя ad-hoc сеть
HART (Highway Addressable Remote Transducer Protocol) – протокол дистанционно управляемого измерительного преобразователя
HCI (Host Controller Interface) – основной интерфейс контроллера
HF (High Frequency) – высокие частоты
HiperLAN (HIgh PErformance Radio Local Area) – высокоэффективный стандарт беспроводной связи
HTML (HyperText Markup Language) – язык гипертекстовой разметки
HTTP (HyperText Transfer Protocol) – протокол передачи гипертекста
IaaS (Infrastructure as a Service) – инфраструктура как услуга
ICMP (Internet Control Message Protocol) – протокол межсетевых управляющих сообщений
ID (Identifier) – идентификатор
IDA (Interactive DisAssembler) – интерактивный дизассемблер
IDS (Intrusion Detection System) – система обнаружения вторжений
IEC (International Electrotechnical Commission) – международная электротехническая комиссия
IEEE (Institute of Electrical and Electronics Engineers) – институт инженеров по электротехнике и радиоэлектронике
IERC (International Electronic Research Corporation) – международная корпорация по научным исследованиям в области электроники
IETF (Internet Engineering Task Force) – инженерный совет Интернета
IMS (IP Multimedia Subsystem) – подсистема мультимедийной связи
IoE (Internet of Everything) – всеохватывающий Интернет
IoP (Internet of People) – Интернет людей
IoT (Internet of Things) – Интернет вещей
IP (Internet Protocol) – межсетевой протокол
IPSO (IP for Smart Objects) – межсетевой протокол для «умных объектов»
IPTV (Internet Protocol Television) – интерактивное телевидение

ISA (International Society of Automation) – международная ассоциация автоматизации
ISM (Industrial, Scientific and Medical) – промышленные, научные и медицинские
ISO (International Organization for Standardization) – международная организация по стандартизации
IT (Information Technology) – информационные технологии
ITS (Intelligent Transportation System) – интеллектуальная транспортная система
ITU (International Telecommunication Union) – международный союз электросвязи
JCA–IoT (Joint Coordination Activity on Internet of Things) – группа по совместной координационной деятельности в области Интернета вещей
L2CAP (Logical Link Control and Adaptation Protocol) – протокол управления логическими каналами и согласования
LAN (Local Area Network) – локальная вычислительная сеть
LBS (Location–based service) – услуги местоположения
LEACH (Low-Energy Adaptive Clustering Hierarchy) – иерархический алгоритм адаптивной кластеризации с низким потреблением энергии
LF (Low Frequency) – Низкие частоты
LLC (Logical Link Control) – подуровень управления логической связью
LPD (Low Power Device) – диапазон радиочастот для маломощных устройств
LTE (Long Term Evolution) – глобальный стандарт для четвертого поколения мобильных сетей
M2M (Machine-to-Machine) – межмашинные коммуникации
MAN (Metropolitan Area Network) – городская сеть
MANET (Mobile Ad hoc NETwork) – беспроводная децентрализованная самоорганизующаяся сеть
MBAN (Medicine Body Area Network) – медицинская сеть для наблюдения за организмом
MCU (Multipoint Control Unit) – блок управления многосторонней связью
MDC (Multi-Domain Cooperation) – мульти-доменное взаимодействие
MIMO (Multiple-Input/Multiple-Output) – множественный вход, множественный выход
MITM (Man-In-The-Middle) – человек-посередине
MMS (Multimedia Messaging Service) – служба мультимедийных сообщений
MQTT (Message Queuing Telemetry Transport) – протокол обмена сообщениями
MSC (Mobile Switching Center) – коммутатор сети сотовой связи
MAC (Media Access Control) – управление доступом к среде
NASA (National Aeronautics and Space Administration) – национальный комитет по астронавтике и исследованию космического пространства
NDEF (NFC Data Exchange Format) – обмен данными в формате NFC
NDP (Neighbor Discovery Protocol) – протокол обнаружения соседей
NFC (Near Field Communication) – коммуникации малого радиуса действия
NGN (Next Generation Networks) – сети следующего поколения
NID (Network Identificator) – сетевой индентификатор
NSCL (Network Service Capabilities Layer) – уровня обеспечения сетевых возможностей
NUD (Neighbor Unreachability Detector) – обнаружение недостижимости соседнего узла
OASIS (Organisation for the Advancement of Standards in Information Society) – организация по развитию стандартов в информационном обществе
OFDM (Orthogonal frequency-division multiplexing) – мультиплексирование с ортогональным частотным разделением каналов
OGC (Open Geospatial Consortium) – открытый геопространственный консорциум
OMG (Object Management Group) – консорциум по разработке и продвижению объектно-ориентированных технологий и стандартов
ONS (Object Name Services) – сервис присвоения имени объекту
OODA (Observe-Orient-Decide-Act) – наблюдение-ориентация-решение-действие
OSI (Open Systems Interconnection) – модель взаимодействия открытых систем

OSIOT (Open Source Internet of Things) – Интернет вещей с открытым исходным кодом
OSS (Operation Support System) – система поддержки операций
OTA (Over The Air) – услуги по воздуху
OWL (Web Ontology Language) – язык описания онтологий для семантической паутины
OHP (Open Horizontal Platform) – открытая горизонтальная платформа
P2P (Peer-to-Peer) – равный к равному
PaaS (Platform as a Service) – платформа как услуга
PAN (Personal Area Network) – персональные сети
PAS (Personal Assistance System) – система персональной помощи
PCF (Point Coordination Function) – функция централизованной координации
PDA (Personal Digital Assistant) – карманный персональный компьютер (дословно - личный цифровой секретарь)
PEGASIS (Power-Efficient GAthering in Sensor Information Systems) – оптимизация энергопотребления в сенсорных информационных системах
PHP (Hypertext Preprocessor) – препроцессор гипертекста
PHY (Physical layer) – физический уровень
PIN (Personal Identification Number) – личный идентификационный номер
PLC (Power Line Communication) – передача данных по электропроводке
PMR (Private Mobile Radio) – частная мобильная радиостанция
PPP (Point-to-Point Protocol) – протокол «точка-точка»
QoS (Quality of Service) – качество обслуживания
QPSK (Quadrature Phase Shift Keying) – квадратурная фазовая манипуляция
RDF (Resource Description Framework) – среда описания ресурса
REST (Representational State Transfer) – передача репрезентативного состояния
RF (Radio Frequency) – радиочастотное поле
RF4CE (Radio Frequency for Consumer Electronics) – радио частоты для бытовой электроники
RFA (Radio Frequency Analysis) – радиочастотный анализ
RFC (Request for Comments) – документ из серии пронумерованных информационных документов Интернета (дословно - запрос на комментарии)
RFD (Reduced Function Device) – устройство с ограниченным набором функций
RFID (Radio Frequency IDentification) – радиочастотная идентификация
RO (Read Only) – только чтение
ROA (Resource-Oriented Architecture) – ресурс-ориентированная архитектура
RRG (Routing Research Group) – исследовательская группа по технологиям маршрутизации
RSM (Request and Situation Matching) – процедуры запроса и совпадения ситуации
RSS (Really Simple Syndication) – очень простое приобретение информации
RTS (Request to Send) – запрос на передачу
RWO (Real-World Object) – объект реального мира
SA (Standards Association) – ассоциация по стандартизации
SaaS (Software as a Service) – программное обеспечение как услуга
SAR (Specific Absorbtion Rate) – удельный коэффициент поглощения
SCADA (Supervisory Control and Data Acquisition) – диспетчерское управление и сбор данных
SDK (Software Development Kit) – набор инструментальных средств разработки программ
SDR (Software Defined Radio) – радиосвязь с программируемыми параметрами
SDS (Software-Defined Storage) – программно-определяемые хранилища данных
SGSN (Study Group on Sensor Networks) – исследовательская группа по сенсорным сетям
SHF (Super High Frequency) – микроволновые частоты
SIG (Bluetooth Special Interest Group) – консорциум по технологии Bluetooth
SIM (Subscriber Identification Module) – модуль идентификации абонента
SMP (Security Manager Protocol) – протокол обеспечения безопасности
SMS (Short Messaging Service) – служба коротких сообщений
SOA (Service-Oriented Architecture) – сервис-ориентированная архитектура

SOAP (Simple Object Access Protocol) — простой протокол доступа к объектам
SOP (Self-Organization Protocol) – самоорганизующийся протокол
SPA (Simple Power Analysis) – простой анализ мощности
SPAN (Standard Portfolio Analysis of Risk) – система портфельного анализа рисков
SPARQL (Protocol and RDF Query Language) – язык запросов к данным RDF и протокол для передачи этих запросов
SRAM (Static Random Access Memory) – статическое оперативное запоминающее устройство
SSL (Secure Sockets Layer) – уровень защищённых сокетов
SSN (Semantic Sensor Network) – сеть семантических датчиков
SWP (Single Wire Protocol) – стандарт физической шины данных и протокола обмена для связи SIM–карты и микросхемы NFC интерфейса
TAN (Tiny Area Network) – малые локальные сети
TCP (Transmission Control Protocol) – протокол управления передачей
TDMA (Time Division Multiple Access) – множественный доступ с разделением по времени
TISPAN (Telecommunications and Internet converged Services and Protocols for Advanced Networking) – конвергенция служб и протоколов телекоммуникационных сетей
TSM (Trusted Service Manager) – доверенная служба управления приложениями
UHF (Ultra High Frequency) – сверхвысокие частоты
UICC (Universal Integrated Circuit Card) – универсальная карта с интегральной схемой
UID (User IDentifier) – идентификатор пользователя
UMTS (Universal Mobile Telecommunications System) – универсальная мобильная телекоммуникационная система
UNI (User-Network Interface) – интерфейс «абонент-сеть»
URI (Uniform Resource Identifier) – унифицированный идентификатор ресурса
USB (Universal Serial Bus) – универсальная последовательная шина
USN (Ubiquitous Sensor Network) – всепроникающая сенсорная сеть
UTRAN (UMTS Terrestrial Radio Access Network) – наземная сеть радиодоступа стандарта UMTS
UWB (Ultra-Wide Band) – сверхширокая полоса
V2I (Vehicle to Infrastructure) – связь «транспортное средство-инфраструктура»
V2V (Vehicle to Vehicle) – связь «транспортное средство-транспортное средство»
VANET (Vehicular Ad Hoc Network) – автомобильная ad-hoc сеть
VAS (Value Added Service) – услуга с добавленной стоимостью
VGA (Video Graphics Array) – видеографическая матрица
VICS (Vehicle Information and Communication System) – система автомобильной информации и связи
VO (Virtual Object) – виртуальный объект
VPN (Virtual Private Network) – виртуальная частная сеть
W3C (World Wide Web Consortium) – консорциумом всемирной паутины
WAN (Wide Area Network) – глобальная сеть
WiMAX (Worldwide Interoperability for Microwave Access) – глобальная связь в микроволновом диапазоне
WLAN (Wireless Local Area Network) – беспроводная локальная сеть
WMMP (Wireless Machine-to-Machine Protocol) – беспроводной протокол взаимодействия «машина-машина»
WORM (Write Once Read Many) – однократная запись и многократное чтение
WoT (WEB of Things) – веб вещей
WPAN (Wireless Personal Area Network) – беспроводная персональная сеть
WSAN (Wireless Sensor and Actuator Networks) – сети беспроводных датчиков и актуаторов
WSC (World Standard Cooperation) – всемирное сотрудничество по стандартам
WSN (Wireless Sensor Network) – беспроводная сенсорная сеть
WWW (World Wide Web) – всемирная паутина

XML (eXtensible Markup Language) – расширяемый язык разметки
БС – базовая станция
БСС – беспроводная сенсорная сеть
ГКРЧ – государственная комиссия по радиочастотам
ГЛОНАСС – глобальная навигационная спутниковая система
ГОСТ – государственный стандарт
ЕС – Евросоюз
ЖКХ – жилищно-коммунальное хозяйство
ИК – инфракрасный
КПД – коэффициент полезного действия
КПК – карманный персональный компьютер
ЛВС – локальная вычислительная сеть
МОС – международная организация по стандартизации
МСЭ – международный союз электросвязи
МЭК – международная электротехническая комиссия
ОС – операционная система
ПЛК – программируемый логический контроллер
ПО – программное обеспечение
РЭС – радиоэлектронные средства
СВЧ – сверхвысокие частоты
ССОП – сеть связи общего пользования
СУБД – системами управления базой данных
ТфОП – телефонная сеть общего пользования

ЛИТЕРАТУРА

1. Богородицкая, И.А. M2M – новые возможности для развития сотового бизнеса [текст] / И.А. Богородицкая // Электросвязь. – 2012. – №1. – С. 38-39.
2. Бхуптани, М. ID-технологии на службе вашего бизнеса [текст] / М. Бхуптани, Ш. Морадпур. – М.: Альпина Паблишер, 2007. – 290 с.
3. Васильков, А. Микрокомпьютеры для интернета вещей: от умного дома к поумневшему окружению [текст] / А. Васильков // Компьютерра, 14 июня 2013г.
4. Вишневский, В. Mesh-сети стандарта IEEE 802.11s – технологи и реализация [текст] / В. Вишневский, Д. Лаконцев, А. Сафонов, С. Шпилев // Первая миля. – 2008. – №2-3. – С. 26-31.
5. Восков, Л.С. Web вещей – новый этап развития интернета вещей [текст] / Л.С. Восков , Н.А. Пилипенко // Качество. Инновации. Образование. – 2013. – № 2. – С. 44-49.
6. Гайкович, Г.Ф. Стандартизация в области промышленных сетей. Развитие беспроводных стандартов для АСУ ТП [текст] / Г.Ф. Гайкович // Электронные компоненты. – 2009. – №1. – С. 48-53.
7. Гиббс, М. Интернет вещей – не только для «умных» [текст] / М. Гиббс // Сети/network world. – 2013. – №3.
8. Голышко, А. Строим «интеллектуальный городок» [текст] / А. Голышко // Мобильные телекоммуникации. – 2013. - №10. – С. 46-51.
9. Гольдштейн, Б.С. Сети связи пост-NGN [текст] / Б.С. Гольдштейн, А.Е. Кучерявый. – СПб.: БХВ-Петербург, 2013. – 160 с.
10. Григорьева, А. Массовое внедрение RFID-технологии – миф или реальность? [текст] / А. Григорьева // Компоненты и технологии. – 2013. – №12.
11. Гудин, М. Технология RFID: реалии и перспективы [текст] / М. Гудин, В. Зайцев // Компоненты и технологии. – 2003. – №4.
12. Джхунян, В.Л. Электронная идентификация. Бесконтактные идентификаторы и смарт карты [текст] / В.Л. Джхунян, В.Ф. Шаньгин. – М.: «Издательство АСТ»: Издательство «НТ Пресс», 2004. – 695 с.
13. Дроздов, С. Eurotech, «интернет вещей» и «облако устройств» [текст] / С. Дроздов, С. Золотарев // Control Engineering Россия. – 2012. - № 8(78). – С. 18-24.
14. Ерохин, С.Д. Протоколы маршрутизации в беспроводных сенсорных сетях: основанные на местоположении узлов и направленные на агрегацию данных [текст] / С.Д. Ерохин, С.С. Макаров // Телекоммуникации и транспорт. T-Com. – 2013. – №3. – С. 44-47.
15. Есауленко, А. Альфа и омега M2M. Платформенные решения – основа основ мира межмашинного взаимодействия [текст] / А. Есауленко // Сети/network world. – 2013. – №3. – С. 21-22.
16. Интернет вещей и межмашинные коммуникации. Обзор ситуации в России и мире [текст] // Мобильные телекоммуникации. – 2013. – №7. – С. 26-28.
17. Калачев, А. Для мобильных стражей: беспроводной стандарт Bluetooth low energy в системах безопасности [текст] / А. Калачев // Новости электроники. – 2013. – № 1. – С. 10-18.
18. Каледин, В.В. NFC в мобильных сетях: перспективы и пути развития [текст] / В.В. Каледин, В.М. Полионов // Электросвязь. – 2011. – №5. – С. 10-14.
19. Кобец, Б. Б. Инновационное развитие электроэнергетики на базе концепции Smart Grid [текст] / Б.Б. Кобец, И.О. Волкова. – НАЦ Энергия, 2010. – 208 с.
20. Колыбельников, А. И. Обзор технологий беспроводных сетей [текст] / А.И. Колыбельников // Труды МФТИ. – 2012. – Том 4. – № 2. – С. 3-29.
21. Комашинский, В.И. Когнитивные системы и телекоммуникационные сети [текст] / В.И. Комашинский, Н.А. Соколов // Вестник связи. – 2011. – №10. – С. 4-8.

22. Коржов, В. Опасный Интернет вещей [текст] / В. Коржов // Открытые системы. СУБД. – 2013. – №4. – С. 29-30.
23. Кортьюэм, Г. Обучение поколения Интернета вещей [текст] / Г. Кортьюэм, А. Бандара, Н. Смит, М. Ричардс, М. Петре // Открытые системы. СУБД. – 2013. – №4. – С. 23-28.
24. Круз, Л. Сотовые телефоны станут датчиками? [текст] / Л. Круз // Мобильные телекоммуникации. – 2013. – №4-5. – С. 36-38.
25. Кучерявый, А.Е. Самоорганизующиеся сети [текст] / А.Е. Кучерявый, А.В. Прокопьев, Е.А. Кучерявый. – СПб, «Любавич», 2011.
26. Кучерявый, Е.А. Интернет нановещей и наносети [текст] / Е.А. Кучерявый, С. Баласубраманиям // Электросвязь. – 2014. – №4. – С. 24-26.
27. Кучерявый, Е. А. Принципы построения сенсоров и сенсорных сетей [текст] / Е. А. Кучерявый, С. А. Молчан, В. В. Кондратьев // Электросвязь. – 2006. – №6. – С.10–15.
28. Лахири, С. RFID. Руководство по внедрению [текст] / С. Лахири. – М.: Кудиц-Пресс, 2007. – 312 с.
29. Майская, В. Беспроводные сенсорные сети, малые системы – большие баксы [текст] / В. Майская // Электроника: Наука, Технология, Бизнес. – 2005. – №10. – С. 18–22.
30. Молчанов, Д.А. Приложения беспроводных сенсорных сетей / Д. А. Молчанов, Е. А. Кучерявый [текст] // Электросвязь. - 2006. - №6. - С.20-23.
31. Петров, Д. Стандарты беспроводной связи диапазона ISM [текст] / Д. Петров // Электронные компоненты. – 2010. – № 10. – С. 28-32.
32. Прохоров, А. Интернет-дом: вчера, сегодня, завтра [текст] / А. Прохоров // КомпьютерПресс. – 2002. – №2. – С. 32-38.
33. Рекомендация МСЭ-Т Y.3001. Будущие сети: целевые установки и цели проектирования, 2011 [электронный ресурс]. – 26 с.
34. Рогов, В.Г. Инфокоммуникации для «умного» города [текст] / В.Г. Рогов // Вестник связи. – 2013. – №8. – С. 39-41.
35. Рынок M2M-коммуникаций в России и мире: ноябрь 2013 года и прогноз развития [текст] // Мобильные телекоммуникации. – 2013. – №9. – С. 32-33.
36. Самсонов, М. Интернет вещей в умном городе [текст] / М. Самсонов, А. Гребешков, А. Росляков, С. Ваняшин // ИнформКурьер-Связь. – 2013. – №10. – С. 58-61.
37. Самсонов, М.Ю. Интернет вещей в умном городе [текст] / М.Ю. Самсонов, А.Ю. Гребешков, А.В. Росляков, С.В. Ваняшин // Информкурьерсвязь. – 2013. – №10. – С. 58-61.
38. Самсонов, М.Ю. Стандартизация Интернета вещей [текст] / М.Ю. Самсонов, А.Ю. Гребешков, А.В. Росляков, С.В. Ваняшин // Электросвязь. – 2013. – №8. – С. 10-13.
39. Самсонов, М.Ю. От интернета людей к интернету вещей [текст] / М.Ю. Самсонов, А.В. Росляков, С.В. Ваняшин // ИнформКурьер-Связь. – 2013. – №5. – С. 62-64.
40. Сафронов, А. Стек протоколов MiWi для беспроводных сетей [текст] / А. Сафронов // Компоненты и технологии. – 2007. - №4. - С. 160-164.
41. Сергиевский, М. Беспроводные сенсорные сети [текст] / М. Сергиевский – М. Сергиевский // КомпьютерПресс. – 2007. – №8. – С. 4-10.
42. Сети следующего поколения NGN [текст] / Под ред. А.В. Рослякова. – М.: Эко-Трендз, 2008. – 424 с.
43. Тихвинский, В.О. Партнерский проект oneM2M [текст] / В.О. Тихвинский // Электросвязь. – 2012. – №11. – С. 18-20.
44. Федоров, М. Стандарты и тенденции развития RFID-технологий [текст] / М. Федоров // Компоненты и технологии. – 2006. – № 1. – С. 108-110.
45. Филин, В. Технология RFID сегодня [текст] / В. Филин //Мир этикетки. – 2005. – №9.
46. Финкенцеллер, К. Справочник по RFID [текст] / К. Финкенцеллер. – М.: Издательский дом «Додэка-XXI», 2008. – 496 с.
47. Футахи, А. LTE и беспроводные сенсорные сети [текст] / А. Футахи, Е. Кучерявый, А. Кучерявый // Мобильные телекоммуникации. – 2012. - №6-10. – С. 38-41.

48. Храмцов, П. Всеобъемлющий Интернет: прогнозы и реальность [текст] / П. Храмцов // Открытые системы. СУБД. – 2013. – №4. – С. 19-22.
49. Чеклецов, В.В. Чувство планеты (Интернет Вещей и следующая технологическая революция) [текст] / В.В. Чеклецов. – М.: Российский исследовательский центр по Интернету Вещей, 2013. – 132 с.
50. Черняк, Л. Интернет вещей: новые вызовы и новые технологии [текст] / Л. Черняк // Открытые системы. СУБД. – 2013. – №4. – С. 14-18.
51. Черняк, Л. От первых радиометок до Интернета вещей [текст] / Л.Черняк // Открытые системы. СУБД. – 2005. – №07-08. – С. 92-94.
52. Черняк, Л. Платформа Интернета вещей [текст] / Л. Черняк // Открытые системы. СУБД. – 2012. – №7. – С. 44-45.
53. Шарфельд, Т. Системы RFID низкой стоимости [текст] / Т. Шарфельд / Под ред. С. Корнеева. – М., 2006. – 197 с.
54. Шнепс-Шнеппе, М.А. Задачи производства изделий M2M: от простого к сложному [текст] / М.А. Шнепс-Шнеппе // Вестник связи. – 2013. – №9. – С. 11-16.
55. ETSI TS 102 690 «Machine-to-Machine communications (M2M); Functional architecture» [электронный ресурс], V1.1.1. – 2011. – 280 p.
56. ETSI TS 102 921 «Machine-to-machine communications (M2M); mIa, dIa and mId interfaces» V1.1.1 [электронный ресурс]. – 2012. – 538 p.
57. Internet of Things Russia [электронный ресурс]. – Режим доступа: http://internetofthings.ru, свободный. – Загл. с экрана.
58. ISO/IEC 18092:2004. Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1) [электронный ресурс].
59. ITU-T Rec. Y.2060 (06/2012): Overview of the Internet of things [электронный ресурс].
60. NFC Forum [электронный ресурс]. – Источник: http://nfc-forum.org/, свободный. – Назв. с экрана.
61. RFID-метки [электронный ресурс]. – Режим доступа: http://rfid-m.ru, свободный. – Загл. с экрана.
62. Wi-Fi Alliance [электронный ресурс]. – Режим доступа: http://www.wi-fi.org/, свободный. – Загл. с экрана.

СОДЕРЖАНИЕ

ИНТЕРНЕТ ВЕЩЕЙ

Учебное пособие

Александр Владимирович Росляков, Сергей Владимирович Ваняшин, Александр Юрьевич Гребешков

Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования
«Поволжский государственный университет

телекоммуникаций и информатики»
443010, г. Самара, ул. Льва Толстого, 23