

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное
образовательное учреждение высшего образования
«Самарский национальный исследовательский университет
имени академика С.П. Королева»

(Самарский университет)

Институт информатики, математики и электроники

Факультет информатики

Кафедра суперкомпьютеров и общей информатики

Отчет по лабораторной работе №1

Дисциплина: «Технологии Интернета вещей»

Выполнил: Мелешенко И.С.

Группа: 6133-010402D.

Дата: 16.05.2022

Самара 2022

СОДЕРЖАНИЕ

| | |
|---|----|
| 1. Определение (понятие) IoT, для этого можно так же привести рисунок иллюстрирующий понятие IoT..... | 3 |
| 2. Концепция IoT..... | 5 |
| 3. Области применения IoT. Привести один из примеров проектов IoT (умный транспорт, умный дом и т.д.) из материалов теории «Умное производство».. | 6 |
| 4. Элементы и технологии IoT с примерами и устройством таких технологий. Дать определение основным элементам IoT и примеры таких элементов. | 8 |
| 5. Привести описание WSN. Топологии WSN..... | 12 |
| 6. Типы сетей которые могут использоваться для IoT (WAN и тп)..... | 15 |
| 7. Как производится обработка и хранение данных в IoT. Сравнение традиционной модели и новой модели IoT (cloud computing и fog computing) | 16 |
| 8. Эталонная модель iot по рек. Y.2060 мсэ-т. Кратко охарактеризовать уровни модели..... | 19 |
| 9. Эталонная модель Всемирного форума IoT. Кратко охарактеризовать уровни модели. | 22 |
| 10. Общая архитектура IoT, Кратко охарактеризовать уровни модели. | 26 |
| 11. Привести основные стандарты IoT и дать кратко характеристику каждого из них..... | 29 |
| 12. В чем особенность стандартов CIoT. Приведите краткое описание этих стандартов..... | 31 |
| 13. Краткая характеристика сетей WPAN. Принципы работы ZigBee..... | 34 |

1. ОПРЕДЕЛЕНИЕ (ПОНЯТИЕ) IOT, ДЛЯ ЭТОГО МОЖНО ТАК ЖЕ ПРИВЕСТИ РИСУНОК ИЛЛЮСТРИРУЮЩИЙ ПОНЯТИЕ IOT.



Понятие Интернет вещей (Internet of Things, IoT) можно представить, как:

- объединение множества объектов (вещей), обладающих встроенными технологиями, в единое целое через глобальную сеть;
- взаимодействие этих объектов друг с другом (получение и обмен информацией) с целью исключения участия человека (полностью или частично) в решении каких либо вопросов производственной и социальной сфер деятельности и создания максимально комфортных условий для жизни.

Таковыми сферами деятельности могут быть: медицина, транспорт, энергетика и ЖКХ, производство, окружающая среда, жилище и т.п.

Интернет вещей подразумевает, что человек определяет цель, а не задаёт программу по ее реализации. Используя искусственный интеллект и машинное обучение, вещи сами анализируют данные, предугадывают желания человека и реагируют на них. Но, так как IoT ориентирован на человека, то ему предоставляется возможность доступа к вещам. Человек постоянно видит актуальную информацию о происходящем, и в каких-то ситуациях конечное слово в принятии решений может оставаться за ним, но при этом ему однозначно будет предоставлена качественная информационная поддержка для выбора этого решения.

Физические объекты + контроллеры, сенсоры, исполнительные механизмы + Интернет (инфокоммуникационные сети) = IoT

Эта формула описывает суть интернета вещей:

- основными строительными блоками IoT являются вещи, окружающие нас;

- вещи имеют конкретный адрес в сети или устройства для их идентификации; снабжены микроконтроллерами, обеспечивающими интеллектуальность; датчиками/сенсорами, способными собирать данные о контролируемом объекте/явлении и/или исполнительными механизмами, срабатывающими от определенного параметра;

- данные с использованием сети Интернет передаются в вычислительные системы/платформы, где они хранятся и обрабатываются, а затем в режиме реального времени используются вещами для выполнения разного рода интеллектуальных действий, которые и делают их «умными (smart) вещами».

2. КОНЦЕПЦИЯ IOT.

Концепция IoT предполагает, что:

- 1) создается база, абсолютно всех необходимых для умного интернета, знаний;
- 2) описываются абсолютно все логические правила;
- 3) интеллектуальные объекты, используя эти знания и взаимодействуя между собой через Интернет, достигают целей, необходимых человеку.

3. ОБЛАСТИ ПРИМЕНЕНИЯ ИОТ. ПРИВЕСТИ ОДИН ИЗ ПРИМЕРОВ ПРОЕКТОВ ИОТ (УМНЫЙ ТРАНСПОРТ, УМНЫЙ ДОМ И Т.Д.) ИЗ МАТЕРИАЛОВ ТЕОРИИ «УМНОЕ ПРОИЗВОДСТВО».

Технологии IoT открывают неограниченные возможности в различных областях, начиная с интернет-подключения вещей дома или на работе, взаимодействия вещей на производстве и заканчивая миром развлечений. Примером работы приложения IoT может быть следующая ситуация. Человек, выключая компьютер в офисе по вкладке «Завершение работы, домой» дает вещам команду на выполнение определенного приложения: ПК передает информацию автомобилю, который включает двигатель, получает данные о скорости машин на пути к дому, строится карта загруженности дорог, помогая найти наиболее быстрый маршрут, автомобиль сообщает расчетное время прибытия, и к этому времени в доме включается свет, микроволновая печь начинает разогревать ужин, после открытия двери дома включается телевизор с определенной для этого времени телепрограммой или музыка, а также выполняются другие «умные» действия, необходимые человеку.

«Умное производство» (smart manufacturing) представляет собой производственную среду, которая включает в себя всю активность, связанную с изготовлением, обеспечением качества продукции, управлением инвентаризацией, логистикой и техническим обслуживанием. «Умное производство» предполагает создание единой системы, в которой машины могут обмениваться данными между собой в режиме реального времени:

- обмен между оборудованием, расположенным непосредственно на производственных площадях и в логистической цепочке, включая бизнес-системы, поставщиков и потребителей;
- передача сведений о своем состоянии обслуживающему персоналу.

При этом производственное оборудование, получая сведения об изменившихся условиях и требованиях, может само вносить корректировки в технологический процесс.

Для достижения своих целей «Умные предприятия» используют специализированное программное обеспечение, лазеры, устройства с искусственным интеллектом, встроенные в машины или инфраструктуру предприятия.

4. ЭЛЕМЕНТЫ И ТЕХНОЛОГИИ ИОТ С ПРИМЕРАМИ И УСТРОЙСТВОМ ТАКИХ ТЕХНОЛОГИЙ. ДАТЬ ОПРЕДЕЛЕНИЕ ОСНОВНЫМ ЭЛЕМЕНТАМ ИОТ И ПРИМЕРЫ ТАКИХ ЭЛЕМЕНТОВ.

Иот предполагает, что для реализации какого либо приложения (услуги), необходимо идентифицировать объект (1), собрать необходимую полезную информацию (2), передать её в вычислительную систему, осуществляющую анализ, обработку, хранение данных и управление определенными действиями (3-4).

Шаг 1. Идентификация

В момент подключения к сети Иот каждое устройство обязано опознать себя. В качестве средства идентификации могут использоваться:

- различные визуально распознаваемые идентификаторы, которые, после считывания, могут быть использованы компьютером для поиска дополнительной информации о продукте:

- штрих-коды (графическая информация, наносимая на поверхность, маркировку или упаковку изделий),

- QR-коды (англ. Quick Response Code (QR code) - код быстрого реагирования) – товарный знак для типа матричных штрихкодов (или двумерных штрихкодов),

- средства определения местонахождения предмета в реальном времени: MAC-адреса, SIM и R-UIM карты.

MAC-адрес (от англ. Media Access Control – управление доступом к среде, или Hardware Address – аппаратный адрес) – уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях Ethernet. MAC-адрес является уникальным аппаратным численно-буквенным номером, который завод-изготовитель присваивает на постоянной основе каждому

выпускаемому сетевому устройству: сетевым картам, маршрутизаторам, Wi-Fi-адаптерам и т.д. На стадии изготовления MAC-адрес вшивается непосредственно в само сетевое устройство и больше уже не может быть изменён.

В сетях мобильной связи для идентификации объектов могут использоваться, например, SIM-карта (англ. Subscriber Identification Module — модуль идентификации абонента), R-UIM (англ. Removable User Identity Module – сменная идентификационная карточка пользователя) и т.п.

Также для идентификации объектов может использоваться технология RFID (англ. Radio Frequency IDentification) – радиочастотная идентификация.

RFID – это способ автоматической идентификации объектов, при котором с помощью радиосигналов считываются или записываются данные, хранящиеся в так называемых транспондерах (англ. transmitter – передатчик, responder – ответчик) или RFID-метках (англ. tag).

RFID система включает RFID-метку и считыватель (англ. reader).

Технология передачи информации по радиоканалу поддерживает как активные, так и пассивные устройства.

Пассивная RFID-метка способна работать без собственного источника энергии, она получает энергию для питания только от сигнала считывателя. При этом необходимо устройство считывания достаточно большой мощности.

Активная метка отличается наличием батареи питания, дальностью считывания в 2-3 раза большей, чем у пассивной метки, а также более высокой скоростью передвижения через зону действия сканера. Активные метки могут содержать набор определенной логики, позволяющей метке обмениваться данными с такой же меткой или считывателем.

Существуют полупассивные (полуактивные) метки со встроенной батареей. В них источник питания дает энергию для работы метки, но при передаче своих данных она использует энергию от считывателя.

Технология связи на малых расстояниях NFC (Near Field Communication – коммуникация в ближнем поле) является логическим продолжением технологии RFID. Это технология беспроводной высокочастотной связи малого радиуса действия (до 10 см), позволяющая осуществлять бесконтактный обмен данными между устройствами с поддержкой NFC, расположенными на небольших расстояниях. Технология NFC разработана для обмена различными типами информации, такими как изображения, файлы формата MP3 или данными цифровой авторизации между двумя устройствами с поддержкой NFC. Данные могут передаваться между мобильными телефонами, имеющими NFC, или между NFC-телефонами и совместимыми RFID чип-картами или считывающими устройствами, расположенными в непосредственной близости друг от друга. Технология может использоваться в качестве ключа доступа к данным или сервисам, например бесконтактные транспортные и банковские карты, электронные ключи, приложения, формирующие контент для услуг на основе NFC.

Реализуется технология при помощи небольшого чипа, который устанавливается в устройства и обладает низким энергопотреблением.

Максимальный радиус действия NFC около 10 см.

Используемая частота: 13,56 МГц.

Скорость передачи данных: 106 Кбит/с, 212 Кбит/с, 424 Кбит/с.

Время установления связи – менее 0,1 с

Шаг 2. Сбор информации

«Умные» объекты интегрированы с сенсорами/датчиками, задачами которых, в рамках технологии интернета вещей, является сбор и обработка информации в реальном времени.

Датчик (transducer) – это средство измерения (контроля) и преобразования одного вида энергии в другой.

Сенсор (sensor) (от латинского sentire – «чувствовать» или «ощущать») – устройство, выполняющее наблюдение за материальным объектом (процессом, средой), его физическим (физико-химическим) состоянием (свет, давление, температура и т.п.), измеряющее его количественные, качественные характеристики и преобразующее их в удобный для хранения, обработки и управления сигнал. Т.к. сенсор преобразует физическую информацию в электрическую, то он тоже является датчиком. Поэтому, далее по тексту, эти понятия будут употребляться, как тождественные.

Датчики могут иметь небольшую память, давая возможность записывать некоторое количество результатов измерений. Они получают необходимые данные и преобразуют их в формат, который смогут воспринять другие объекты IoT, например, актуаторы – исполнительные устройства.

Актуатор – это устройство системы автоматического управления или регулирования, воздействующее на управляемый объект (процесс) в соответствии с получаемой командной информацией. Входные и выходные сигналы исполнительных устройств, а также их методы воздействия на объект управления могут иметь различную физическую природу.

5. ПРИВЕСТИ ОПИСАНИЕ WSN. ТОПОЛОГИИ WSN.

Датчики собирают данные, поступающие от большого числа источников, и далее, эти данные обрабатываются для обеспечения реакции, соответствующей зафиксированным событиям (например, срабатывание актуатора, передача показаний счетчиков электроэнергии в систему тарификации,

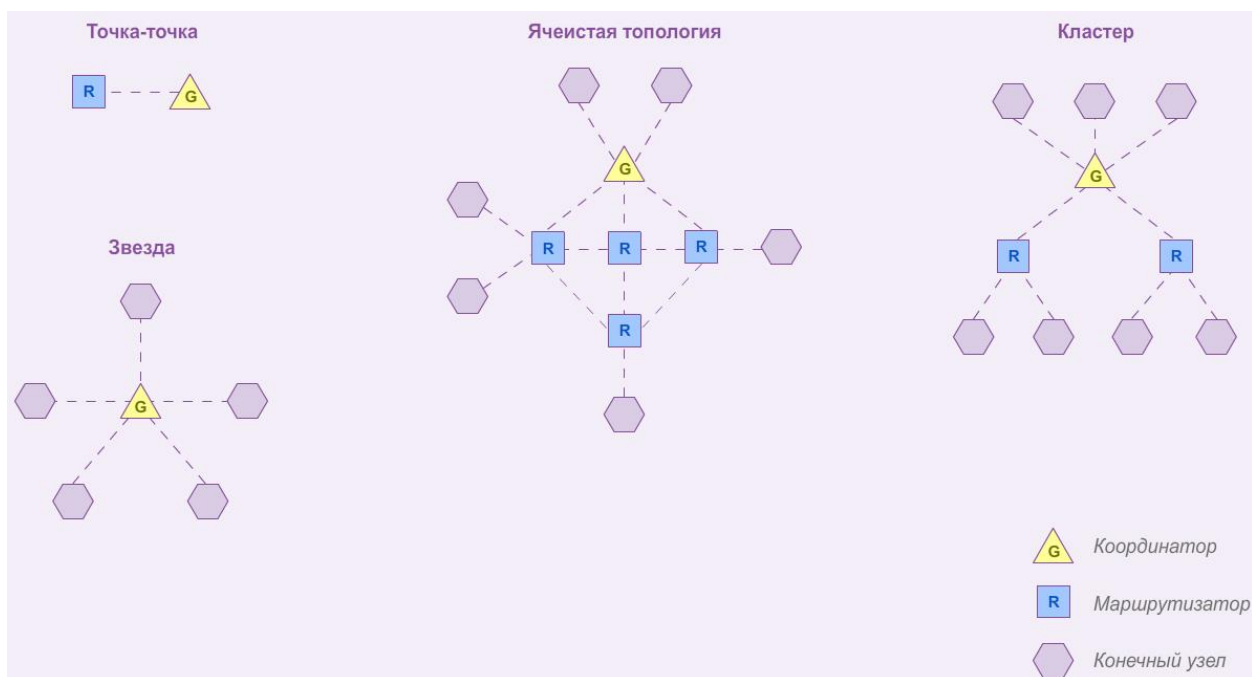
отображение информации на смартфоне).

В качестве примера можно рассмотреть сельское хозяйство, где для достижения хорошего урожая необходимо контролировать (с помощью датчиков) состояние влажности почвы, концентрации содержащихся в грунте веществ и ряд других параметров, и уже, исходя из этих данных, принимать решение о необходимости полива, внесении удобрений и иных действиях.

Чтобы осуществлять подобную деятельность автоматизировано, необходимо обеспечить обмен информацией между всеми задействованными в процессе устройствами, т.е. создать единую сеть датчиков: влажности, состава почвы и исполнительных устройств: поливочная машина, дозатор удобрений. Для этих целей в IoT используются различные технологии, в том числе, технология беспроводных сенсорных сетей WSN (Wireless Sensor Network).

Беспроводные сенсорные сети – это масштабное по числу узлов и занимаемой площади организованное множество отдельных чувствительных элементов и исполнительных устройств, объединенных при помощи беспроводного канала для обмена информацией. Эти сети способны функционировать как автономно, так и во взаимодействии с другими сетями и вычислительными мощностями для реализации приложений IoT. Беспроводные сенсорные сети относятся к классу беспроводных персональных вычислительных сетей WPAN (Wireless Personal Area Networks).

Узел WSN сети (sensor node) содержит датчик, воспринимающий данные от внешней среды, микроконтроллер, память, радиопередатчик, автономный источник питания и иногда исполнительные механизмы.



Беспроводные сенсорные сети WSN могут быть одноранговые, кластерные и Mesh.

Каждый узел одноранговой сети обладает такими же полномочиями, как и все остальные, т.е. все узлы в сети равны. Такое равенство позволяет добиться оптимальной маршрутизации, экономит энергию сенсоров и время передачи информации. Одноранговые сети имеют топологии «точка-точка», «звезда». Связь с внешними сетями осуществляется с использованием координатора (шлюза или базовой станции), т.е. устройства, которое управляет подчиненными устройствами сети и взаимодействует с внешней сетью.

Кластерная сеть состоит из кластеров, узлы которых не равноправны. Кластер состоит из маршрутизатора и сенсоров. Сенсоры только собирают информацию и передают маршрутизатору, который буферизирует данные и осуществляет их дальнейшую передачу. Маршрутизаторы передают информацию друг другу до достижения координатора.

Mesh сеть – это распределенная, ячеистая сеть. Ячеистой называют сеть, где реализуется одна из двух возможных схем соединения: с полной и с неполной (частичной) связью. В первом случае каждый узел непосредственно соединен со всеми остальными, а во втором – определенные узлы связаны напрямую только с теми, с которыми у них в основном происходит обмен данными. Т.е. в такой сети каждое устройство может связываться с любым другим устройством как напрямую, так и через промежуточные узлы сети.

Ячеистая топология предлагает альтернативные варианты выбора маршрута между узлами. Сообщения поступают от узла к узлу, пока не достигнут конечного получателя. Возможны различные пути прохождения сообщений, что повышает доступность сети в случае выхода из строя того или иного звена. Ячеистые сети имеют функцию самоорганизации и самонастройки. При включении узел такой сети автоматически подключается к существующим участникам, автоматически определяет состояние соседних узлов и свою роль в общей топологии сети. Узлы в сети обмениваются маршрутной информацией, выбирая оптимальный, а при выходе из строя одного из узлов, сеть автоматически переопределяет маршруты (перенаправляет данные).

6. ТИПЫ СЕТЕЙ КОТОРЫЕ МОГУТ ИСПОЛЬЗОВАТЬСЯ ДЛЯ ИОТ (WAN И ТП).

Для передачи информации от вещей могут использоваться различного рода сети: PAN, LAN, MAN, WAN, GAN.

Глобальная сеть Интернет GAN (Global Area Network), охватывающая всю планету, состоит из сетей стран и континентов WAN (Wide Area Network), которые связывают сети городов MAN (Metropolitan Area Network). Сети городов, в свою очередь, объединяют локальные сети LAN (Local Area Network) предприятий, учреждений, жилых районов и т.п. Компьютерные сети, которые используются для передачи данных между устройствами, расположенными на достаточно небольшом расстоянии и зачастую принадлежащими одному пользователю, – это персональные сети PAN (Personal Area Network) и нательные сети BAN (Body Area Network).

Глобальная вычислительная сеть служит для объединения разрозненных сетей таким образом, чтобы участники этой сети, где бы они ни находились, могли взаимодействовать со всеми остальными её участниками.

В роли глобальной сети для интернет-вещей используется сеть Интернет. Общим протоколом является IP. Таким образом вещи имеют возможность взаимодействия для решения совместных вычислительных задач.

7. КАК ПРОИЗВОДИТСЯ ОБРАБОТКА И ХРАНЕНИЕ ДАННЫХ В ИОТ. СРАВНЕНИЕ ТРАДИЦИОННОЙ МОДЕЛИ И НОВОЙ МОДЕЛИ ИОТ (CLOUD COMPUTING И FOG COMPUTING)

В концепции интернета-вещей, вычислительная сеть, в которой хранятся и обрабатываются данные для функциональной реализации IoT, – это облачные вычисления (англ. Cloud Computing (CC)). Облачные вычисления подразумевают аренду услуг и ресурсов для хранения и обработки данных в глобальной сети. Облачное хранилище данных (англ. cloudstorage) – модель онлайн-хранилища, в котором данные хранятся на многочисленных распределённых в сети серверах, предоставляемых в пользование клиентам, в основном, третьей стороной. Доступ к информации обеспечивается в любом месте и в любое время, при условии наличия Интернета.

В отличие от модели хранения данных на собственных серверах, приобретаемых специально для подобных целей, количество или какая-либо внутренняя структура облачных серверов пользователю не видна. С точки зрения пользователя, cloudstorage – один большой виртуальный сервер. Физически же, это многочисленные сервера, которые могут располагаться географически удалённо друг от друга. Провайдер «облачного» центра предоставляет возможности по организации совместной работы с данными, резервированию и сохранению целостности данных в случае аппаратных сбоев, без вовлечения в этот процесс пользователя.

Развитие интернета вещей потребовало поддержки мобильности устройств IoT для различных местоположений с геолокацией и с малой задержкой на обработку данных. Но в облачной модели, используемой в IoT, пропускная способность каналов операторов связи, по которым осуществляется обмен данными между «облаком» и «умными» устройствами, является слабым местом. Поэтому в IoT наряду с облачными технологиями применяются технологии, где более рационально выполнять большую часть обработки данных как можно ближе к датчикам и другим устройствам

генерации Big Data (физически на краю сети IoT). Данная концепция получила название «Туманные Вычисления» (Fog Computing) и предполагает обработку данных на конечных устройствах сети (компьютерах, мобильных устройствах, датчиках, смарт-узлах и т.п.), а не в облаке. Термин «Fog Computing» ввёл в оборот вице-президент компании Cisco Флавио Бономи (Flavio Bonomi) в 2011 году.

Примером приложения, для которого требуется высокое быстродействие и критична задержка в принятии решения, может быть автономная система вождения ADS (Autonomous Driving System), в которой автопилот управляет автомобилем. Для принятия решения система использует различные многорежимные сенсоры, технологии компьютерного зрения и анализа изображений, спутниковое и сетевое позиционирование на картах, которые необходимо сверхбыстро анализировать и обрабатывать, поэтому Fog-узел с элементами искусственного интеллекта должен быть размещен непосредственно в транспортном средстве.

Также задачей Fog Computing является обеспечение взаимодействия многочисленных устройств между собой и «облаком», т.к. некоторые приложения IoT требуют фильтрации или предварительной обработки данных перед отправкой в «облако». Такими приложениями могут быть:

- приложения с низкой и предсказуемой задержкой передачи информации по сети,
- приложения, требующие локальной обработки данных в реальном времени (интеллектуальные системы электроснабжения (Smart Grid), интеллектуальные транспортные системы (ИТС), геофизическая разведка недр, управление трубопроводами, сенсорные сети мониторинга окружающей среды и пр.).

Преимуществом новой модели анализа и обработки данных с применением туманных вычислений является снижение объема данных,

передаваемых в «облако», уменьшение требований к пропускной способности сети, увеличение скорости обработки данных и снижение задержек в принятии решений.

Повышение пропускной способности каналов связи Cloud Computing может обеспечить новый подход к их построению - использование технологии Software-Defined Networks (SDN), внедрение которой позволит повысить эффективность работы каналов связи между Cloud Computing и IoT.

Разработкой системной архитектуры для «туманных» моделей и методов практического внедрения новых моделей вычислений занимается Консорциум (Consortium) OpenFog , учрежденный в 2015 году компаниями ARM, Cisco, Dell, Intel, Microsoft и Принстонским университетом.

Область применения архитектуры с Fog Computing обозначена компанией Cisco: "туманные вычисления, в наибольшей степени, подходят для работы с системами межмашинного взаимодействия (machine-to-machine, M2M) и устройств, использующих человеко-машинный интерфейс (human-machine interface, HMI)".

После обработки информации в вычислительных системах реализуется завершающий этап приложения IoT - осуществляется управление различными действиями, направленными на получение желаемого результата.

8. ЭТАЛОННАЯ МОДЕЛЬ ИОТ ПО РЕК. Y.2060 МСЭ-Т. КРАТКО ОХАРАКТЕРИЗОВАТЬ УРОВНИ МОДЕЛИ.



Разработкой эталонных моделей IoT занимаются Международный союз электросвязи МСЭ-Т (англ. ITU - International Telecommunication Union) и Всемирный форум по Интернету вещей (англ. IoTWorldForum, IWF). Целью создания таких обобщенных моделей является обеспечение взаимной совместимости всех IoT- компонентов: объектов и контроллеров, сетей, вычислительных систем, хранилищ данных, приложений и аналитики. Эталонная модель IoT по Рекомендации Y.2060 Международного союза электросвязи состоит из четырех уровней с поддержкой функций управления и обеспечения безопасности, действующими между уровнями. Одним из важных аспектов модели МСЭ-Т является утверждение, что IoT на деле не является сетью физических вещей. Это скорее сеть устройств, взаимодействующих с физическими вещами, и прикладных платформ (компьютеры, планшеты и смартфоны), которые взаимодействуют с этими устройствами.

Уровень устройства включает возможности устройства и возможности шлюза. Этот уровень можно сравнить с физическим и канальным уровнями

модели OSI. Предназначен уровень непосредственно для передачи потока данных.

Возможности устройства предполагают его прямой обмен с сетью связи, обмен через шлюз, обмен через беспроводную сеть.

Возможности шлюза предполагают поддержку множества интерфейсов для взаимодействия с устройствами (шина CAN, ZigBee, Bluetooth, WiFi и др.) и для взаимодействия с сетями доступа/транспортными сетями (2G/3G, LTE, DSL и др.). Еще одной возможностью шлюза является конвертация протоколов, в случае, если протоколы интерфейсов устройств и сетей отличаются друг от друга.

Уровень сети определяет возможности сети и транспортные возможности.

Возможности сети - это возможности сетевой инфраструктуры, которая создается путем интеграции разнородных сетей в единую сетевую платформу.

Транспортные возможности - это возможности сети по передаче информации служб и приложений IoT, а также информации управления и контроля IoT. Можно сказать, что эти возможности соответствуют сетевому и транспортному уровням модели OSI.

Уровень поддержки услуг и поддержки приложений предоставляет возможности, которые используются приложениями, по обработке и хранению данных, управлению базами данных (БД).

Этот уровень включает, как общие возможности для различных объектов IoT, так и ограниченные или специализированные возможности поддержки, необходимые только для некоторых приложений IoT или групп таких приложений.

Уровень приложения включает различные типы приложений, взаимодействующих с IoT-устройствами.

Уровень возможностей управления охватывает следующие функции управления сетью:

- управление устройствами (обнаружение устройств, аутентификацию, активацию и деактивацию устройств, диагностику, обновление прошивки и/или ПО, управление рабочим статусом устройства)

- управление неисправностями, конфигурацией, трафиком и перегрузками, учетом, а также управление безопасностью.

Специализированные (ограниченные) возможности управления тесно связаны с требованиями приложений, например с требованиями по контролю линии передачи электроэнергии в «умной» электросети.

Уровень возможностей обеспечения безопасности включает общие возможности обеспечения безопасности, которые не зависят от конкретных приложений. В Рекомендации Y.2060 приведены следующие примеры общих возможностей обеспечения безопасности:

- на уровне приложения: авторизация, аутентификация, защита конфиденциальности и целостности данных приложения, защита неприкосновенности частной жизни, аудит безопасности и антивирусная защита;

- на уровне сети: авторизация, аутентификация, конфиденциальность данных об использовании и данных сигнализации, а также защита целостности данных сигнализации;

- на уровне устройства: аутентификация, авторизация, проверка целостности устройства, управление доступом, защита конфиденциальности и целостности данных.

Специализированные (ограниченные) возможности обеспечения безопасности тесно связаны с требованиями приложений, например, требованиями безопасности мобильных платежей.

9. ЭТАЛОННАЯ МОДЕЛЬ ВСЕМИРНОГО ФОРУМА IOT. КРАТКО ОХАРАКТЕРИЗОВАТЬ УРОВНИ МОДЕЛИ.



Всемирный форум IoT объединяет представителей бизнеса (IBM, Intel и Cisco), госструктур и вузовской науки. Его эталонная модель IoT была опубликована в октябре 2014 года. Она явилась полезным дополнением к модели МСЭ-Т, т.к. документы МСЭ-Т наибольшее внимание уделяют поддержке разработки стандартов взаимодействия с устройствами IoT (уровень устройства и шлюза), а в эталонной модели IWF предложена семиуровневая модель, уделяющая наибольшее внимание вопросам разработки приложений и функциям поддержки корпоративного (промышленного) интернета вещей.

Уровень 1 – физические устройства и контроллеры (physical devices & controllers) и **Уровень 2** - связь (connectivity) примерно соответствуют уровням

устройств и сети в модели МСЭ-Т. Основное отличие в том, что модель IWF относит шлюзы к Уровню 2, в то время как в модели МСЭ-Т они относятся к Уровню 1.

Задачей **Уровня 3** - периферийных вычислений (edge computing level) является базовая обработка больших объемов генерируемых устройствами данных для частичного снижения этой функции с прикладных программ IoT. В результате обработки информации на этом уровне, данные будут занимать гораздо меньший объем.

Примерами операций на уровне периферийных вычислений в эталонной модели IWF являются:

- анализ: анализ данных по критериям того, подлежат ли они обработке на более высоком уровне;
- форматирование: переформатирование данных для единообразной высокоуровневой обработки;
- разархивирование/декодирование: обработка криптографических данных;
- дистилляция/сокращение: сокращение данных;
- оценка: определение того, представляют ли данные пороговое значение или аварийный сигнал, чтобы перенаправить данные дополнительным получателям.

На **Уровне 4**, данные помещаются в хранилище, где будут доступны для более высоких уровней.

В IoT существуют приложения, где генерация данных происходит в реальном времени: либо периодически, либо по возникновению какого-либо события, на появление которого необходимо реагировать. Такие данные, проходящие сквозь сеть, называются «данными в движении».

Но многим приложениям не требуется обрабатывать данные со скоростью сетевой передачи. Они имеют дело с «данными в покое», т.е. данными, помещенными в том или ином легкодоступном хранилище. Таким

образом, приложения могут обращаться к данным по мере необходимости, либо вне режима реального времени.

К операциям, выполняемым на уровне накопления данных, относятся:

- преобразование «данных в движении» в «данные в покое»;
- преобразование формата данных из сетевых пакетов в реляционные таблицы баз данных;
- переход от вычислений по событиям к вычислениям по запросу;
- фильтрация данных и выборочное хранение.

С уровня периферийных вычислений в хранилище накопления данных может поступать огромное количество разных видов информации, в разных форматах и от разнородных обработчиков, которые, практически, не приспособлены к потребностям конкретных приложений. Уровень абстракции данных (*уровень 5*) агрегирует и форматирует эти данные такими способами, которые делают доступ приложений к ним более управляемым и эффективным. В числе задач этого уровня могут быть следующие:

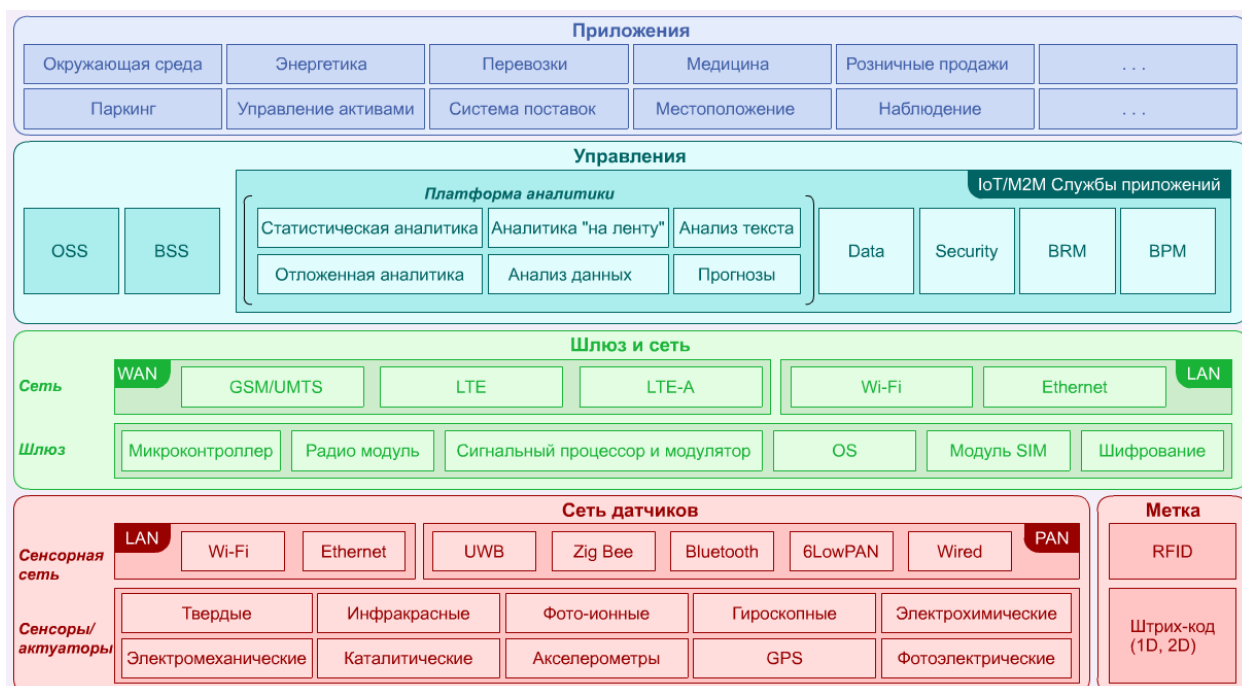
- комбинирование данных из различных источников и выполнение необходимых преобразований для обеспечения единообразной семантики;
- помещение отформатированных данных в соответствующую базу данных;
- оповещение приложений о том, что данные заполнены или достигнут определенный уровень данных;
- консолидация данных в одном месте, либо предоставление доступа к нескольким источникам данных путем виртуализации данных;
- защита данных путем соответствующей аутентификации и авторизации.

Уровень приложения (уровень 6) содержит приложения любого типа, использующие данные IoT на входе или управляющие IoT-устройствами. Как правило, приложения взаимодействуют с уровнем 5 и с данными в покое. Но IWF считает, что следует предусмотреть упрощенный режим работы, который

позволит приложениям миновать промежуточные уровни 4-5 и напрямую взаимодействовать с уровнем 3 или даже уровнем 2.

Уровень 7 «сотрудничество и процессы» подразумевает, что с приложениями смогут взаимодействовать люди и бизнес-процессы путем обмена данными и/или управляющей информацией по Интернету или корпоративной сети.

10. ОБЩАЯ АРХИТЕКТУРА ИОТ, КРАТКО ОХАРАКТЕРИЗОВАТЬ УРОВНИ МОДЕЛИ.



Получив информацию о моделях IoT, рассмотрим общую архитектуру Интернета вещей.

Архитектура IoT включает четыре функциональных уровня:

1. Сеть датчиков
2. Шлюзов и сетей
3. Управления
4. Приложений

Сеть датчиков или уровень датчиков (сенсоров/актуаторов) и сенсорных сетей.

На этом уровне располагаются датчики и беспроводные сенсорные сети, которые могут подключаться к шлюзам с использованием локальной вычислительной сети LAN (Ethernet, Wi-Fi) или персональных сетей PAN (ZigBee, Bluetooth, UWB, 6Low PAN, проводные).

Для датчиков, которые не требуют подключения к шлюзу, связь с приложениями может предоставляться с использованием глобальных беспроводных сетей WAN, таких как GSM, UMTS, LTE.

Так как нижний уровень архитектуры интернета вещей состоит из датчиков и сенсорных сетей, то для обеспечения взаимодействия этих устройств между собой, а также с верхними уровнями (обработка, управление), необходимы "собственные" протоколы, поскольку стандартные прикладные инфокоммуникационные протоколы не приспособлены к условиям сети IoT.

Для IoT разработаны следующие специальные протоколы, которые используются на различных участках сети: CoAP (Constrained Application Protocol), MQTT (Message Queue Telemetry Transport), DDS (Data Distribution Service), XMPP (Extensible Messaging and Presence Protocol), SOAP (Simple Object Access Protocol), STOMP – Simple (или Streaming) Text Oriented Message Protocol. Работа таких протоколов, как MQTT и CoAP, будут рассмотрены далее в данном курсе.

Основные задачи протоколов различны, различны архитектуры и возможности. Ключевые особенности протоколов зависят от их предполагаемого применения, поэтому разработчики выбирают для конкретного приложения оптимальный протокол, объективно взвешивая все его положительные и отрицательные свойства.

Уровень шлюзов и сетей.

Шлюзы, которые состоят из процессоров обработки сигналов и модуляторов, микро-контроллеров, встроенных операционных систем, отвечают за маршрутизацию данных, поступающих от датчиков, взаимодействие различных сетевых протоколов и передачу данных к уровню Управления по сетям LAN и WAN.

Уровень Управления содержит набор информационных услуг, призванных автоматизировать технологические операции и бизнес процессы в IoT :

- поддержка операционной и бизнес деятельности OSS/BSS (Operation Support System/Business Support System),

- аналитическая обработка информации различного рода (статистическая, интеллектуального анализа данных и текстов, прогностическая аналитика и др.),

- хранение данных (Data),

- обеспечение информационной безопасности (Security),

- управление бизнес-правилами (BRM, Business Rule Management),

- управление бизнес-процессами (BPM, Business Process Management).

Уровень Приложений включает различные типы приложений для соответствующих сфер деятельности (окружающая среда, паркинг, энергетика, транспорт, торговля, медицина, образование и др.).

11. ПРИВЕСТИ ОСНОВНЫЕ СТАНДАРТЫ ИОТ И ДАТЬ КРАТКО ХАРАКТЕРИСТИКУ КАЖДОГО ИЗ НИХ.

Требования, предъявляемые к сетям IoT, зависят от конкретного сервиса (услуги), а каждый сервис требует от сети совершенно разных возможностей. Единой сетевой технологии, которая бы удовлетворяла одновременно всем требованиям IoT, на данный момент не существует. Поэтому для интернета вещей целенаправленно создаются независимые специализированные IoT-сетевые решения, или выискиваются способы модернизации технологий мобильной связи.

Ввиду сложности физической реализации, проводные сети (кабель связи, оптоволокно) для сбора и передачи информации IoT используются очень редко, а применяются технологии беспроводных сетей, такие как WPAN, WLAN, LPWAN.

LPWAN (Low-power Wide-area Network) - Беспроводные технологии Глобальных сетей малой мощности (также может использоваться термин — LPWA - Low Power Wide Area).

Распространенными, на данный момент, технологиями сетей дальнего радиуса действия LPWAN являются:

- LoRaWAN,
- SIGFOX,
- "Стриж",
- интернет вещей в сетях сотовой связи CIoT (Cellular Internet of Things), включающий технологии: EC-GSM, LTE-M, NB-IoT.

Но существует и масса других LPWAN сетей, менее востребованных, но использующихся: ISA-100.11.a, Wireless, DASH7, SymphonyLink, RPMA и т.п.

Беспроводные персональные сети WPAN (Wireless Personal Area Network) и беспроводные локальные сети WLAN (Wireless Local Area Network) – это сети, задачей которых является сбор и передача информации от интернет вещей и их взаимодействие. Такие сети могут использоваться как автономно, для объединения отдельных устройств между собой и решения задач в рамках сети, так и для передачи данных в сети более высокого уровня и реализации приложений на уровне глобальной сети.

К технологиям/стандартам, используемым на сетях WPAN, относятся такие, как ZigBee, 6LoWPAN, Wi-Fi, Thread, BLE 4.2 (BluetoothMesh), Z-Wave, Wireless RF и другие, характеризующиеся низким потреблением энергии и небольшим радиусом приема сигналов.

12. В ЧЕМ ОСОБЕННОСТЬ СТАНДАРТОВ CIOT. ПРИВЕДИТЕ КРАТКОЕ ОПИСАНИЕ ЭТИХ СТАНДАРТОВ.

Конкурентами технологий SIGFOX, LoRaWAN, «Стриж» и т.п. на рынке сетей LPWAN являются технологии сетей сотовой связи для IoT - CIoT, использующие лицензируемые частотные диапазоны:

- EC-GSM (ExtendedCoverage GSM), которая также носит названия EC-GPRS, EC-GSM-IoT;
- LTE-M (LTE для M2M-коммуникаций), которая также носит названия eMTC, LTE Cat.M1;
- NB-IoT (Narrowband IoT) - узкополосный IoT;
- пятое поколение сотовой связи 5G (fifth generation).

Данные технологии разрабатываются консорциумом 3GPP и предназначены для построения беспроводных сетей LPWAN для IoT на основе существующей инфраструктуры операторов сотовой связи.

В отличие от традиционных технологий сетей мобильной связи (GSM/WCDMA/LTE) эти технологии должны обеспечить:

- лучшее покрытие сети, обеспечивающее достаточно устойчивую передачу данных не только в населенных пунктах, но и там, где могут быть расположены устройства IoT, и где людей большую часть времени нет: отдаленные районы, протяженные железнодорожные перегоны, поверхность обширных водоемов, подвалы, изолированные бетонные и металлические короба, лифтовые шахты, и т.п.;
- низкое энергопотребление и продолжительное время автономной работы конечных устройств, т.к. многие сценарии и области применения IoT предусматривают автономное питание подключенных устройств от встроенных элементов;
- более низкую стоимость мобильных устройств, которые для большинства IoT сценариев не должны иметь полный набор сетевых технологий, включая передачу голоса;
- поддержку большого количества доступных устройств.

Технологии CIoT отличаются высокой пропускной способностью больших объемов данных.

Технология EC-GSM использует частотные диапазоны стандарта GSM. Предусматривает сравнительно небольшие изменения относительно базового стандарта GSM/GPRS/EDGE, что позволяет использовать подавляющее большинство установленных базовых станций этого стандарта без замены или модернизации аппаратного обеспечения, а только с обновлением программного обеспечения. Максимальная скорость передачи данных – 70-240 Кбит/с.

LTE-M является адаптацией сетей LTE для IoT. Используемый частотный спектр – несущая 1,08 МГц в рамках полосы LTE. LTE-M имеет высокую степень готовности сетевой инфраструктуры и может быть развернута на существующих сетях LTE путем обновления ПО. Максимальная скорость передачи данных – 1 Мбит/с.

NB-IoT используется в рамках полосы частот, используемой сетью LTE., но имеет свой стандарт радиодоступа. Максимальная скорость передачи данных – вниз – 250 Кбит/с, вверх – 20 или 250 Кбит/с. Количество устройств интернета вещей - приблизительно 50 000 на один сектор базовой станции.

Стратегическим направлением в CIoT являются сотовые сети нового поколения 5G. Технология 5G, предназначенная для работы с разнородным трафиком, обеспечит подключение к Интернет как мобильных устройств (смартфонов, телефонов, планшетов и т.д.), так и умных устройств с разными параметрами (энергопотреблением, скоростями передачи данных и т.д.).

Основными показателями, характеризующими сети мобильной связи пятого поколения являются:

- сверх-широкополосный мобильный доступ (enhanced Mobile Broadband, eMBB);

- ультранадежная связь с низкими задержками (Ultra-Reliable and Low Latency Communications, URLLC);
- массовое подключение различных датчиков и устройств «интернета вещей» (massive Machine Type Communications, mMTC);
- максимальная плотность подключенных к сети в городских условиях устройств интернета вещей - 1 000 000 устройств/км²;
- автономная работа устройств интернета вещей без подзарядки аккумулятора в течение 10 лет;
- максимальная скорость передачи данных > 10 Гбит/с.

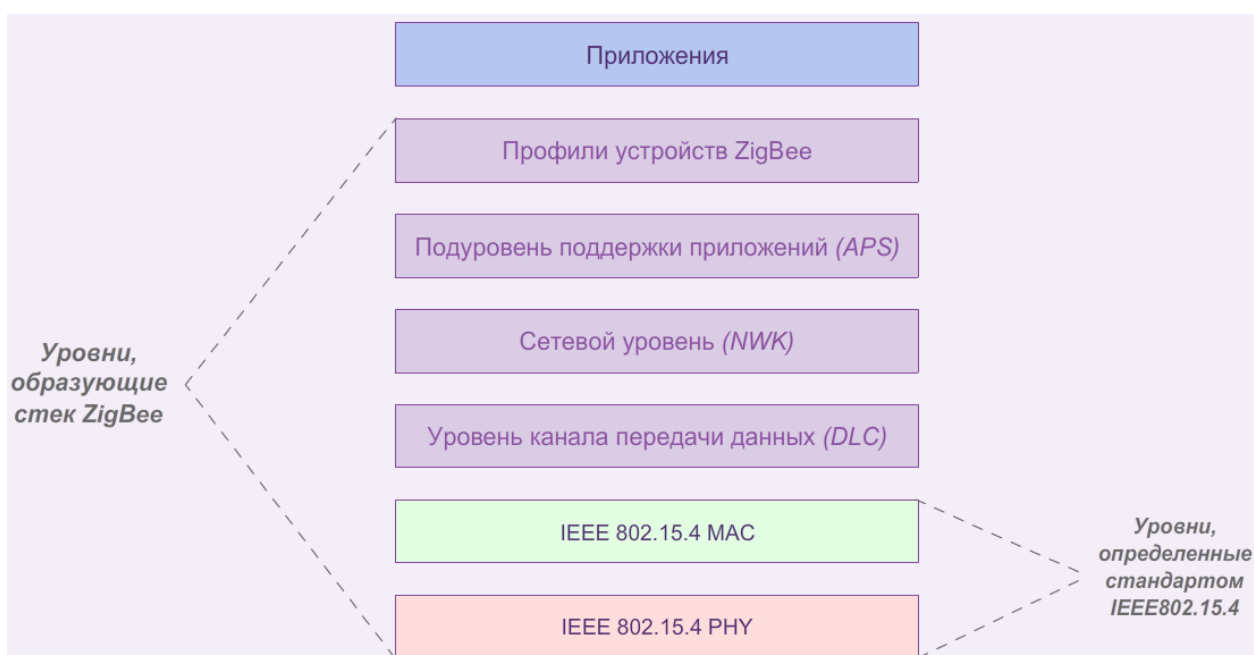
13. КРАТКАЯ ХАРАКТЕРИСТИКА СЕТЕЙ WPAN. ПРИНЦИПЫ РАБОТЫ ZIGBEE.

Беспроводные персональные сети WPAN (Wireless Personal Area Network) и беспроводные локальные сети WLAN (Wireless Local Area Network) – это сети, задачей которых является сбор и передача информации от интернет вещей и их взаимодействие. Такие сети могут использоваться как автономно, для объединения отдельных устройств между собой и решения задач в рамках сети, так и для передачи данных в сети более высокого уровня и реализации приложений на уровне глобальной сети.

К технологиям/стандартам, используемым на сетях WPAN, относятся такие, как ZigBee, 6LoWPAN, Wi-Fi, Thread, BLE 4.2 (BluetoothMesh), Z-Wave, Wireless RF и другие, характеризующиеся низким потреблением энергии и небольшим радиусом приема сигналов.

Рассмотрим один стандарт WPAN – ZigBee.

ZigBee, прежде всего, используется в системах безопасности, охранных устройствах, системах освещения помещений и объектов инфраструктуры, системах вентиляции, автоматизации, кондиционирования.



Стек ZigBee представляет собой иерархическую модель, построенную по принципу семиуровневой модели взаимодействия открытых систем OSI (Open Systems Interconnection). Спецификация стека определяет какими свойствами должны обладать устройства, из которых строится сеть, каким образом пакет информации передается от одного узла сети к другому, как новое устройство подключается к сети, и кто в сети является главным, а кто подчиненным.

Стек включает в себя уровни стандарта IEEE 802.15.4, отвечающие за реализацию канала связи, программные сетевые уровни и уровни поддержки приложений.

- Физический уровень IEEE802.15.4 PHY, уровень доступа к среде IEEE802.15.4. MAC.

На уровнях PHY и MAC используется стандарт IEEE 802.15.4. IEEE 802.15.4-2003, который используется и для других сетей WPAN. IEEE 802.15.4 определяет физические параметры передатчика: диапазон частот (868 МГц, 915 МГц, 2,4 ГГц); число радиочастотных каналов (1 -16); тип модуляции (QPSK и BPSK).

Уровень PHY осуществляет: активизацию/деактивизацию приемопередатчика; выбор физического частотного канала; индикацию качества связи; оценку свободного канала для реализации протокола множественного доступа к среде с контролем несущей и предотвращением коллизий.

- MAC уровень - отвечает за надежную связь устройства с непосредственными соседями, определяет число адресуемых устройств, описывает механизмы проверки и подтверждения целостности принятых данных, процедуры оценки качества канала и алгоритм предотвращения коллизий (ограничение на одновременную работу нескольких передатчиков).

- Уровень канала передачи данных (DLC) обеспечивает формирование пакетов данных и управление потоками информации.

- Сетевой уровень (NWK) обрабатывает сетевые адреса и маршрутизацию по вызовам MAC: запуск сети (если устройство является координатором); присвоение сетевых адресов; добавление и удаление сетевых устройств; маршрутизация сообщений; применение политики безопасности; осуществление поиска маршрутов.

- Подуровень поддержки приложений (APS) - отвечает за предоставление данных приложениям и профилям устройства ZigBee. Подуровень также управляет присоединениями в сети ZigBee и хранит данные о таких присоединениях в своей таблице.

- Профили устройств определяют устройства в соответствии с их назначением. В ZigBee поддерживается режим «профилей устройств» или профилей для различных датчиков, которые могут «понимать» друг друга, т.е. совместимы на уровне стека протокола и могут передавать и принимать информацию.

Устройства ZigBee стандартизованы не только на сетевом уровне, но и на уровне приложений, т.е. беспроводные узлы различных производителей могут понимать друг друга и на уровне приложения. Для этого разработана библиотека кластеров ZigBee (ZCL), в которой определены профили с набором стандартных устройств, таких как выключатели, блоки управления освещением, интерфейс для подключения датчиков, счетчиков и т.п. Стандартный профиль описывает стандартные команды и поведения конкретного устройства. Сеть ZigBee может быть построена из устройств различных профилей, но понимать друг друга могут только устройства одного профиля, например, выключатель и электрическая лампочка. В ZigBee разработаны профили для устройств следующего назначения: домашняя автоматизация; энергетика; строительство, автоматизация коммерческого строительства; телекоммуникационные приложения, медицина, игрушки. Если какие-то профили не заложены в стандарт, они могут быть созданы дополнительно.

- Уровень приложений состоит из фермы приложений (Application Framework), объекта устройства ZigBee (ZD0).

Ферма приложений (Application Framework) содержит описание порядка создания профилей в стеке ZigBee, гарантирующего их совместимость, а также определяет стандартные типы данных для профилей, дескрипторы, помогающие в обнаружении служб, форматы кадров для транспортировки данных и значения пар ключей. Это позволяет быстро разрабатывать простые профили на основе атрибутов.

Объекты приложений (Application Objects) – программные модули, управляющие устройствами ZigBee в конечных точках. Конечная точка 0 зарезервирована для объекта устройства ZigBee (ZD0).

Объект устройства ZigBee (ZigBee Device Object – ZD0):

- определяет роль устройства ZigBee: координатор, маршрутизатор или конечное устройство;
- инициирует запросы поиска и присоединения и/или отвечает на такие запросы;
- устанавливает безопасную связь между устройствами ZigBee.

Сети ZigBee поддерживают топологии mesh, «точка-точка», «кластер», «звезда».

Наибольший интерес представляет mesh-топология, в которой за счет наличия избыточных связей между устройствами повышается ее надежность. Поэтому далее будем рассматривать сеть ZigBee этой топологии.

Сеть строится на базе следующих элементов: координатор, маршрутизаторы и конечные устройства.

- Координатор формирует сеть, выполняет функции центра управления сетью, задает настройки в процессе присоединения устройств к сети, служит шлюзом для передачи данных во внешние сети, а также выполняет функции маршрутизатора. Координатор по умолчанию является Trust-центром, который устанавливает политику безопасности в сети ZigBee. Trust-центр дает разрешение на подключение устройств и работает с ключами шифрования

(обновление ключей, уведомление узлов об обновлении ключа). В целях обеспечения безопасности ZigBee использует стандарт шифрования AES-128.

- Маршрутизатор транслирует пакеты, осуществляет динамическую маршрутизацию, восстанавливает маршруты при перегрузках в сети или отказе какого-либо устройства. При формировании сети маршрутизаторы присоединяются к координатору или другим маршрутизаторам и могут присоединять дочерние устройства – маршрутизаторы и конечные устройства.

- Конечное устройство может принимать и отправлять пакеты, но не занимается их трансляцией и маршрутизацией. Конечные устройства могут подключаться к координатору или маршрутизатору, но не могут иметь дочерних устройств. Именно конечные устройства имеют дело с датчиками, локальными контроллерами и исполнительными механизмами.