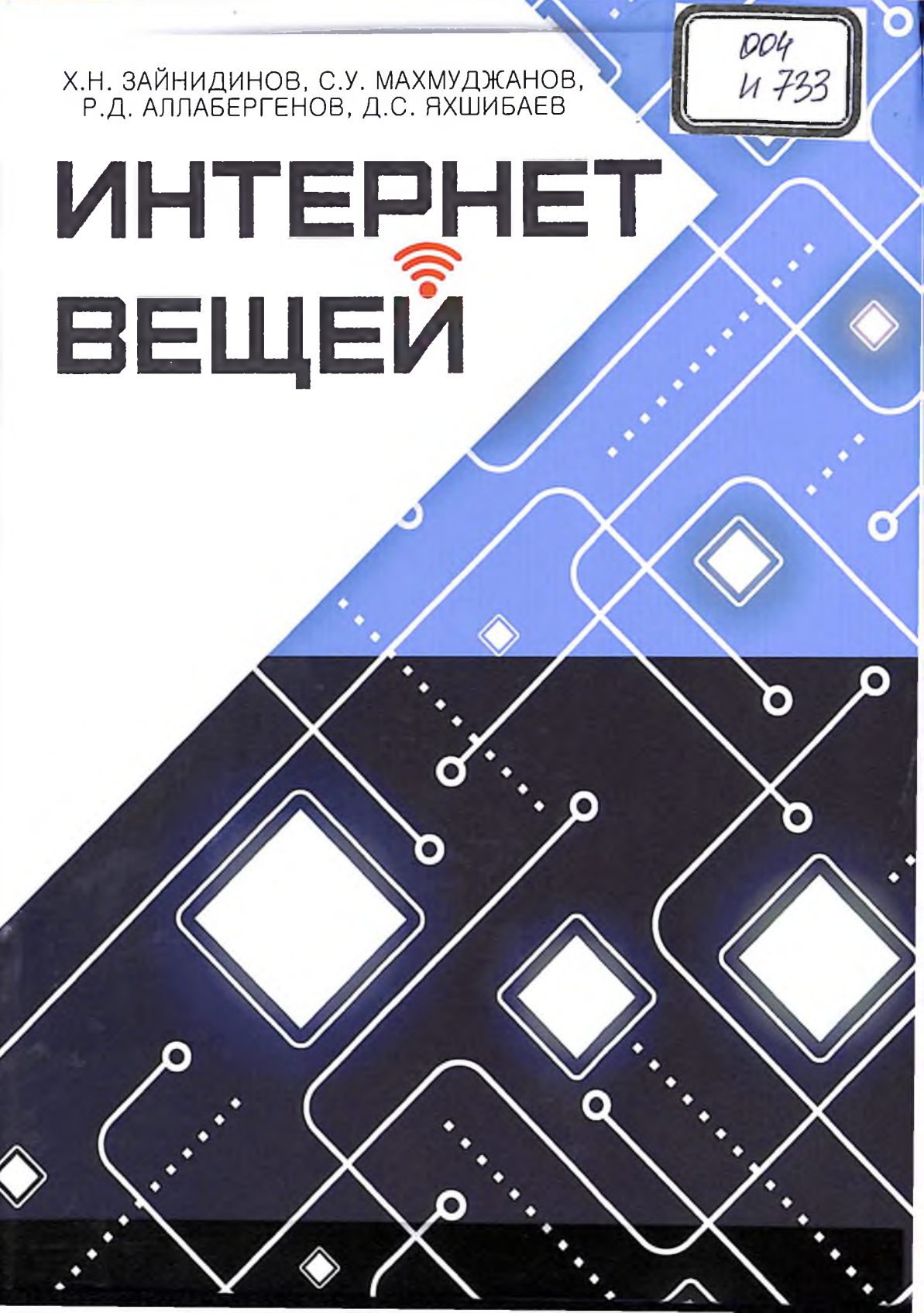
Х.Н. ЗАЙНИДИНОВ, С.У. МАХМУДЖАНОВ,
Р.Д. АЛЛАБЕРГЕНОВ, Д.С. ЯХШИБАЕВ

ИНТЕРНЕТ ВЕЩЕЙ



МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИМЕНИ МУХАММАДА АЛ-ХОРАЗМИЙ

Х.Н. ЗАЙНИДИНОВ, С.У. МАХМУДЖАНОВ,
Р.Д. АЛЛАБЕРГЕНОВ, Д.С. ЯХШИБАЕВ

ИНТЕРНЕТ ВЕЩЕЙ (IoT)

(Учебное пособие)

ТАШКЕНТ – 2019

УДК: 004.738.5(075.8)
ББК: 32.973.202

Х.Н. Зайнидинов, С.У. Махмуджанов, Р.Д. Аллабергенов, Д.С. Яхшибаев Интернет вещей (учебное пособие). Т., «Aloqachi», 2019, 220 стр.

ISBN 978–9943–5897–0–4

Пособие направлено на обучение студентов с систематическими профессиональными знаниями и эффективными практическими навыками в области компьютерных технологий, коммуникационных сетей и информационных технологий, которые предоставляют широкий спектр приложений в Интернете вещей.

Пособие дает студентам сильные навыки проектирования сенсорных сетей и планирования сетей для IoT. Темы включают в себя: введение в IoT. Понимание IoT с точки зрения рынка. Управление данными и знаниями, а также использование устройств в технологии IoT. Понимание архитектуры IoT и применение IOT в различных технологиях.

Пособие предназначено для профессорско-преподавательского состава и студентов высших, средне-специальных и профессиональных учебных заведений.

Пособие издано на основе постановления учебно-методического совета Ташкентского университета информационных технологий имени Мухаммада ал-Хоразмий.

УДК: 004.738.5(075.8)
ББК: 32.973.202

Рецензенты: Маматов А.З. – д.т.н. профессор.
Джуманов Ж.Х. – д.т.н. профессор.

ISBN 978–99432–5897–0–4

ВВЕДЕНИЕ

Влияние технологий на нашу жизнь трудно переоценить. Колесо дало нам возможность двигаться и перевозить людей и предметы. Его изобретение изменило все вокруг — от сельского хозяйства до политических систем. Электрические лампочки осветили дома и предприятия, и это навсегда изменило то, как архитекторы проектируют сооружения, а градостроители планируют целые города. Автомобиль позволил человеку быстро перемещаться между исходным и конечным пунктом, что помогло ему переосмыслить ритм жизни и работы. А компьютер открыл нам цифровой мир, в котором данные можно хранить и передавать самыми разнообразными и необычными способами. Это изменило то, как люди действуют…и взаимодействуют.

Каждое из перечисленных изобретений, а также бесчисленное множество других — от холодильников и швейных машинок до телефонов, печатных машинок и фотоаппаратов — постепенно влились в общество и вызвали огромное количество политических, социальных и практических перемен.

Они превратились в вещи, которыми люди пользуются каждый день - и которые по большей части воспринимаются как нечто само собой разумеющееся. Также они изменили то, как люди решают свои многочисленные повседневные задачи, и позволили им переосмыслить способы взаимодействия, коммуникации и выполнения своей ежедневной работы.

В 1957 г. Джо Болен, Джордж Бил и Эверетт Роджерс из Государственного университета штата Айова ввели понятие кривой внедрения технологий. Они выдвинули идею о том, что любой новый продукт или решение движется по относительно предсказуемой траектории, похожей на гауссову кривую. Первые разработчики технологии называются новаторами, на втором этапе появляются первопроходцы, за ними следуют массы, а уже за массами — поздние последователи. Такая схема работает до сих пор, хотя в последние пару десятилетий этот жизненный цикл ускорился до сверхсветовой скорости. В некоторых случаях эта схема вместо нескольких лет или десятилетий укладывается в несколько месяцев.

В эпицентре этой ударной волны находится Интернет вещей — причем он только начинается. Когда-нибудь он станет практической основой жизни и бизнеса, пока же этот тренд затрагивает в основном новаторов и первопроходцев. Подключенные друг к другу устройства существовали со времен появления первых компьютерных сетей и бытовой электроники. Однако пока не появился интернет, никому не приходило в голову, что связь может быть глобальной. В 1990-х гг. исследователи выстраивали теоретические построения о том, как сочетание человека и машины даст совершенно новую форму коммуникации и взаимодействия.

А теперь эта реальность разворачивается у нас на глазах. Хотя и не известно, что было той искрой, из которой разгорелось пламя этой революции, можно с уверенностью сказать, что решающим событием стал выпуск компанией Apple в 2007 г. устройства под названием iPhone. Смартфоны попали в руки масс. Благодаря этому стала возможна связь в реальном времени между двумя точками на карте посредством устройства, которое можно держать в руке.

В это же время развились технологии радиочастотной идентификации (RFID), далеко вперед шагнули сенсорные технологии, ускорились процессы минимизации объемов, и совершило гигантский скачок программное обеспечение. Сближение этих технологий — наряду с практически повсеместным распространением беспроводных сетей и облачных компьютерных систем — привело к появлению идеи о роботах-насекомых и роботах-животных, нанороботах и микророботах, которые могут функционировать внутри человека, и дронах, выполняющих различные задания на большой высоте. Нет никаких сомнений, что мы вступаем в дивный новый мир встроенных технологий, предусматривающих полное погружение в виртуальную среду. Этот мир на первый взгляд больше похож на научную фантастику, нежели на научный факт.

Но этот мир — факт. Интернет вещей предлагает нам одновременно телескоп и микроскоп для того, чтобы взглянуть на когда-то незримый мир между людьми, машинами и физическими объектами. Присваивая объектам ярлыки и подключая их к Интернету, мы вдруг получаем возможность не

только следить за ними и собирать новые типы данных, но и, комбинируя всевозможные данные, постигать новые глубины информации и знаний. Знаний, о которых еще несколько лет назад никто и думать не смел.

Это как будто взять и с ходу переписать привычные законы физики. Интернет вещей соединяет искусственный интеллект и разум человека новыми, совершенно удивительными и подчас пугающими способами. Он способен осмыслить движения между предметами и среди предметов, включая людей, животных, транспортные средства, воздушные потоки, вирусы и многое другое. Он распознает взаимосвязи и предсказывает алгоритмы, которые слишком сложны для разума и чувств человека, — например, состояние моста или дороги; тенденции физических процессов, происходящих в атмосфере. Интернет вещей обеспечивает поддержку систем, работающих без наблюдения за ними человеком, и, во что уже трудно поверить, становится со временем умнее, изменяя свой базовый алгоритм.

Интернет вещей — это вторая волна мощной цифровой революции, которая началась с повсеместным распространением компьютеров в 1970–1980-х гг. И как все революции, она обещает, что будут и победители, и побежденные. Интернет вещей дает потребителю новые товары и услуги, и многие из существующих товаров и услуг оказываются безнадежно устаревшими. Технологии делают ненужными старые должности, но при этом приводят к появлению новых направлений деятельности. Взаимосвязанные системы влияют на сферу образования, государственное управление и бизнес, вносят существенные изменения в наши действия, поведение и социальные нормы. Новые технологии влияют абсолютно на все, начиная от процедур голосования на выборах до посещения ресторанов и способов проведения отпуска.

Тем не менее потенциальная польза не обходится без больших проблем и множества непредусмотренных последствий. В будущем могут появиться новые виды преступлений, оружия и методов ведения войны. Также, вследствие того, что люди становятся все дальше друг от друга — а этому в числе прочего способствуют новые технологии, — могут возникнуть серьезные политические и социальные проблемы. Обществу определенно

придется пересматривать взгляды на представления о конфиденциальности и безопасности.

В последующие годы Интернет вещей затронет практически каждый аспект нашей жизни. Но, поскольку рассмотреть каждый в настоящей книге не представляется возможным, мы лишь одним глазком заглянем в мир, который обещает изменить нашу жизнь быстрее и серьезнее, чем все прочие технические изобретения в истории человечества. Вопрос состоит не в том, наступит ли эпоха Интернета вещей, а в том, как именно это произойдет и насколько сильно изменит мир.

ГЛАВА I. ОБЩИЕ ПОЛОЖЕНИЯ ИНТЕРНЕТА ВЕЩЕЙ

1.1. Что такое Интернет вещей?

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 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 (Soft switch) 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 развитии 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, интернируюсь с интернет, позволяют обеспечить простую связь различных технических устройств («вещей»), число которых может быть огромным.

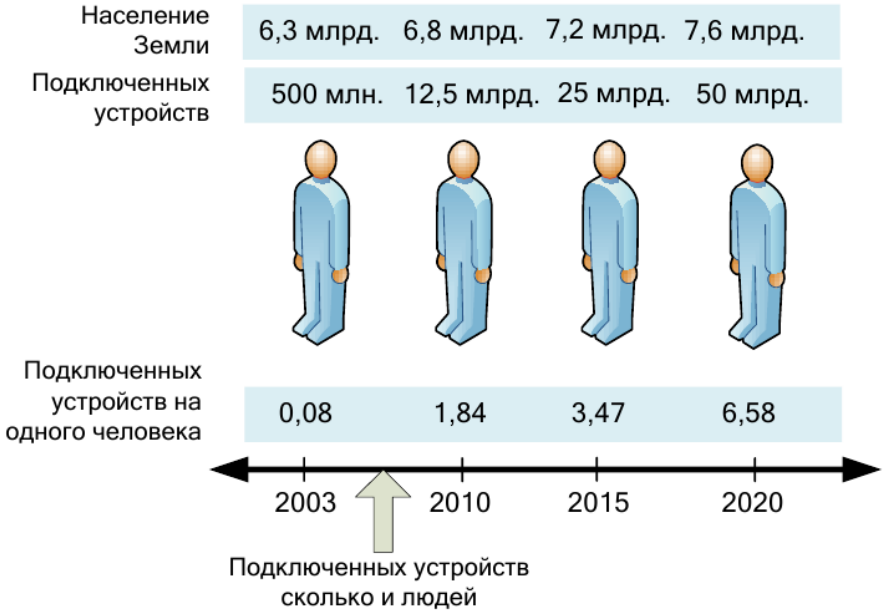


Рис. 1.1. Временная шкала изменения количества людей и предметов,
подключенных к интернету (*Источник: Cisco IBSG, 2011*)

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.

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.

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 Интернет вещей

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. 1.2).

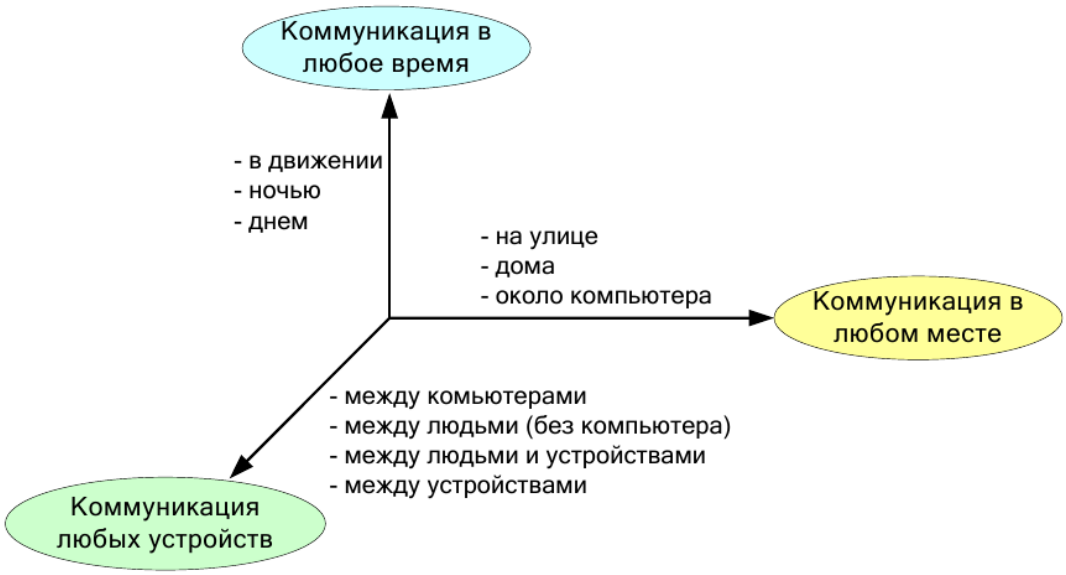


Рис. 1.2. Новое направление коммуникаций, реализуемое Интернетом вещей (*Источник: МСЭ-Т Y.2060*)

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.

Схема отображения физических и виртуальных вещей представлена на рис. 1.3. 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.

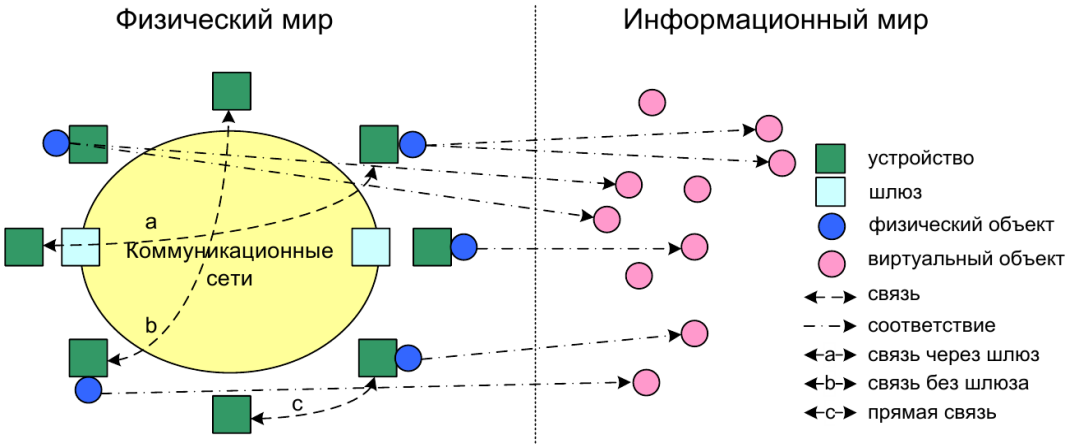


Рис. 1.3. Схема отображения физических и виртуальных вещей (источник: МСЭ-Т Y.2060)

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 Интернет вещей

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 инфо-коммуникаций, 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. 1.4):

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

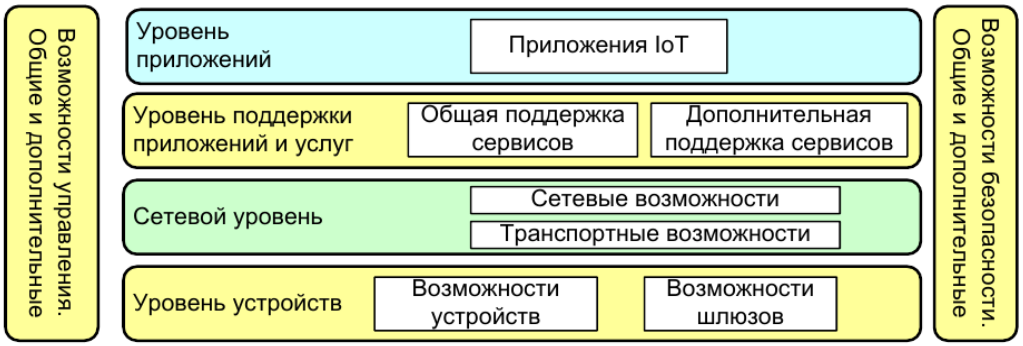


Рис. 1.4. Эталонная модель IoT согласно МСЭ-Т Y.2060

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. 1.5) несколько отличается от модели МСЭ (рис. 1.4), хотя она тоже является иерархической, но состоит уже из семи горизонтальных уровней, дополняемых двумя вертикальными (управление и безопасность), которые участвуют во всех процессах.

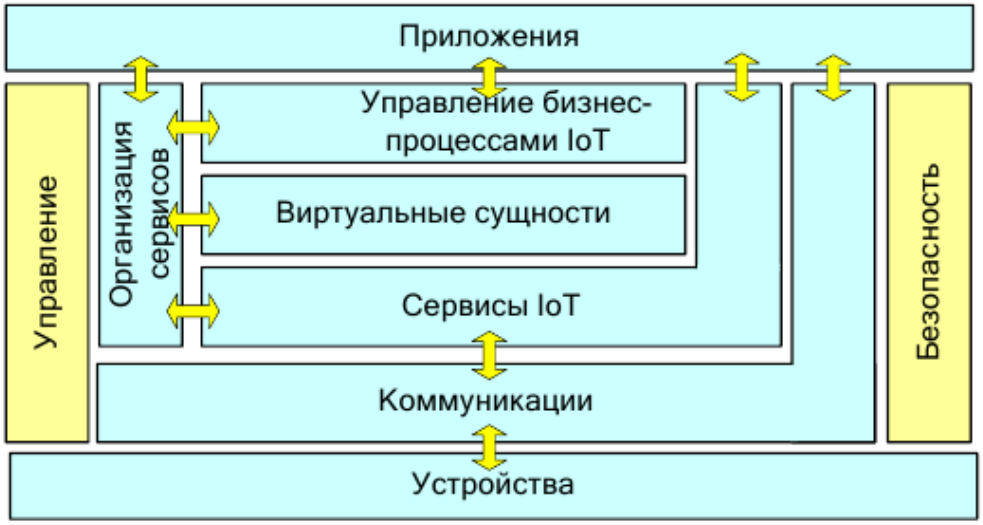


Рис. 1.5. Функциональная модель архитектуры IoT-A

Если обратиться к техническим особенностям модели на рис. 1.6, 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.

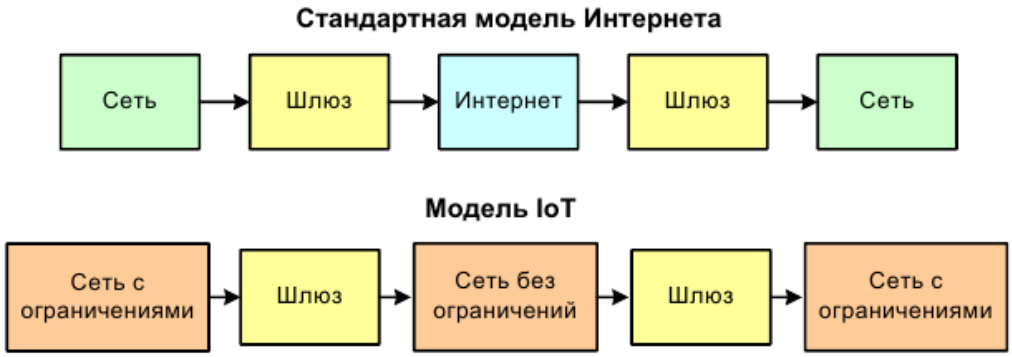


Рис. 1.6. Сравнение моделей передачи данных в Интернете и в IoT

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. 1.6.

1.4. Архитектура Интернет вещей

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. 1.7), описанных ниже.

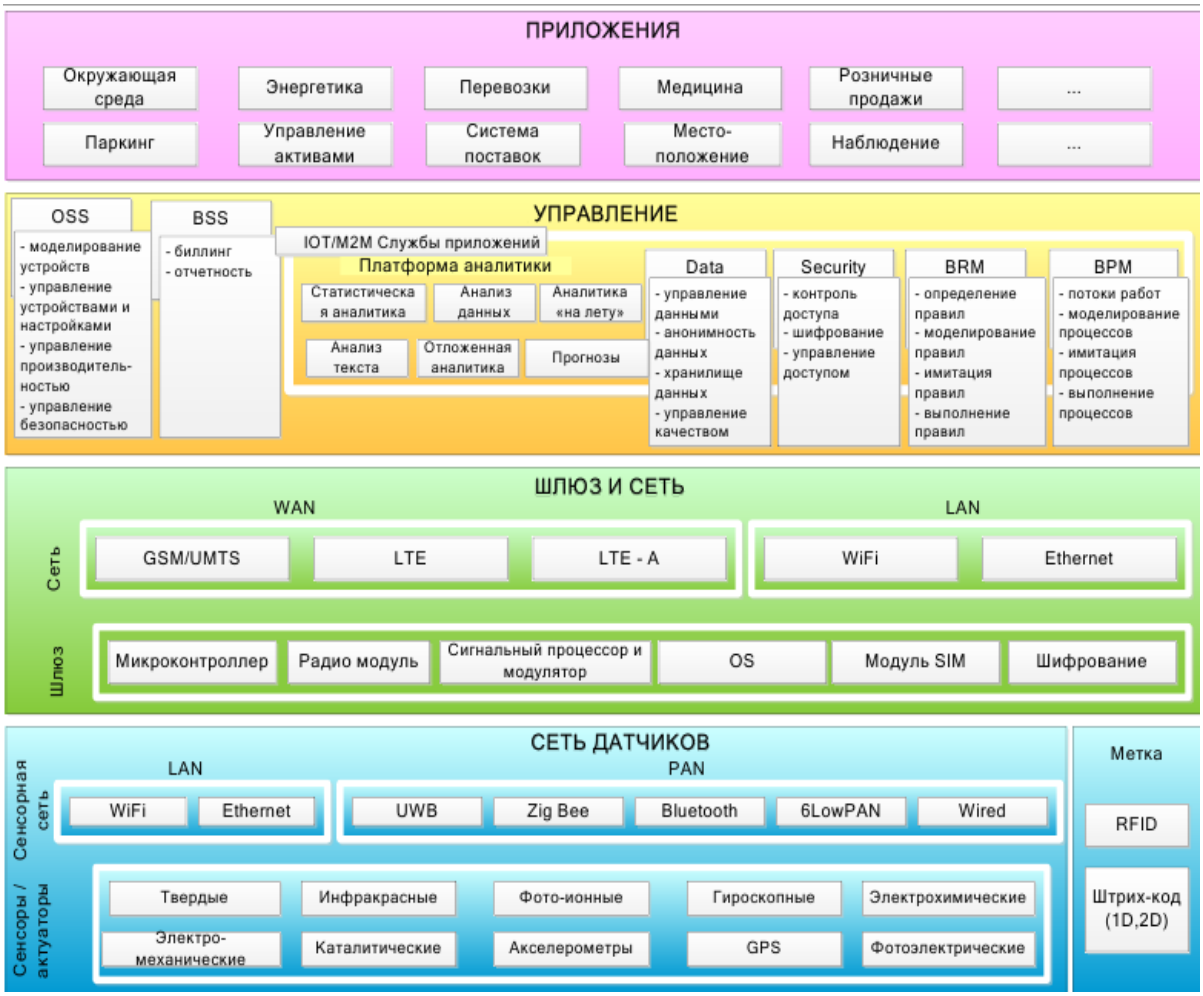


Рис. 1.7. Архитектура IoT

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 агрегатом 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.

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 (Hyper Text Transfer Protocol), стиль построения архитектуры распределенного приложения REST (Representational State Transfer) и др.

WoT - перспективное направление развития Всемирной паутины, объединяющее стандартизованные решения по использованию инфраструктуры Интернет для реализации взаимодействия между физическими объектами, изначально не имеющими отношения к компьютерам и вычислительным сетям.

Термин «Веб Вещей» (Web of Things, англ., WoT — аббр.) возник в конце XX века для обозначения концепции, включающей принципы, архитектурные стили и программные шаблоны, которые позволяют объектам реального мира стать частью Всемирной паутины.

Так же, как WWW (Application Layer) является прикладным сервисом Интернет (Network Layer), так и Веб Вещей обеспечивает сервисы прикладного уровня для создания приложений «Интернета вещей».

Фактически WoT предусматривает реализацию концепции IoT на прикладном уровне с использованием уже существующих архитектурных решений, ориентированных на разработку web-приложений.

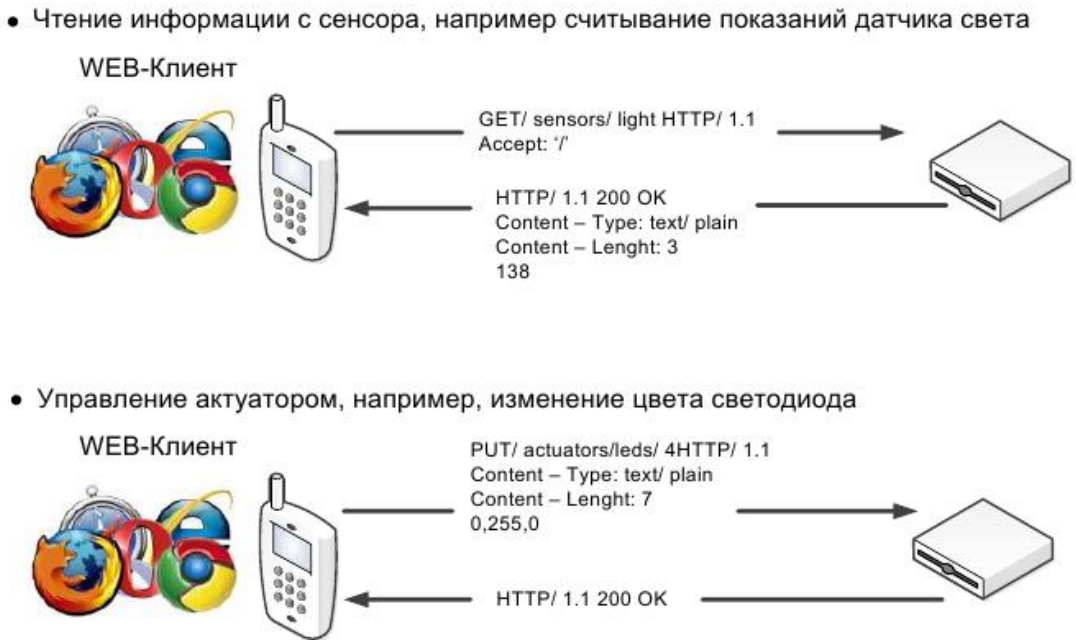


Рис. 1.8. Примеры веб-взаимодействия с устройствами сенсорной сети

Другими словами, данные с умных вещей или управление ими должно быть доступно через WWW-страницы. На рис. 1.8 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.

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.

Пока предпринимаются усилия по стандартизации, Веб Вещей остается набором готовых практических решений, которые могут быть классифицированы в соответствии с архитектурой системы.

Обобщенная архитектура (в текущем состоянии) может быть представлена в виде четырех уровней, включающих различные протоколы и шаблоны проектирования:

- Уровень доступа к устройствам;
- Уровень обнаружения;
- Уровень общего доступа;
- Уровень интеграции.

Далее кратко рассмотрим назначение каждого из логических уровней в архитектуре Веба Вещей.

Уровень доступа к устройствам.

Это базовый уровень, который обеспечивает возможности доступа вещей к глобальной сети и гарантирует доступ к их сервисам через программные Веб-интерфейсы. Этот уровень построен на основе двух шаблонов:

- Во-первых, все вещи обладают способностью публиковать свои сервисы через RESTful API (напрямую или через интеллектуальный шлюз). Поскольку REST поддерживается на уровне протокола HTTP 1.1, это легко реализуется на практике.
- Во-вторых, чтобы обойти ограничения клиент-серверной сути HTTP (чередование запросов клиента и ответов сервера), не очень подходящей событийно-управляемым приложениям в сетях беспроводных датчиков (являющихся частью Интернета вещей), разработчики предлагают использовать полнодуплексный протокол WebSocket.

Подключение устройств к Интернету может быть, как прямым, так и через интеллектуальные шлюзы.

Уровень обнаружения.

Задачи этого уровня — обеспечение «находимости» устройств: размещение информации о них в сети и возможности поиска.

Этот уровень находится под сильным влиянием семантического Веба и здесь могут использоваться такие спецификации как HTML5 Microdata, RDF/RDFa, JSON-LD или EXI. Это позволяет искать объекты как с помощью традиционных поисковых систем или онлайн-каталогов, а также устанавливать непосредственное взаимодействие между ними, используя небольшой набор хорошо известных стандартов и форматов.

Уровень общего доступа.

Веб Вещей во многом базируется на идее о том, что объекты-вещи размещают информацию о себе в Вебе и к ней можно применять шаблоны для обработки больших объемов данных.

Это, в свою очередь, возможно при условии эффективного распределения данных между сервисами. Уровень общего доступа гарантирует, что данные поступающие от вещей будут представлены в общий доступ эффективно и безопасно.

Уровень интеграции.

Роль последнего уровня заключается в интеграции сервисов и данных, представленных объектами Веба Вещей, с веб-инструментами вышележащего уровня (аналитическое ПО, приложения-агрегаторы и т.п.) для упрощения создания приложений, включающих и вещи, и виртуальные веб-сервисы.

Диапазон инструментов на этом уровне широк: от различных Javascript SDK до программируемых виджетов и инструментария для создания гибридных сервисов, позволяющих реализовывать приложения для Веба Вещей даже пользователям, не имеющим навыков программирования.

1.6. Интернет нано-вещей

Нано-технологии привели к разработке миниатюрных устройств, размеры которых варьируются от одного до нескольких сотен нанометров.

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. 1.9 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.

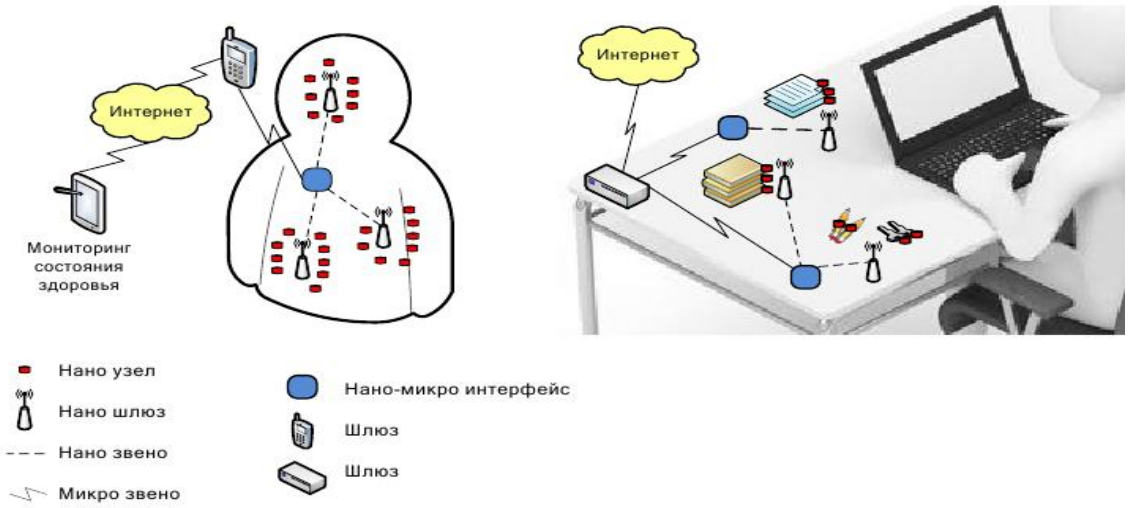


Рис. 1.9. Примеры архитектуры Интернета нано-вещей

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-микроинтерфейсы* – 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;
- само конфигурация 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.

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. 1.10).

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.

Рис. 1.10. Схема когнитивного управления

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 когнитивной и когнитивного управления применительно к интернету вещей.

1.8. Основные 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. 1.11.

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.

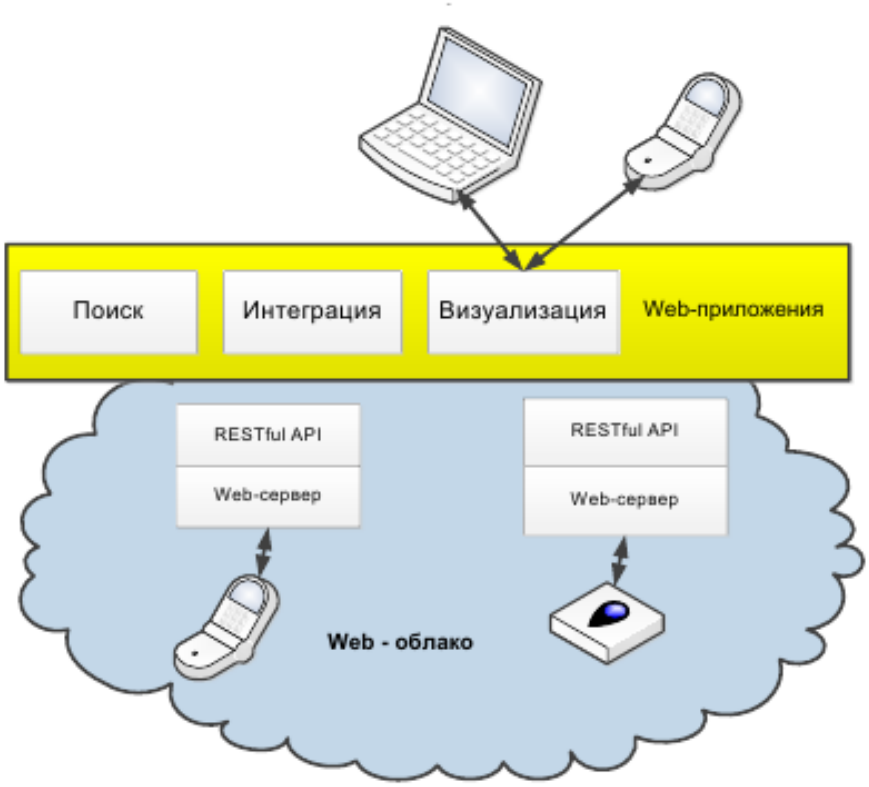


Рис. 1.11. Прямой доступ к IP-устройствам через API

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 Интернет-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. 1.12).

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.

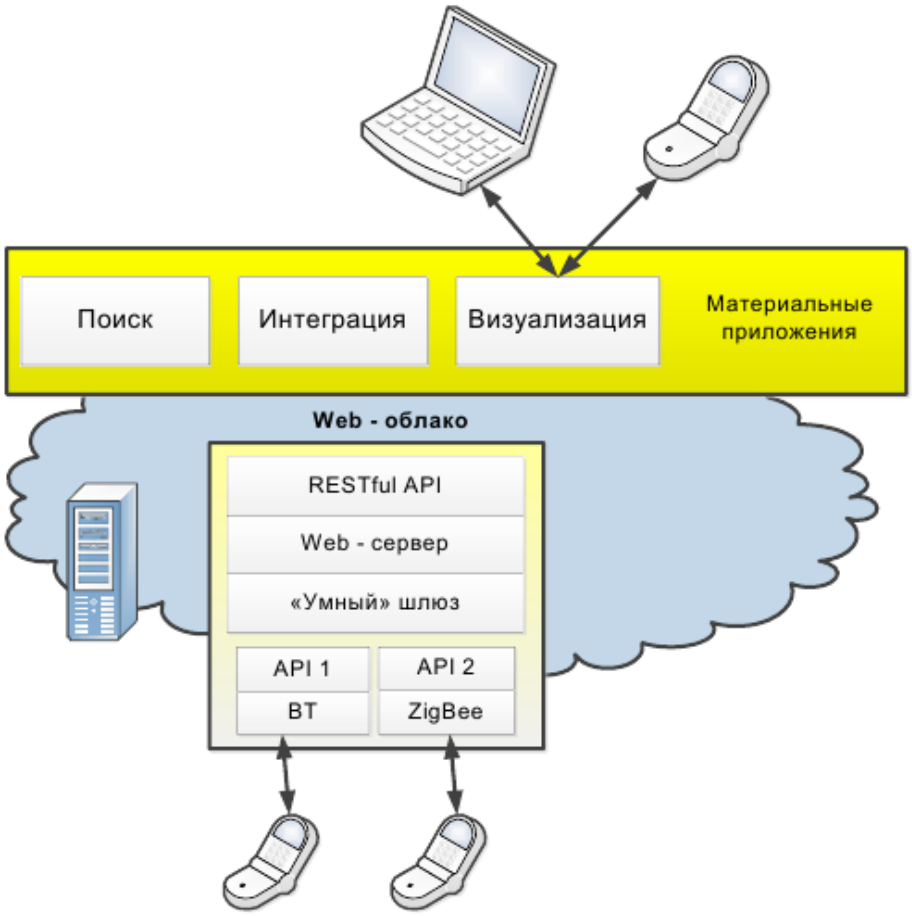


Рис. 1.12. Доступ к не IP-устройствам через интеллектуальный шлюз

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 хайпа1), 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. 1.13).

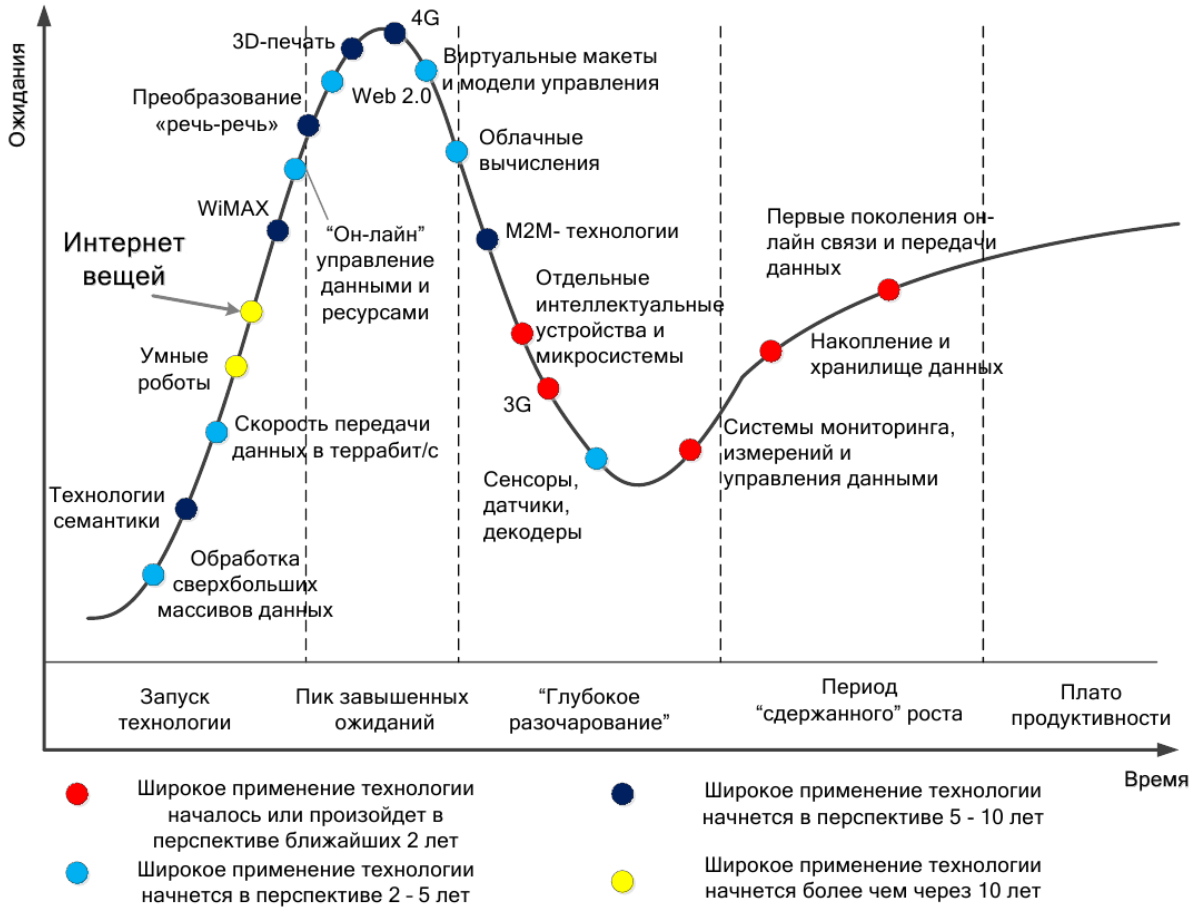


Рис. 1.13. Цикл зрелости технологий IoT (источник: Gartner, 2012)

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.

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.

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 интернет-вещами
11. Какова зрелость концепции IoT и ее базовых составляющих?

ГЛАВА II. ВЗАИМОДЕЙСТВИЕ IOT С 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. 2.1.

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).

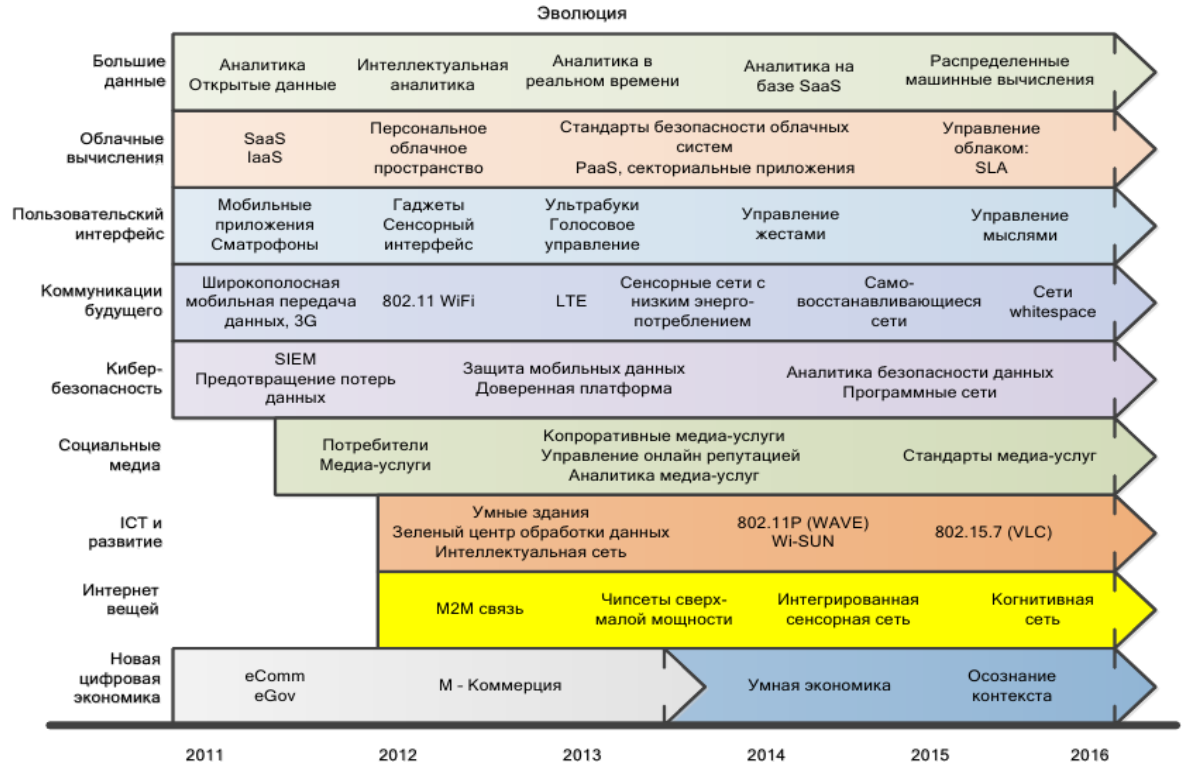


Рис. 2.1. Эволюция Интернета вещей и сопутствующих инфокоммуникационных технологий(*Источник: компания IDA, Сингапур, 2012*)

2.1. 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. 2.2).

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.

Рис. 2.2. Три основные характеристики больших данных

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.

2.2. 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. 2.3):

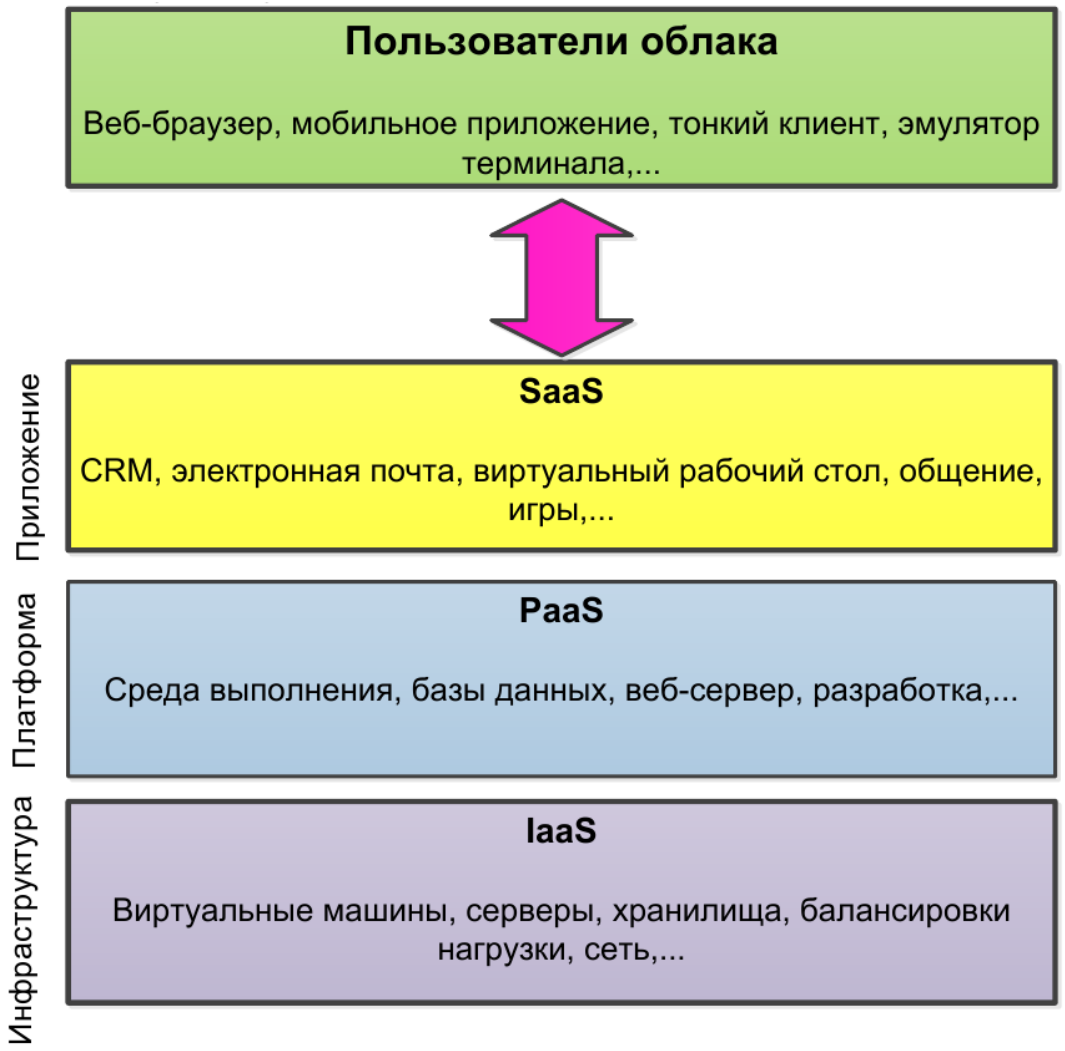


Рис. 2.3. Классы услуг облачных вычислений

- «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 коллективным или индивидуальным разработчикам.

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.

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.

2.3. 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.

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.

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.

2.4. Направления практического применения интернета вещей

На основе Интернета вещей могут быть реализованы всевозможные «умные» (smart) приложения в различных сферах деятельности и жизни человека (рис. 2.4):

- «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 не возобновляемыми 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.

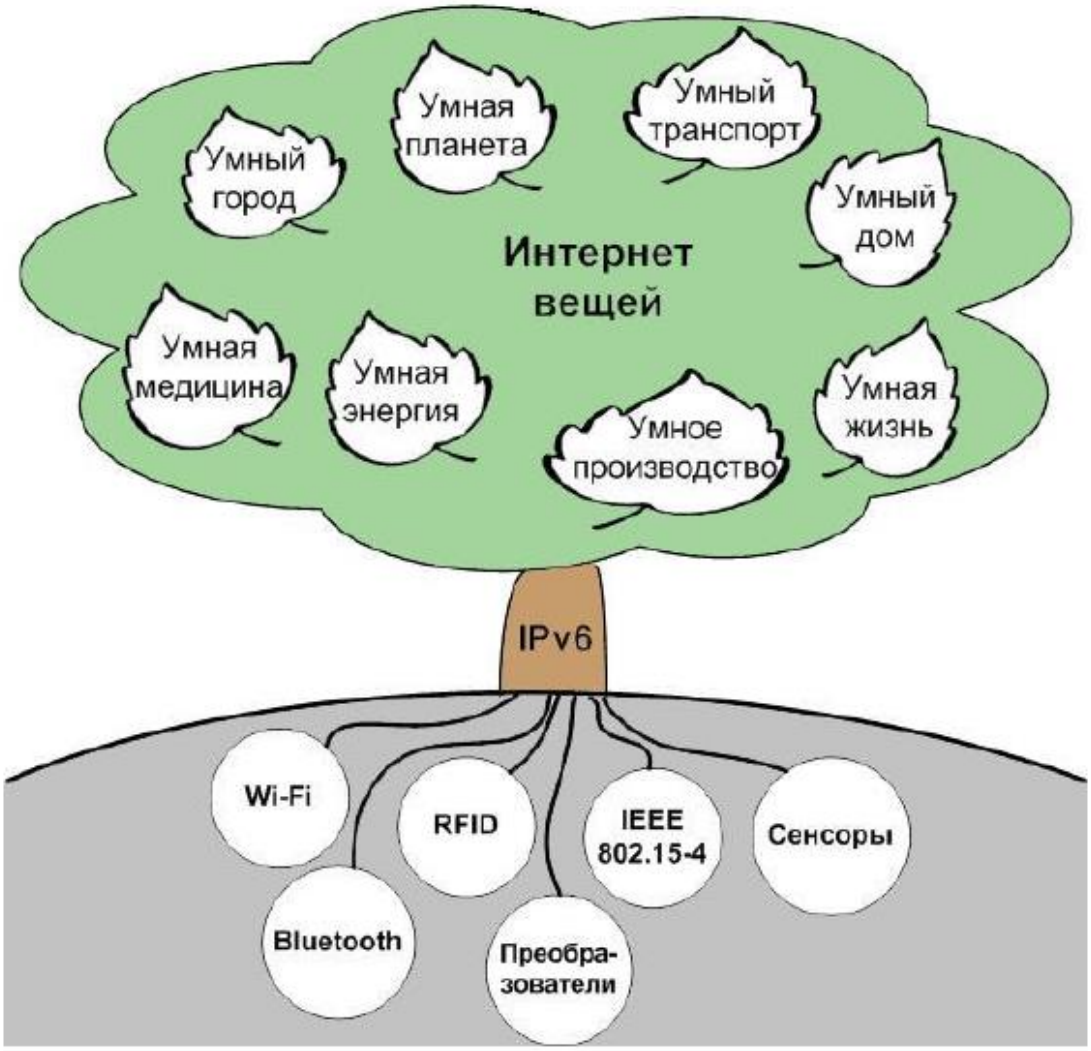


Рис. 2.4. Умные приложения на основе Интернета вещей

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.

Рис.2.5 показывает прогноз Gartner на 2020 год по распределению подключенных устройств.

Можно по-разному относиться к данному прогнозу, также, как и к множеству других, порой противоречивых оценок, но понимание общего тренда развития и многообразия применений IoT, а также превалирования количества подключений в бытовом интернете вещей (ЛЮДИ) относительно индустриального (БИЗНЕС) он дает.

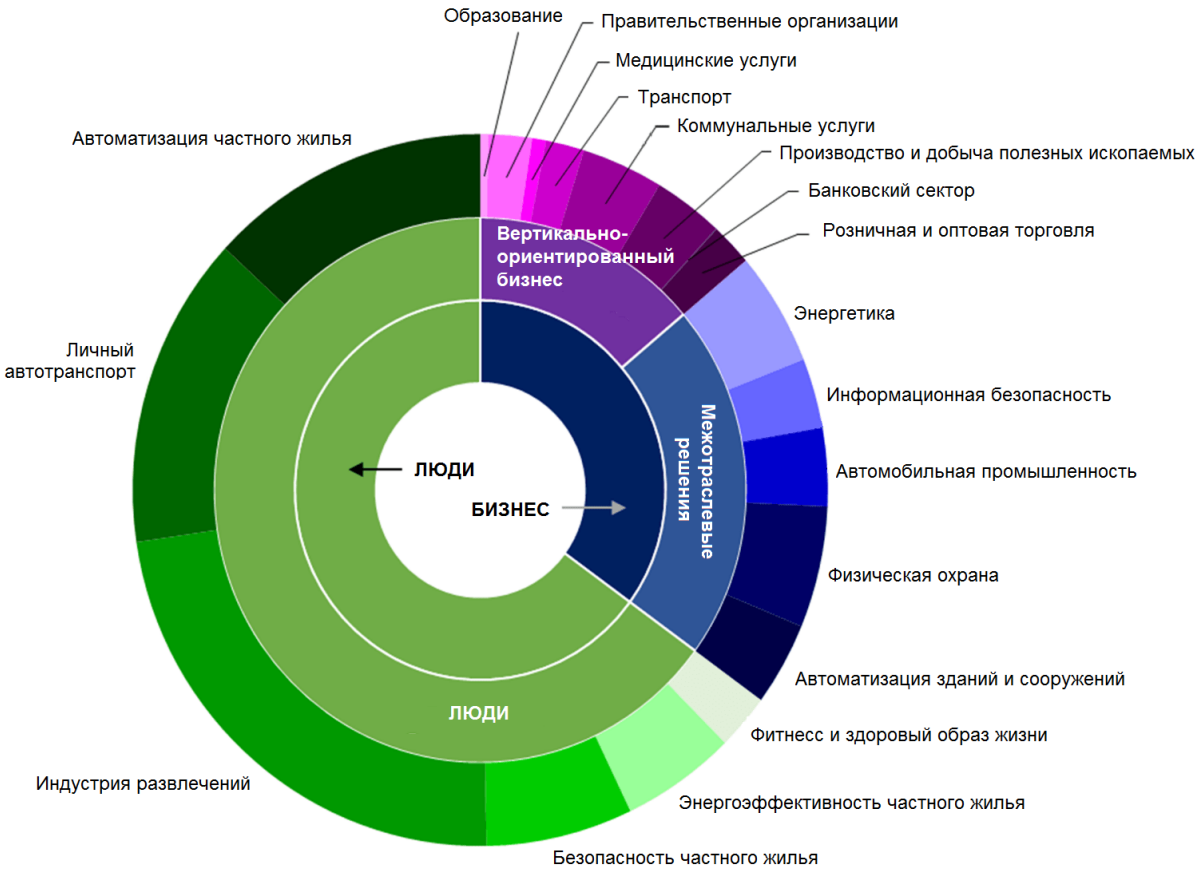


Рис. 2.5. Прогноз по секторам применения IoT к 2020 году: Gartner, April 2016

На рис. 2.6 приведены оценки перспектив Интернета вещей по числу подключенных устройств в целом на основании различных прогнозов. Как видно, оценки различаются на порядок. Так, к 2020 году, по мнению аналитиков Gartner число подключений достигнет 21 млрд. штук, а по мнению Intel – 200 млрд. Несмотря на существенное отличие оценок, можно констатировать высокие темпы роста рынка Интернета вещей, что вызывает серьезный интерес к этому сегменту со стороны промышленных компаний, крупных поставщиков устройств, разработчиков платформ и приложений, исследовательских агентств и национальных государственных органов.

Кейсы внедрения технологий «Интернета вещей» можно разделить на две большие группы:

1. Бытовой интернет вещей – решения, направленные на улучшение качества жизни и безопасности жителей, а также снижение их расходов по различным направлениям (категория «ЛЮДИ»).

2. Индустриальный «Интернет вещей», призванный повысить эффективность бизнеса, а также обеспечить развитие и внедрение новых услуг.

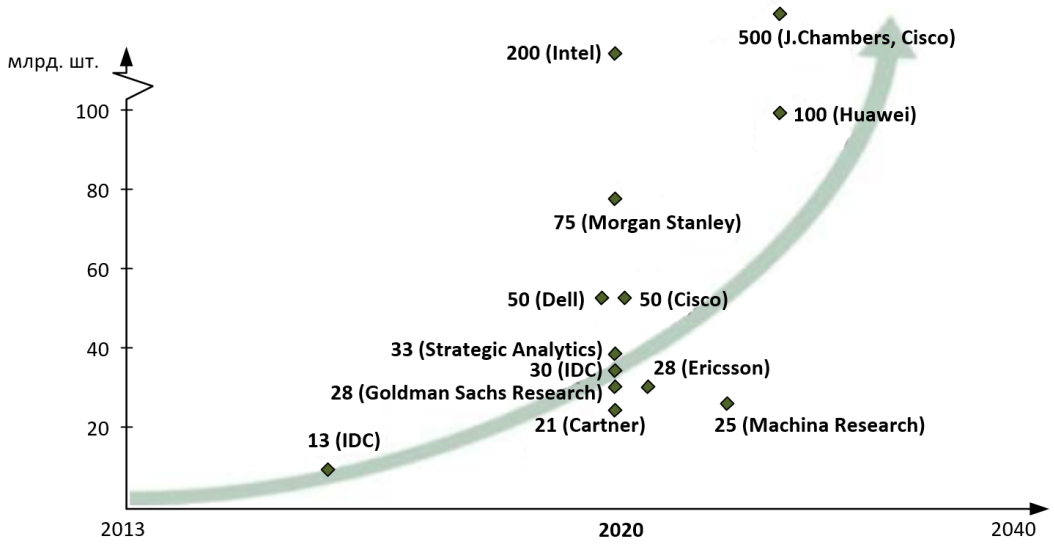


Рис. 2.6. Прогноз по количеству устройств: SigFox 2016

Рассмотрим несколько примеров (реальных и эмпирических):

- Автомобильные страховые компании, имеющие доступ к данным телеметрии транспортных средств, предлагают дисциплинированным водителям выгодные финансовые условия при приобретении страховых полисов;
- Коммунальные службы, получающие информацию с температурных датчиков, установленных в помещениях клиентов, предоставляют им скидки за сокращение потребления энергии в периоды пикового спроса;
- Мегаполисы управляют автомобильными потоками, путем гибкого регулирования режимов работы светофоров на основе текущей и исторической информации о загрузке автотрасс, а также внедряют системы контроля занятости парковочных мест;
- Логистические компании отслеживают перемещение и сохранность грузов;
- Медицинские копании внедряют системы удаленного контроля состояния здоровья пожилых и больных людей, а также системы автоматического введения лекарственных препаратов;

Компания «Rio Tinto» (Австралия) внедрила беспилотные карьерные самосвалы, управляемые из удаленного центра.

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.

Таблица 1/ Драйверы и барьеры рынка Интернета вещей

Драйверы	**Барьеры**
Стремительное развитие инфокоммуникационных технологий	Необходимость принятия общих стандартов
Мода на смартфоны, планшеты и	Медленный переход к

другие мобильные устройства	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	

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. 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.

Контрольные вопросы по главе 2

1. Укажите основные характеристики подхода «большие данные».
2. Что такое «облачные вычисления» и какие существуют модели «облаков»?

3. В чем суть идеи повсеместной компьютеризации?
4. Перечислите основные направления практического внедрения IoT.
5. Укажите основные движущие силы и барьеры на пути внедрения Интернета вещей.
6. Расскажите проблемы внедрения IoT.

ГЛАВА III. РАДИОЧАСТОТНАЯ ИДЕНТИФИКАЦИЯ RFID

3.1. 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. 3.1).

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.

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. 3.2).

Содержимое памяти специфично для каждой метки и позволяет идентифицировать носителя метки (человека или объект).

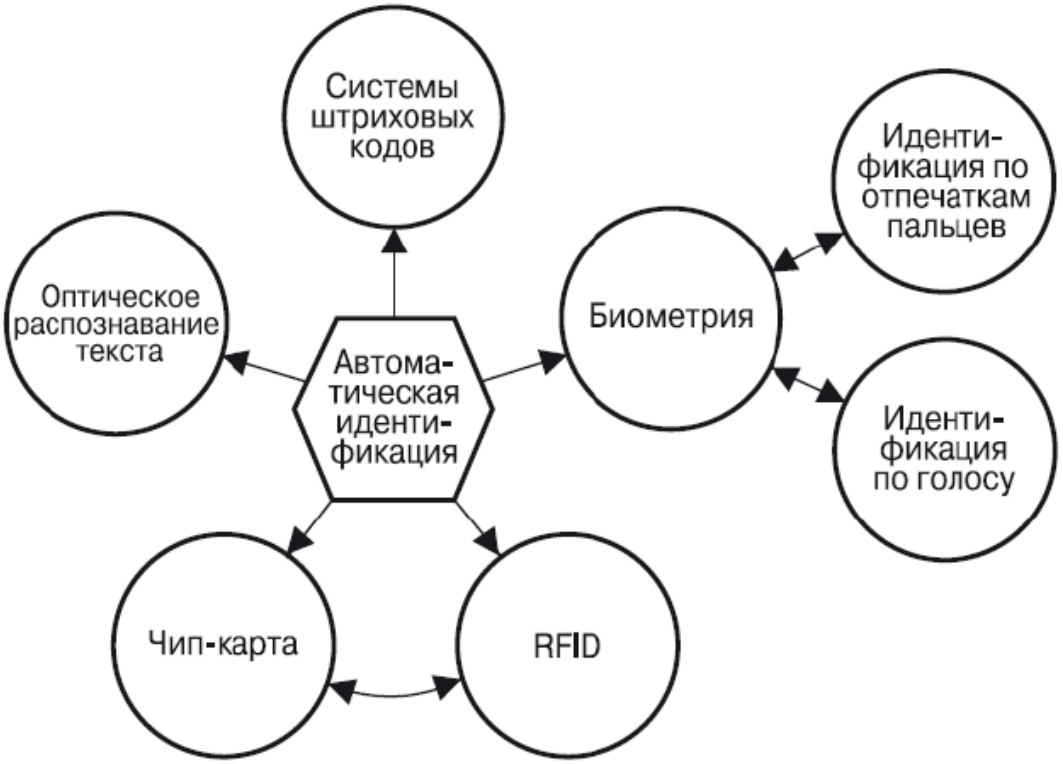


Рис. 3.1. Основные системы автоматической идентификации

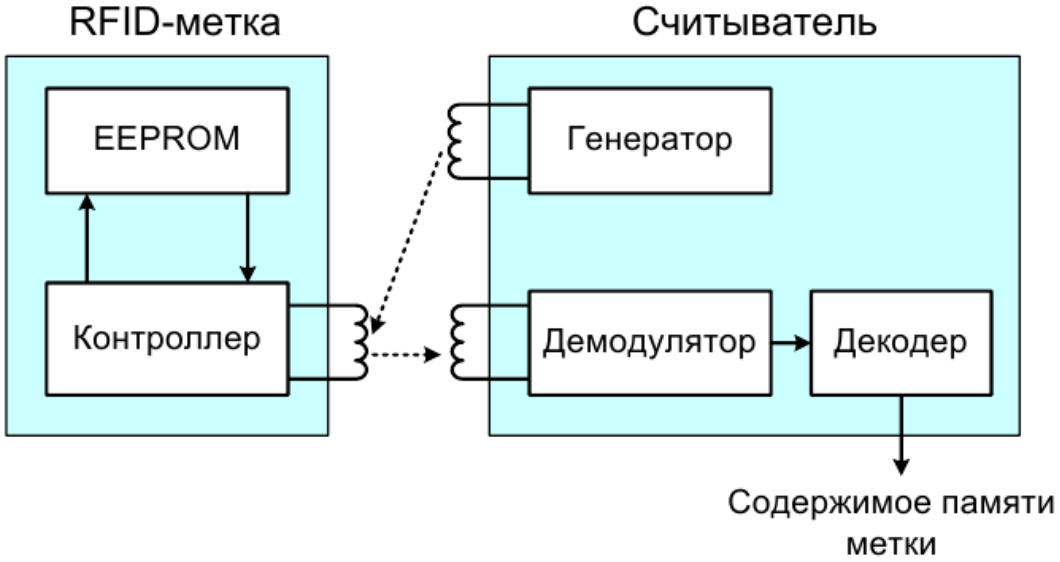


Рис. 3.2. Основные компоненты системы RFID

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. 1).

Табл. 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	Повышенная прочность и	Зависит от материала, на

окружающей среды	сопротивляемость	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	Возможно	Возможно
Использование стационарных и ручных считывателей	Да	Да
Возможность введения в тело человека/ животного	Возможно	Затруднена
Габаритные характеристики	Средние и малые	Малые
Стоимость	Средняя и высокая	Низкая

3.2. 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. 3.3). Первая –

интегральная схема для хранения и обработки информации, модулирования и демодулирования радиочастотного сигнала и некоторых других функций. Вторая – антенна для приема и передачи сигнала.

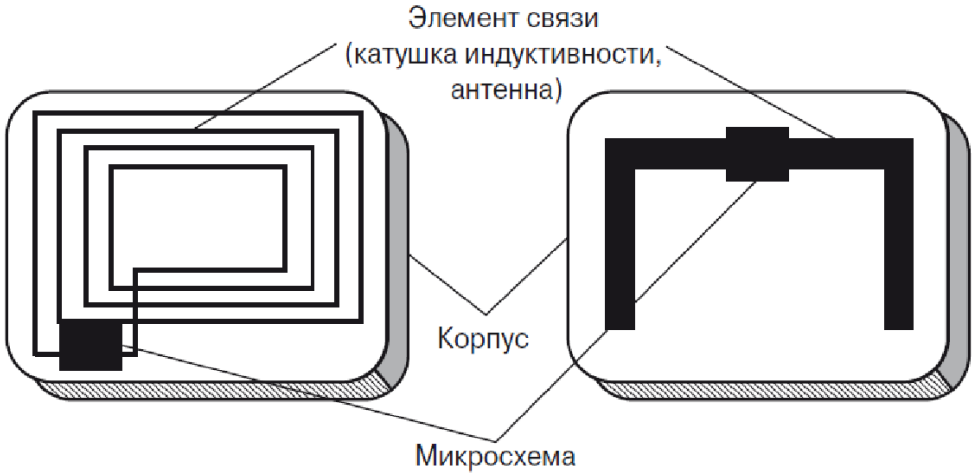


Рис. 3.3. Принципиальная схема RFID метки: слева – метка с индуктивной связью, справа – микроволновая метка с антенной-диполем

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.

RFID метки бывают пассивные и активные (рис. 3.4). 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. 3.4. 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. 3.5).

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.

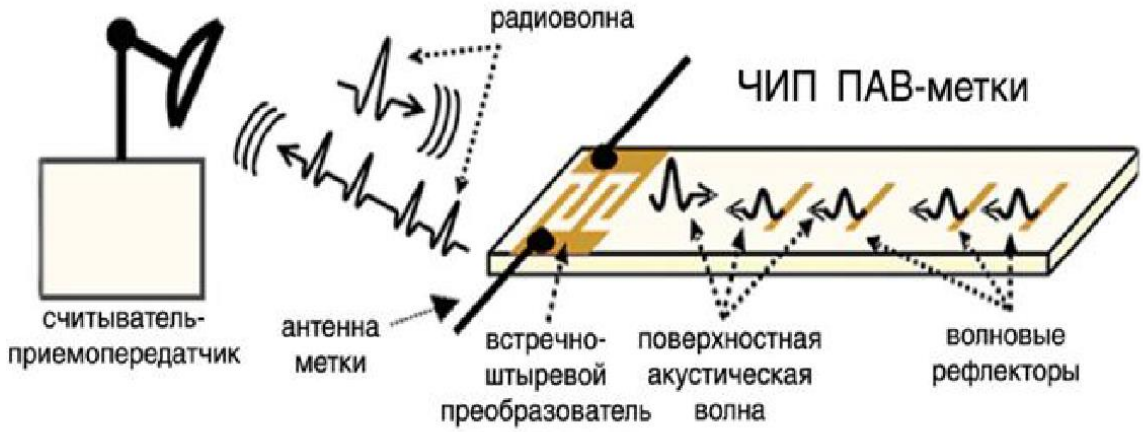


Рис. 3.5. Конструкция SAW-метки

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.

3.3. 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. 3.6).

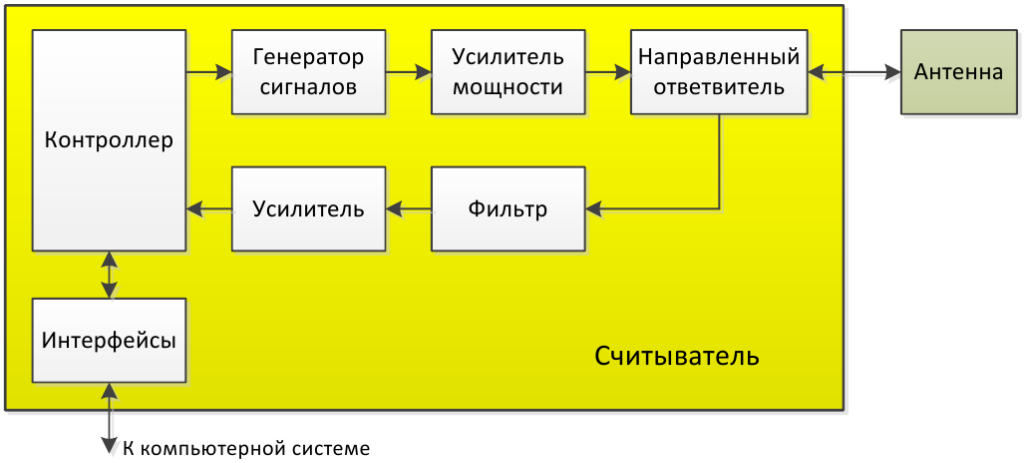


Рис. 3.6. Структурная схема RFID-считывателя

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.

Конструктивно считыватели бывают ручные, настольные и стационарные (рис. 3.7). 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, тереть, перезаписать информацию с метки. В основном они используется в библиотеках, на складах.

а) б) в)

Рис. 3.7. 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.

3.4. 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 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.

3.5. 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 радио идентификационных 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.

3.6. 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, без операторного отпуска 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 3

1. Каково назначение системы радио идентификации 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 IV. БЕСПРОВОДНЫЕ СЕНСОРНЫЕ СЕТИ WSN

4.1. 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. 4.1 (пунктиром показаны необязательные процессы).

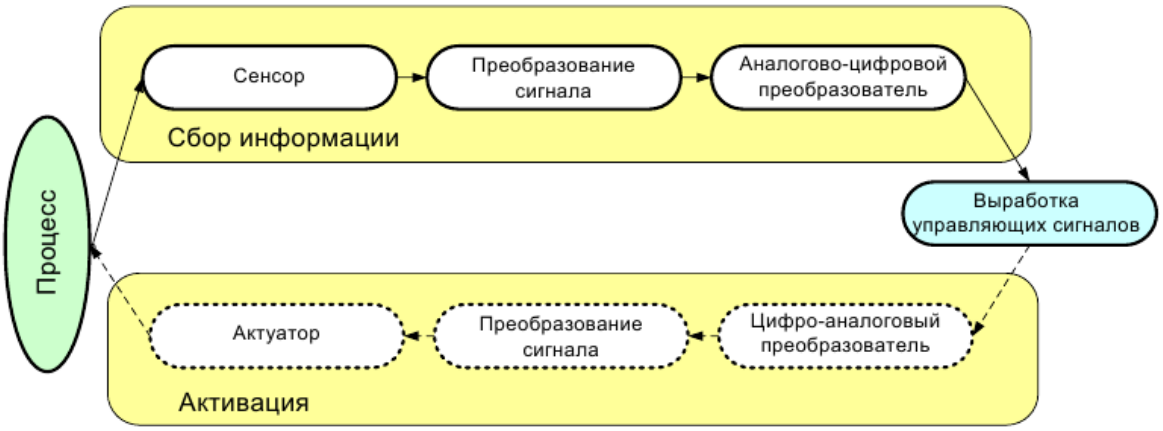


Рис. 4.1. Сбор данных и управление в сенсорных сетях

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. 4.2).

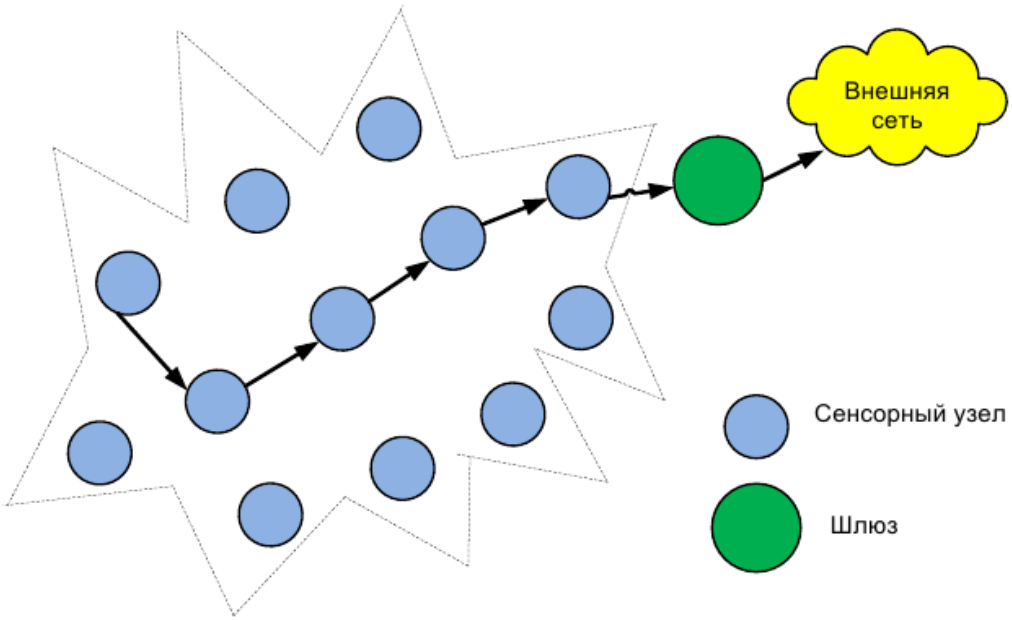


Рис. 4.2. Маршрутизация информации в сенсорной сети

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.

4.2. 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. 4.3).

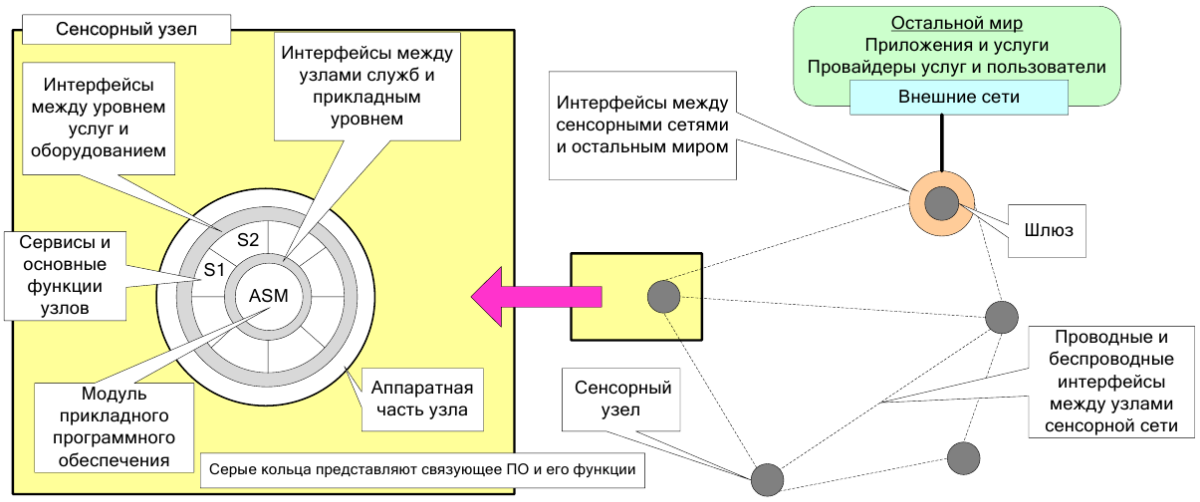


Рис. 4.3. Основные элементы и интерфейсы сенсорной сети

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).

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. 4.4):

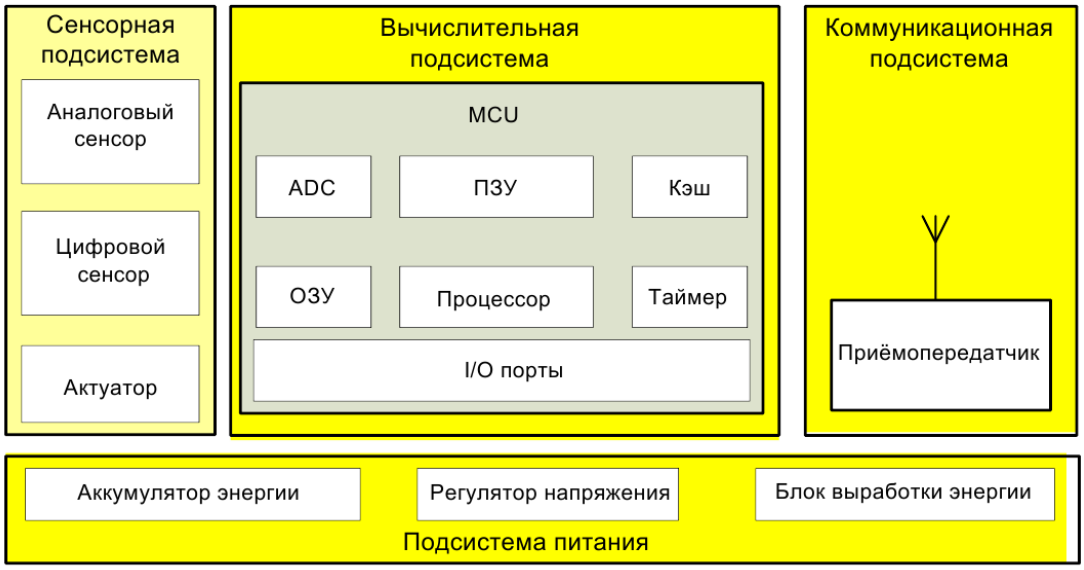


Рис. 4.4. Узел беспроводной сенсорной сети

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.

Датчики могут быть самыми разнообразными. Чаще других используются датчики температуры, давления, влажности, освещенности, вибрации, местоположения, реже – магнитоэлектрические, химические (например, измеряющие содержание CO, CO2, 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. 4.5.

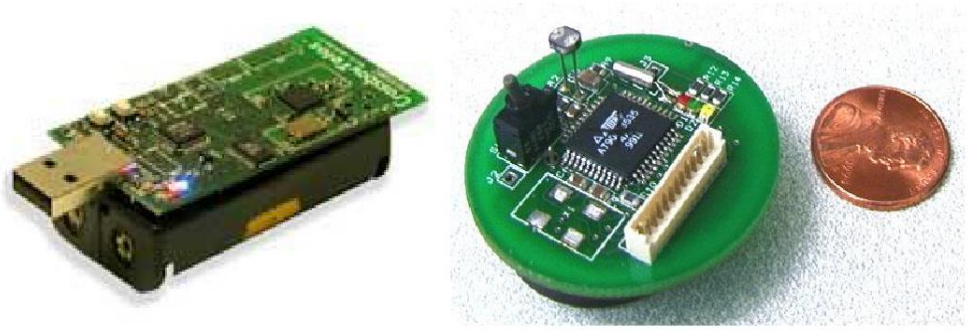


Рис. 4.5. Внешний вид сенсорных узлов

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.

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.

4.3. 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.

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).

Типы узлов БСС. Типовая архитектура БСС включает три типа узлов (рис. 4.6):

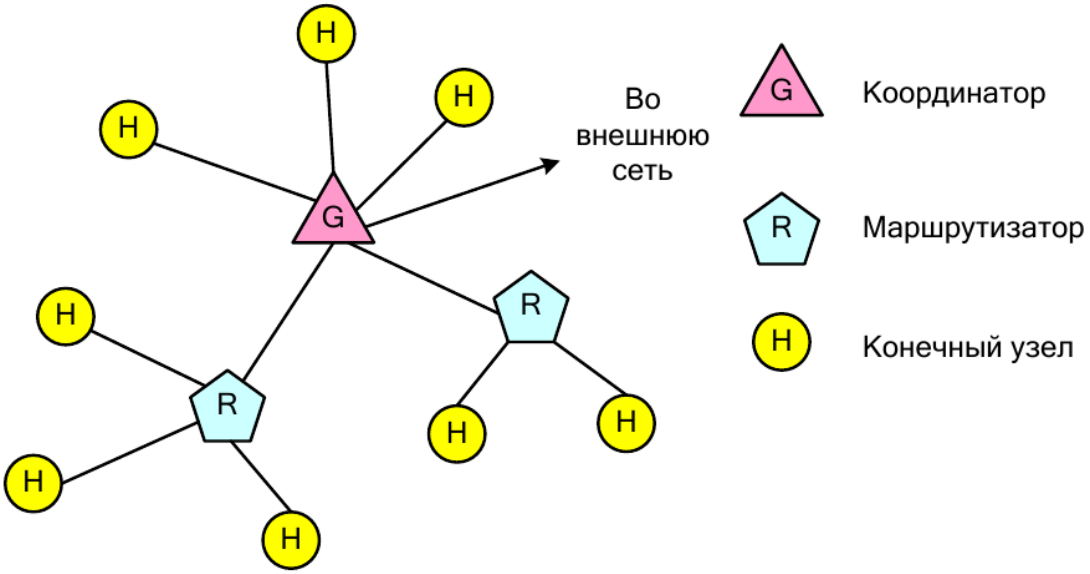


Рис. 4.6. Типы узлов БС

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 устройствам FFD, оконечные устройства могут быть FFD или RFD.

4.4. Типовые архитектуры и топологии БСС

Выделяют два типа архитектуры беспроводных сенсорных сетей: однородные (одно ранговые) 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.

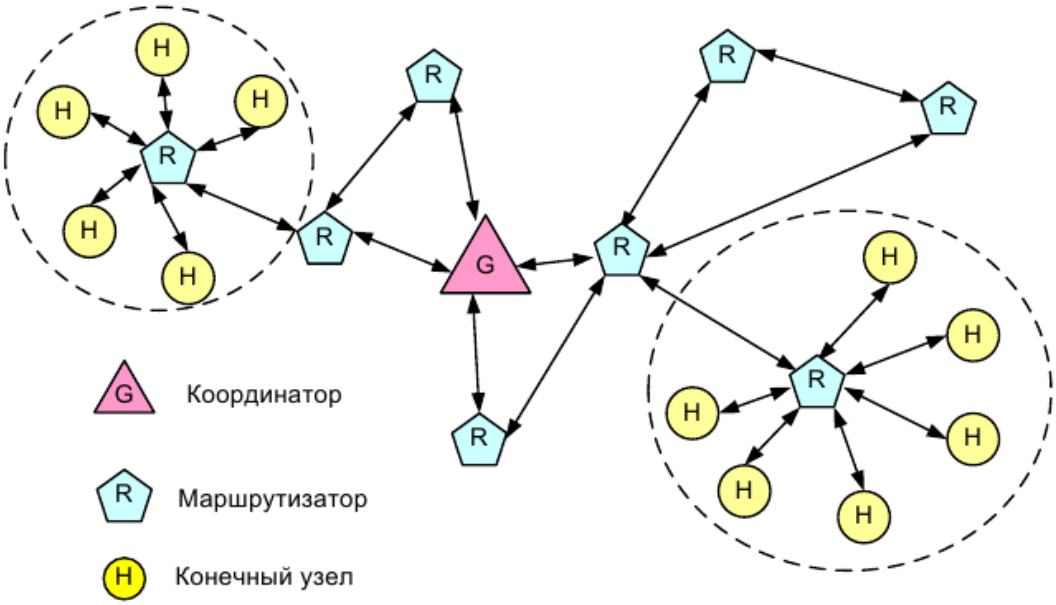


Рис. 4.7. Кластерная структура БСС

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. 4.7).

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 одно ранговых ячеистых сетей (рис. 4.8). 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».

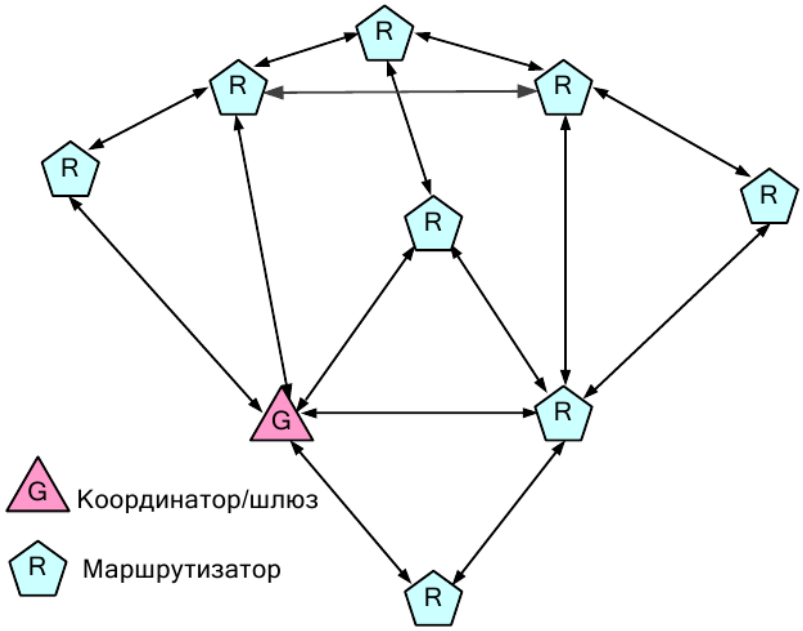


Рис. 4.8. Ячеистая структура БСС

Возможные топологии сенсорной сети приведены на рис. 4.9. 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.

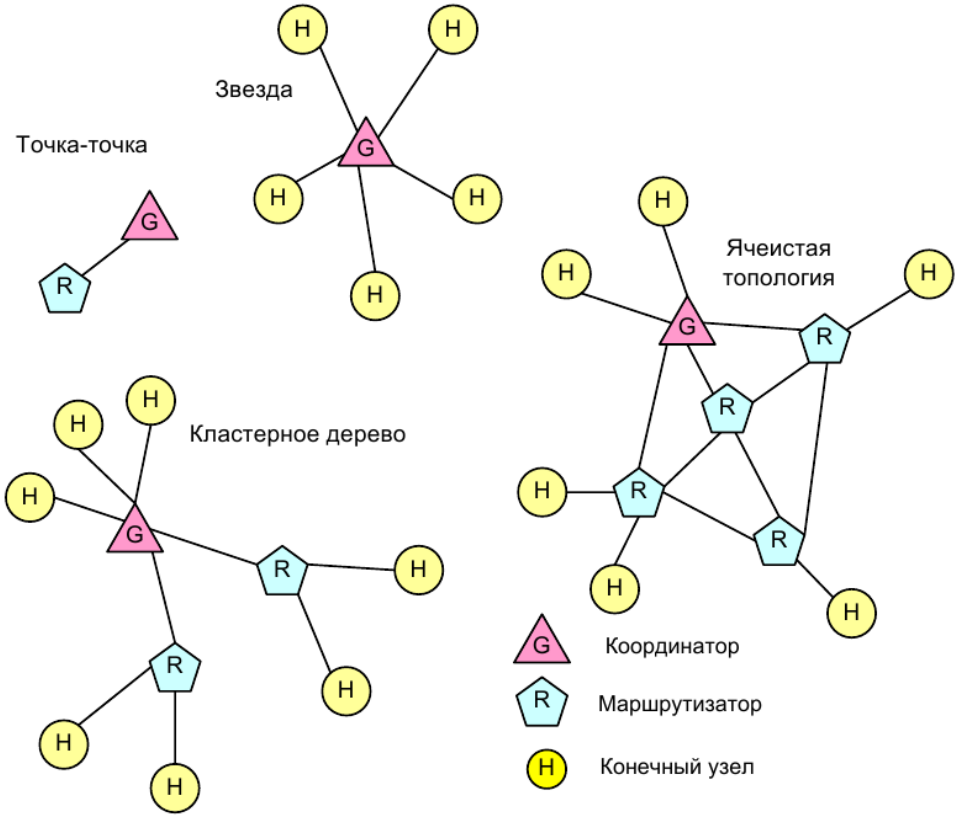


Рис. 4.9. Возможные топологии сенсорной сети

Примером одно ранговой 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 мульти кластеры из сетевых устройств.

4.5. 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.

4.6. 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 (само конфигурирование, самовосстановление и само оптимизация).
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.

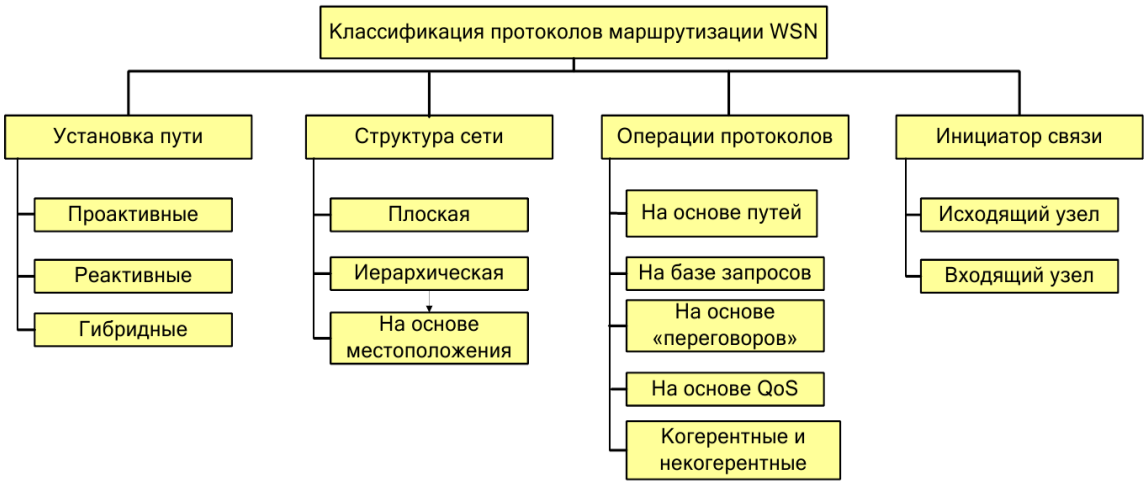


Рис. 4.10. Классификация протоколов маршрутизации БСС

Существует большое количество протоколов маршрутизации для БСС,
классифицировать их можно по разным признакам (рис. 4.10). 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.

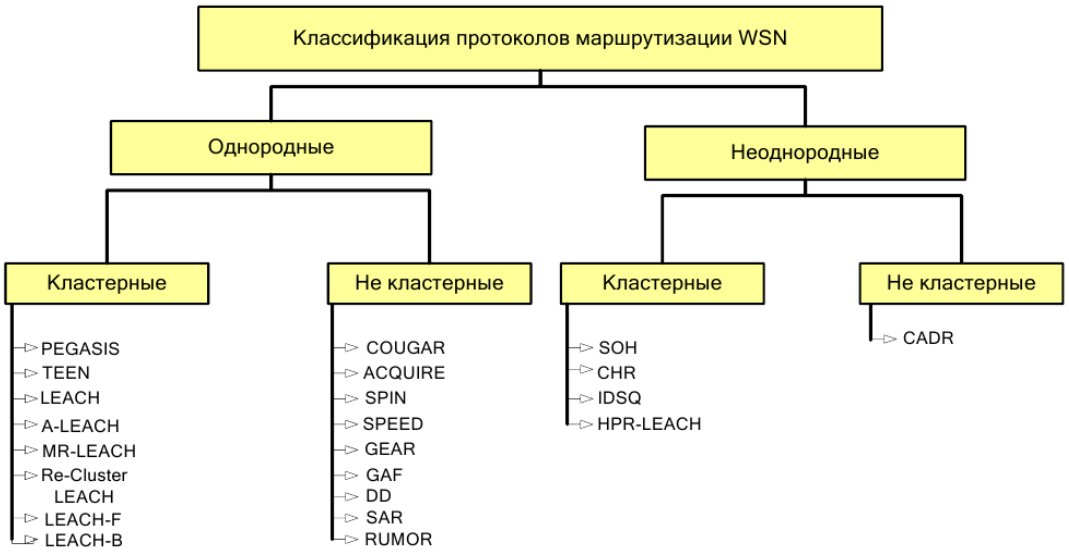


Рис. 4.11. Классификация протоколов маршрутизации БСС на основе типов узлов

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. 4.11.

4.7. 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. 4.12) 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.

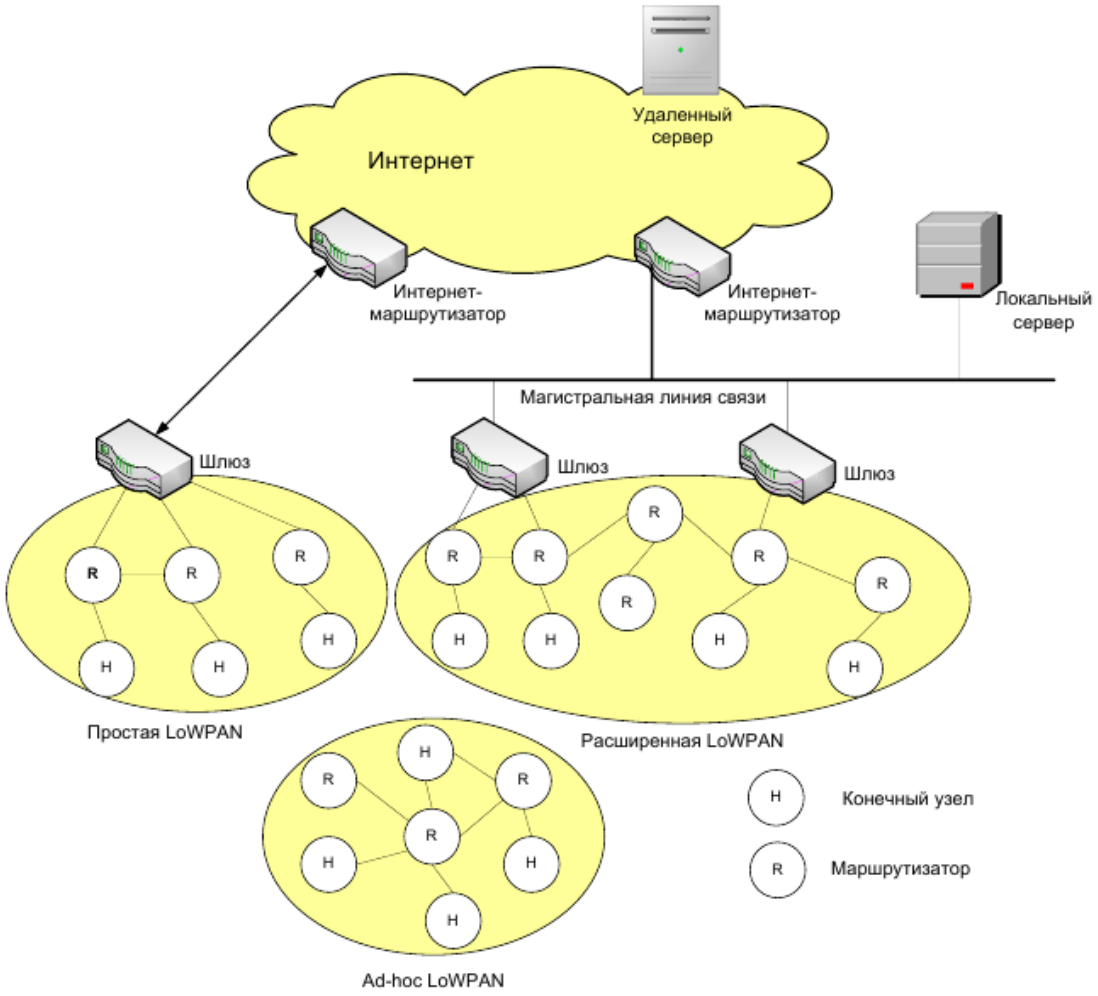


Рис. 4.12. Архитектура сети 6LoWPAN

4.8. 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:

$$\boldsymbol{P}\text{пр} \sim \boldsymbol{P}\text{прд} / \mathbf{D}^2,$$

где *Рпр* - мощность принятого сигнала;
*Р*прд - 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.

4.9. Беспроводные сенсорные сети и Интернет вещей

Благодаря таким характеристикам БСС, как миниатюрность узлов, низкое энергопотребление, встроенный радио интерфейс, 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.), нефти- 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 4

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 протоколы и технологии передачи данных используются в БСС?
8. Укажите отличия основных типов узлов БСС.
9. Какие основные архитектуры применяются для построения БСС?
10. Какие типовые топологии используются в БСС? В чем их отличие?
11. В каких режимах может работать БСС?
12. Какие задачи решают протоколы маршрутизации в БСС?
13. Поясните принципы классификации протоколов маршрутизации в БСС.
14. Перечислите основные проблемы практической реализации БСС.
15. Приведите примеры использования БСС для реализации концепции Интернета вещей.

ГЛАВА V. МЕЖМАШИННЫЕ КОММУНИКАЦИИ M2M

5.1. 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 еѐ 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. 5.1).

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. 5.1 - 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 рименяются 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).

5.2. 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. 5.2). 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.

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.

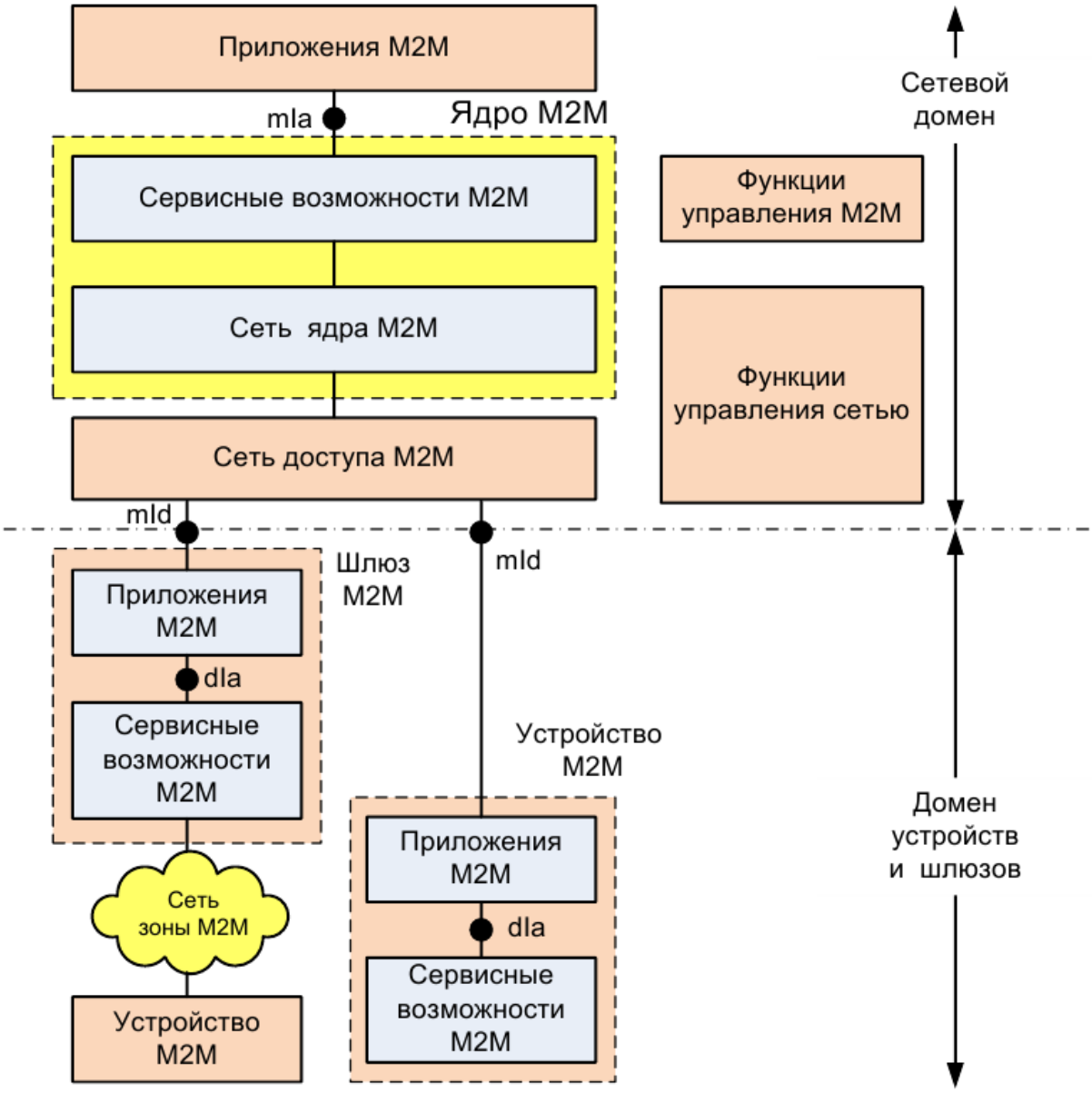


Рис. 5.2. Высокоуровневая архитектура ETSI M2M (источник: ETSI)

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. 5.3):

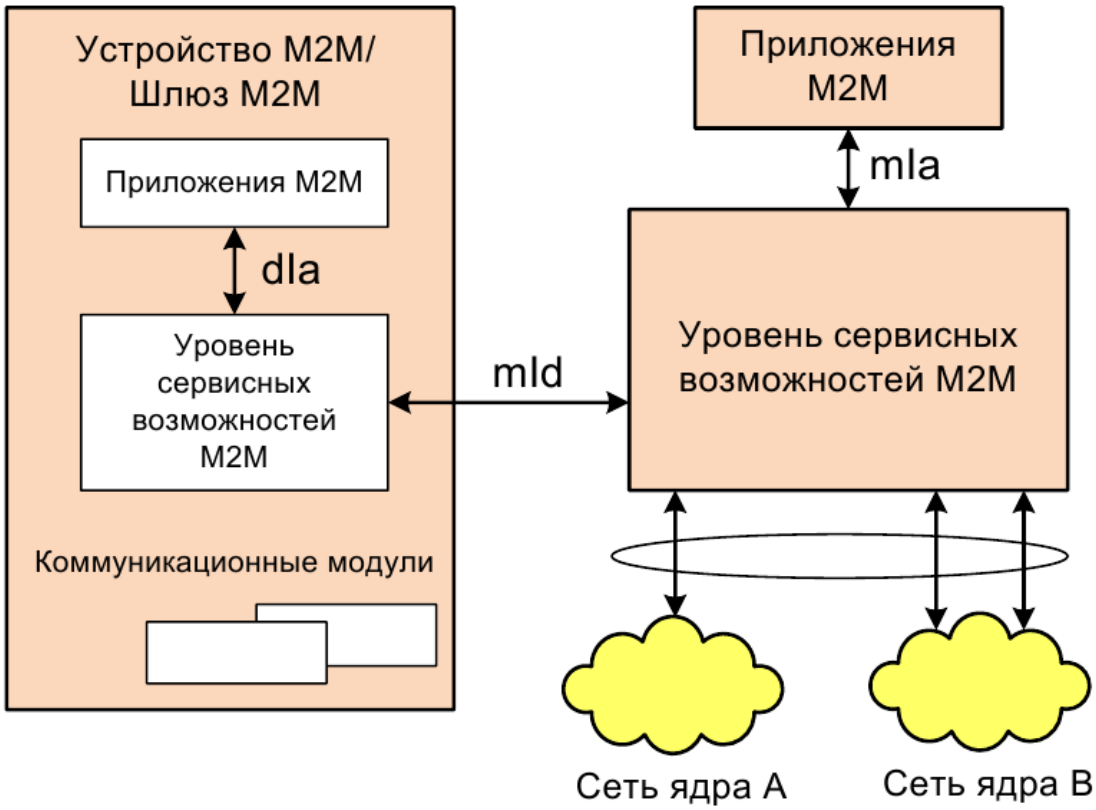


Рис. 5.3. Интерфейсные точки функциональной архитектуры M2M (источник: ETSI)

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 писания 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.

5.3. 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. 5.4).

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.

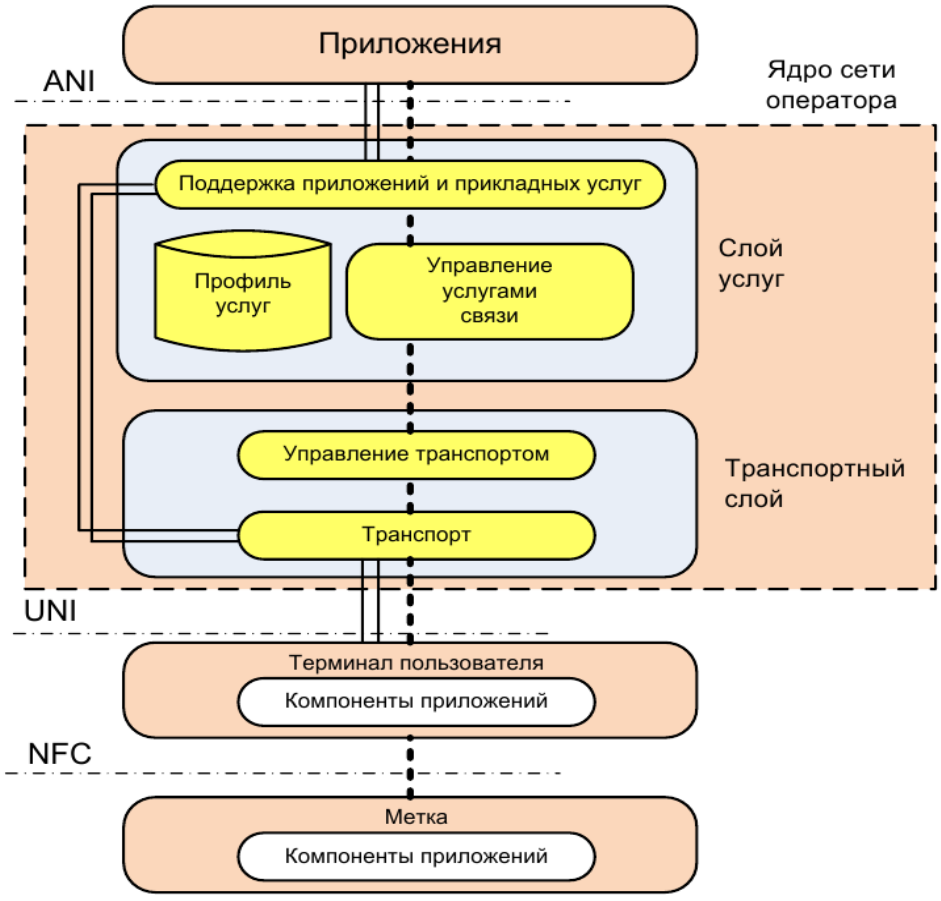


Рис. 5.4. Место технологии NFC в архитектуре сети NGN

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. 5.5). 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.

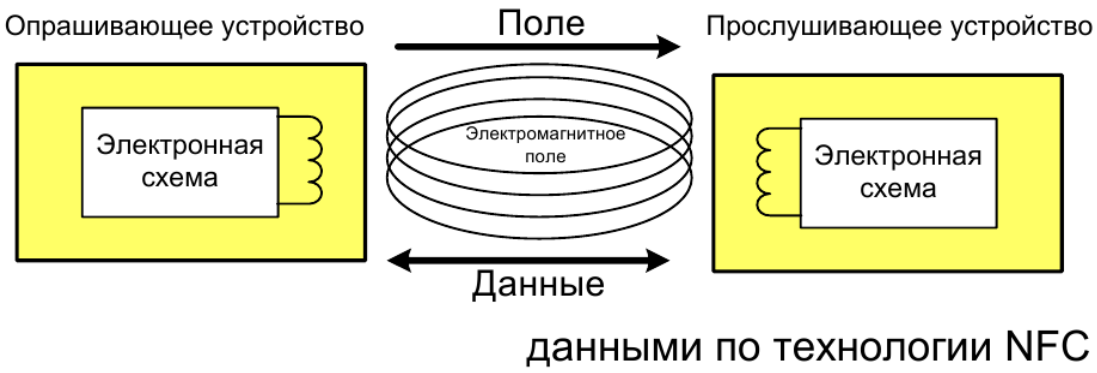


Рис. 5.5. Принцип обмена данными по технологии NFC

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.

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.

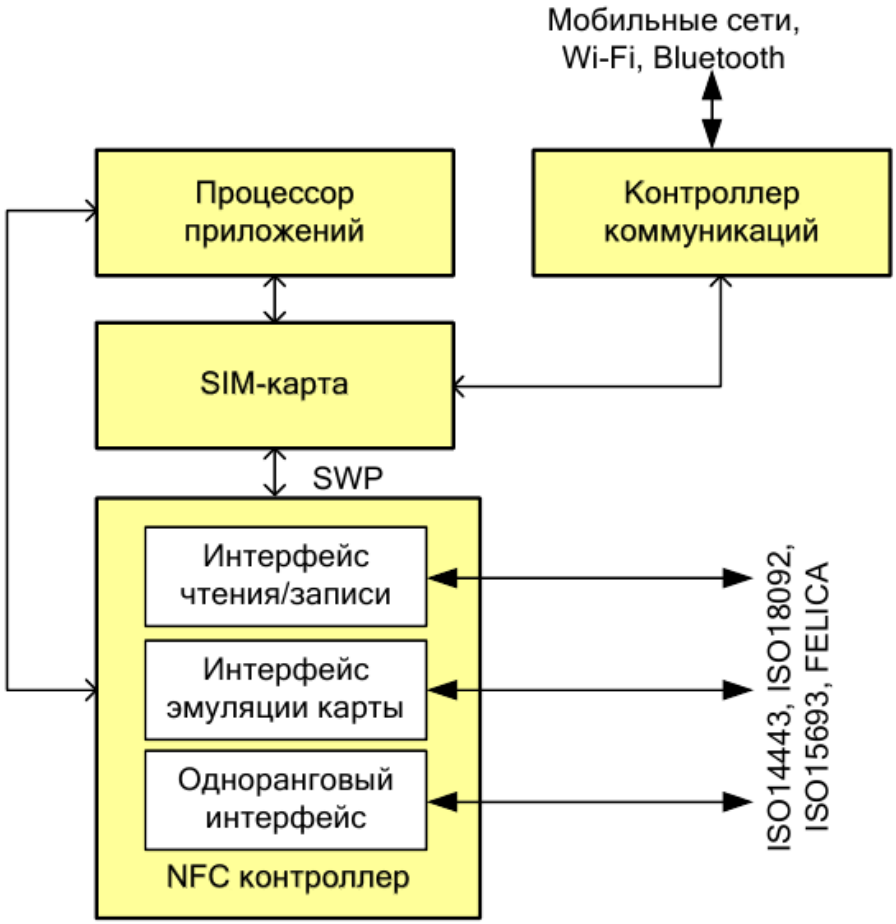


Рис. 5.6. Структурная схема мобильного телефона с модулем NFC

В модуле NFC есть микропроцессор (рис. 5.6), 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. 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.

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. 5.7 показан сценарий запроса и немедленного получения платной услуги с использованием мобильного телефона с функцией 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.

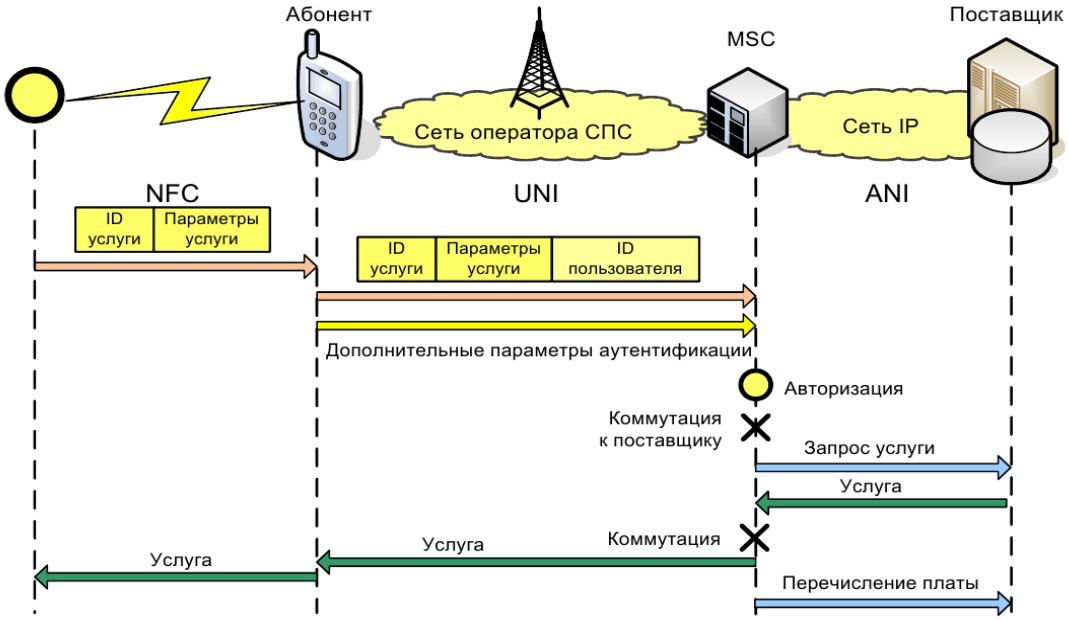


Рис. 5.7. Сценарий запроса и немедленного получения платной услуги с помощью NFC

5.4. 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.

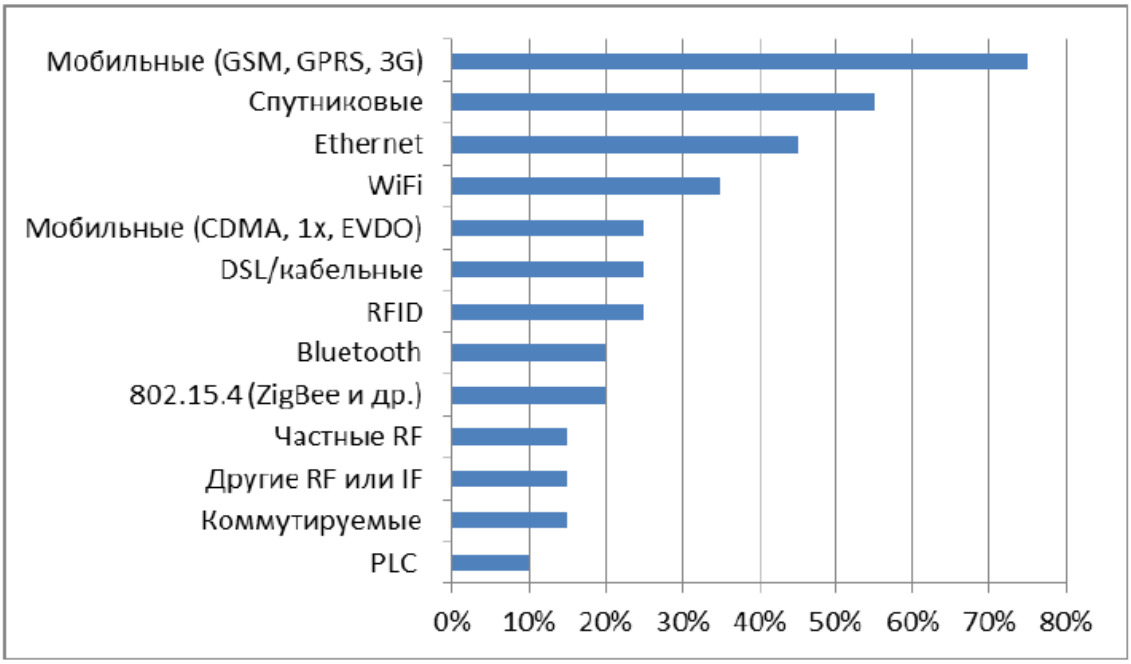


Рис. 5.8. Доля беспроводных технологий, используемых в системах M2M (источник: Duke-Wooley, 2012)

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. 5.8).

Контрольные вопросы по главе 5

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 VI. ЭКОСИСТЕМА И БИЗНЕС-МОДЕЛИ IOT

6.1. Экосистема IoT

Экосистема IoT - локальные или глобальные сети устройств, а также компоненты, дающие возможность присоединения к ним новых, обеспечивающие удаленное управление, хранение, передачу и безопасность данных.

Экосистема IoT имеет сложную структуру. Она состоит из сетей сенсоров и «умных устройств», предназначенных для подключения пользовательских и промышленных объектов, чтобы сделать их более «интеллектуальными» и улучшить их взаимодействие как с человеком, так и между собой.

Экосистема включает все компоненты, которые позволяют связать корпоративные, государственные и пользовательские системы с их IoT-устройствами, – пульты и панели управления, сети, шлюзы, аналитику, хранение и защиту данных.

Эксперты выделяют в экосистеме Интернета вещей четыре основных направления:

- оборудование — самое разнообразное, от устройств до сетей и серверов;
- программное обеспечение — все приложения, обеспечивающие доступ к системам Интернета вещей и управление ими;
- регулятивные правила и стандарты, способствующие раскрытию потенциала технологий;
- сервисы, обеспечивающие получение пользы широкому кругу компаний.

Экосистема IoT состоит из множества участников деятельности. Каждый участник деятельности играет как минимум одну деловую роль, однако ролей может быть и больше. Выявленные деловые роли IoT приведены на рис. 6.2.

Поставщик устройств отвечает за устройства, предоставляющие необработанные данные и/или контент поставщику сети и поставщику приложений в соответствии с логикой услуги.

Рис. 6.1 Основные компоненты экосистемы IoT

Рис. 6.2. Экосистема IoT

Поставщик сети играет одну из главных ролей в экосистеме IoT. Так, в частности, поставщик сети осуществляет следующие основные функции:

- доступ и интеграция ресурсов, предоставляемых другими поставщиками;
- поддержка инфраструктуры возможностей IoT и управление этой инфраструктурой;
- предоставление возможностей IoT, в том числе возможностей сети, и выделение ресурсов другим поставщикам.

Поставщик платформы предоставляет возможности интеграции и открытые интерфейсы. Разные платформы могут предоставлять поставщикам приложений разные возможности. Возможности платформы включают типовые возможности интеграции, а также хранение данных, обработку данных или управление устройством. Также возможна поддержка разных типов приложений IoT.

Поставщик приложений использует возможности или ресурсы, предоставленные поставщиком сети, поставщиком устройств и поставщиком платформы, для того чтобы предоставить приложения IoT абонентам приложений.

Абонент приложений – это пользователь приложения(й) IoT, предоставленного(ых) поставщиком приложений.

6.2. Бизнес-модели IoT

В реальных вариантах внедрения между участниками экосистемы IoT могут существовать различные взаимосвязи.

Мотивы этих разнообразных взаимосвязей основаны на разных возможных бизнес-моделях. В настоящем дополнении рассматриваются только некоторые бизнес-модели IoT с точки зрения услуг электросвязи и операторов сетей. Ниже приводится описание пяти бизнес-моделей с этой точки зрения.

Модель 1. В модели 1 участник A эксплуатирует устройство, сеть, платформу и приложения и напрямую обслуживает абонента приложений, как показано на рис. 6.3. Как правило, в *модели 1* в качестве участника A выступают операторы электросвязи и некоторые вертикально интегрированные предприятия (например, предприятия, обслуживающие "умные" электросети и интеллектуальные транспортные системы (ИТС)).

Рис. 6.3. Модель 1

Модель 2. В модели 2 участник А эксплуатирует устройство, сеть и платформу, а участник В эксплуатирует приложение и обслуживает абонентов приложений, как показано на рис. 6.4.

Как правило, в модели 2 в качестве участника А выступают операторы электросвязи, а в качестве участника В – другие поставщики услуг.

Рис. 6.4. Модель 2

Модель 3. В модели 3 участник А эксплуатирует сеть и платформу, участник В эксплуатирует устройство и приложения и обслуживает абонентов приложений, как показано на рис. 6.5.

Как правило, в качестве участника А выступают операторы электросвязи, а в качестве участника В – другие поставщики услуг.

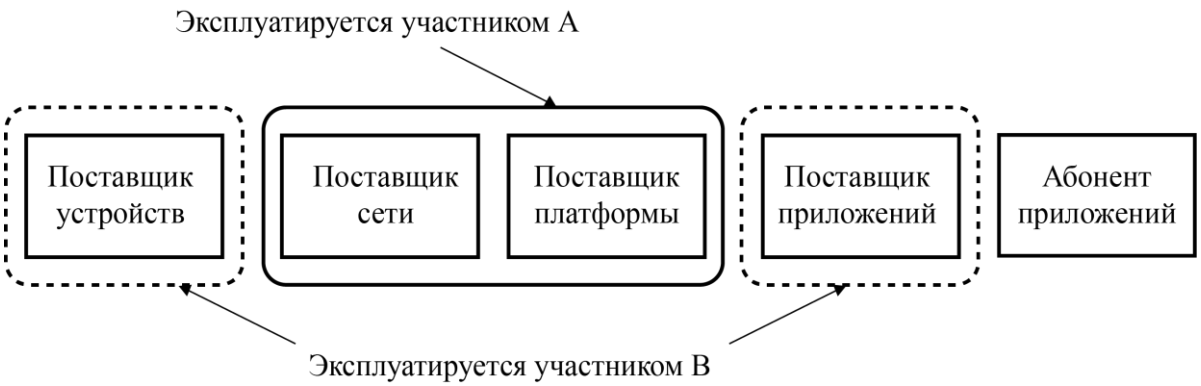


Рис. 6.5. Модель 3

Модель 4. В модели 4 участник А эксплуатирует только сеть, а участник эксплуатирует устройство и платформу, предоставляя приложения абонентам приложений, как показано на рис. 6.6.

Как правило, в модели 4 в качестве участника А выступают операторы электросвязи, а в качестве участника В – другие поставщики услуг и вертикально интегрированные предприятия.

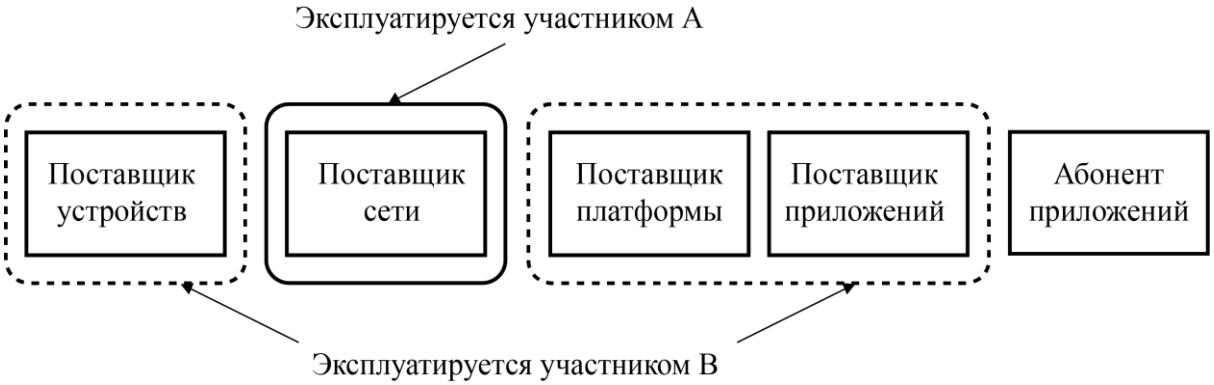


Рис. 6.6. Модель 4

Модель 5. В модели 5 участник А эксплуатирует только сеть, участник В эксплуатирует платформу, а участник С эксплуатирует устройства и предоставляет приложения абонентам приложений, как показано на рис. 6.7.

Как правило, в модели 5 в качестве участника А выступают операторы электросвязи, в качестве участника В – другие поставщики услуг, а в качестве участника С – вертикально интегрированные предприятия.

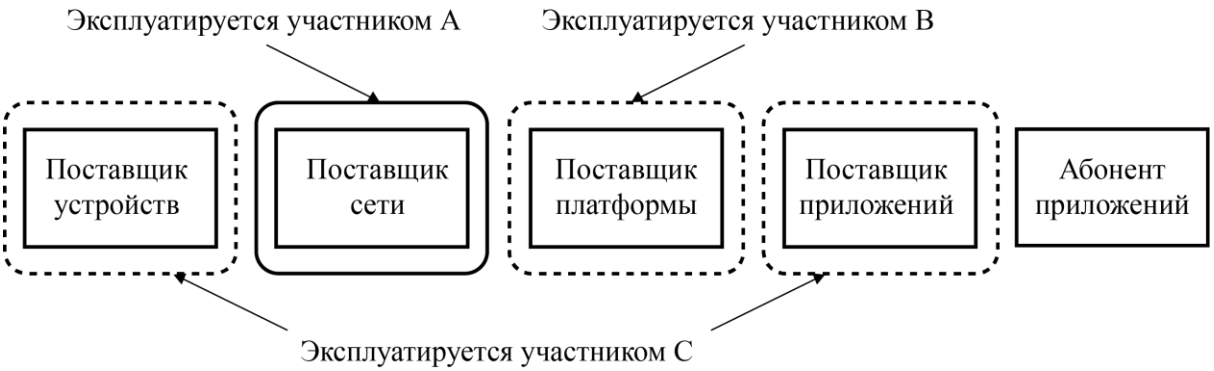


Рис. 6.7. Модель 5

Контрольные вопросы по главе 6

1. Что такое «Экосистема IoT»?
2. Расскажите основные направления Экосистемы IoT.
3. Что такое «Бизнес-модели IoT»?

ГЛАВА VII. СТАНДАРТЫ И ПРОТОКОЛЫ ПЕРЕДАЧИ ДАННЫХ В IOT

7.1. 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. 7.1):

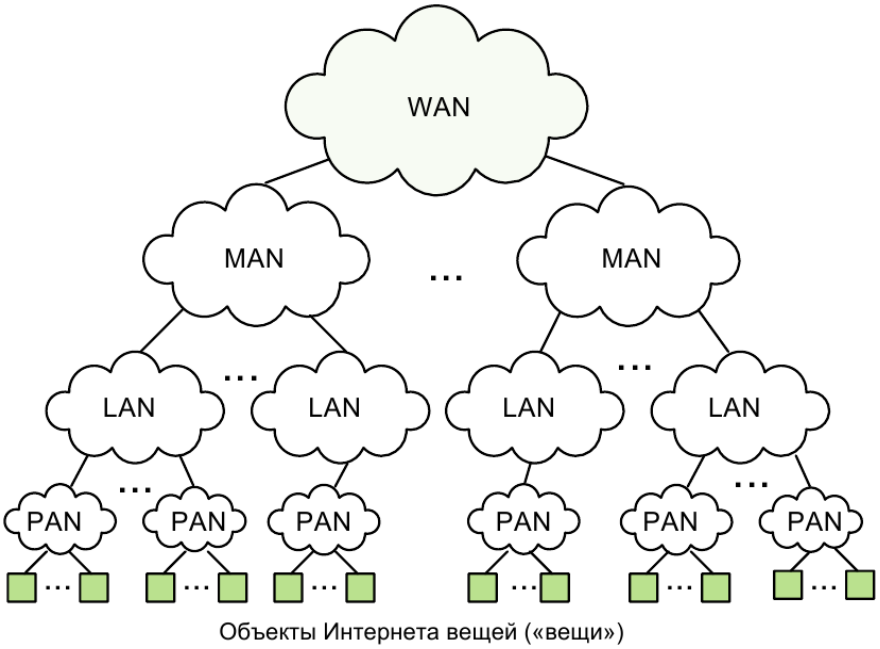


Рис. 7.1. Иерархия сетевых технологий, используемых в IoT

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.

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 развѐрнута с использованием различных сетевых технологий, например, Bluetooth, ZigBee, 6LoWPAN и других.

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.

Для взаимодействия огромного количества разнообразных устройств в IoT требуются стандартизированные интерфейсы, форматы данных и коммуникационные протоколы. В табл.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).

Таблица 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	+	+	+	+	+	+	+
ISA100.1	2400	250	+	+	+	+	+	+	+

1a									
Z-Wave	865/915/869	9,6/40	+	+	+	-	+	-	-
Bluetooth LE	2400	1000	+	+	+	+	+	+	+
DECT ULE	1880-1900	1000	+	+	+	-	-	+	+

7.2. 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. 7.2).

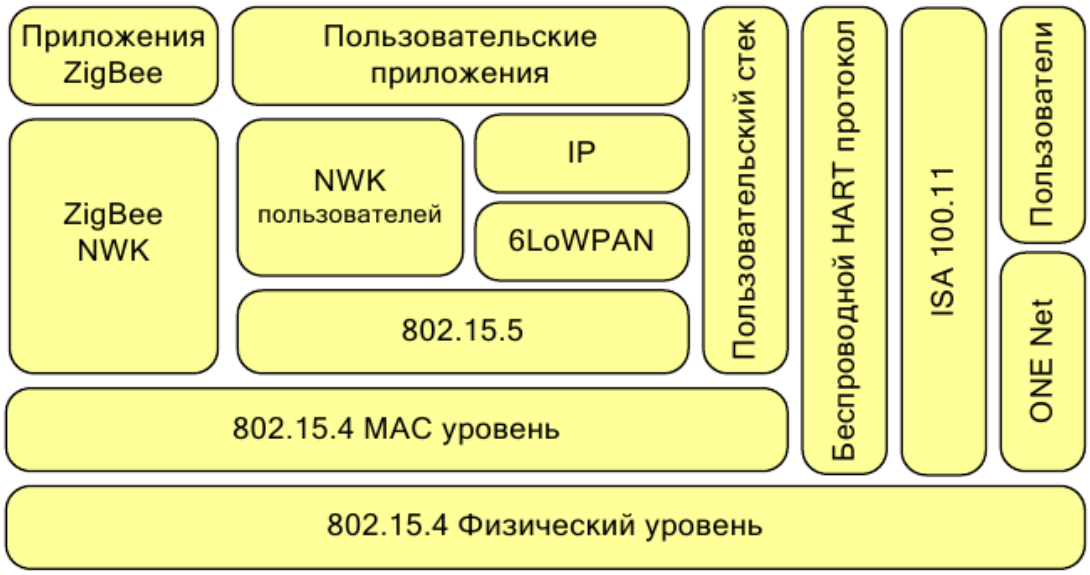


Рис. 7.2. Стек протоколов для стандарта IEEE Std 802.15.4

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.

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. 7.3).

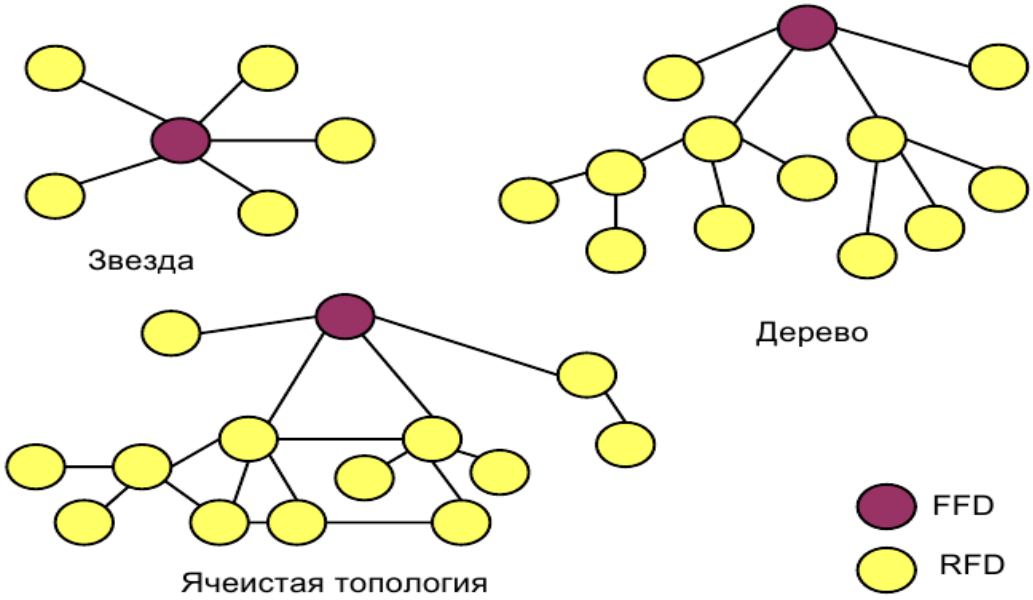


Рис. 7.3. Варианты топологии сетей стандарта IEEE Std 802.15.4

7.3. 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.

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. 7.4).

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.

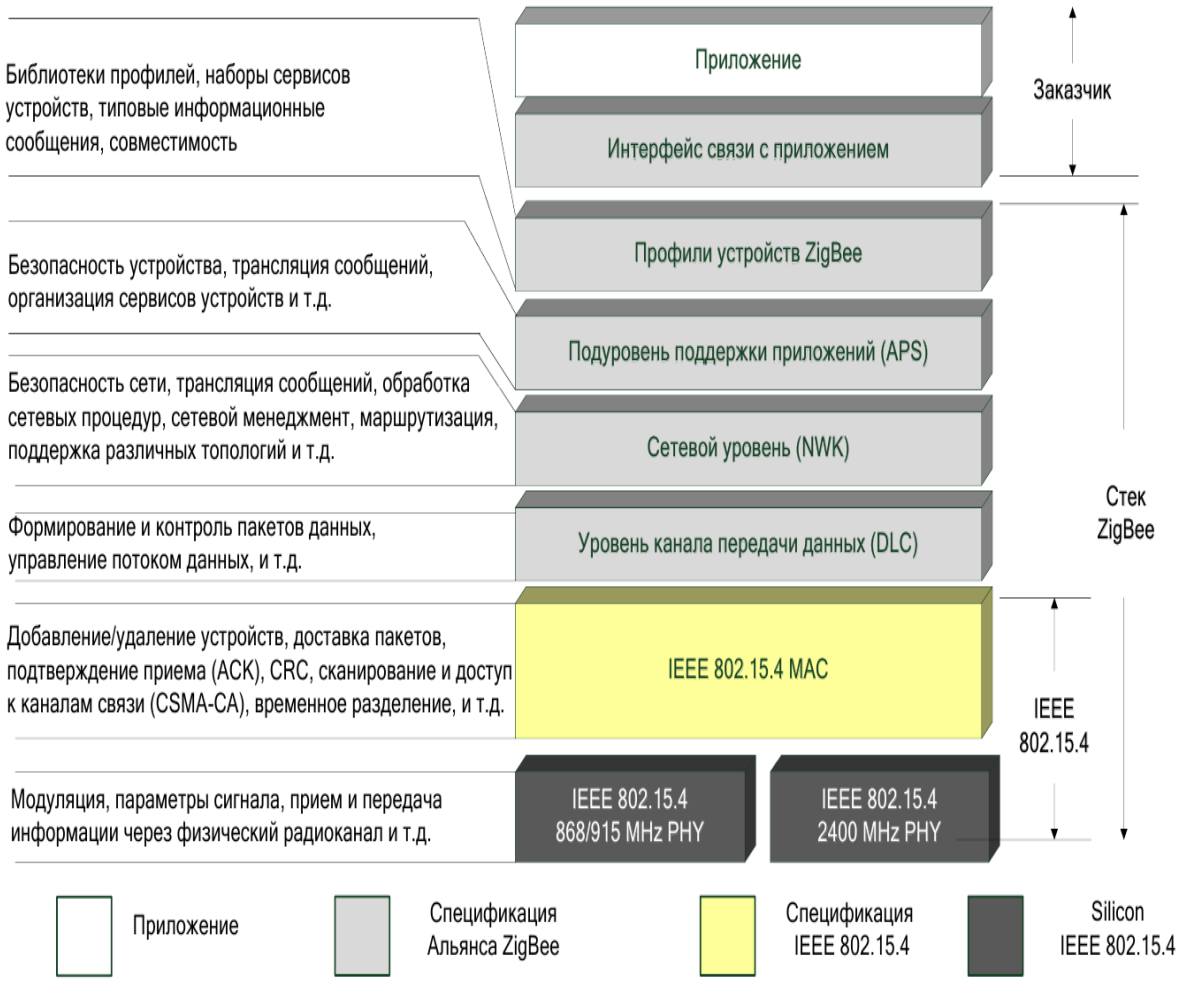


Рис. 7.4. Конфигурация стеков протоколов 802.15.4 и ZigBee

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.

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. 7.5).

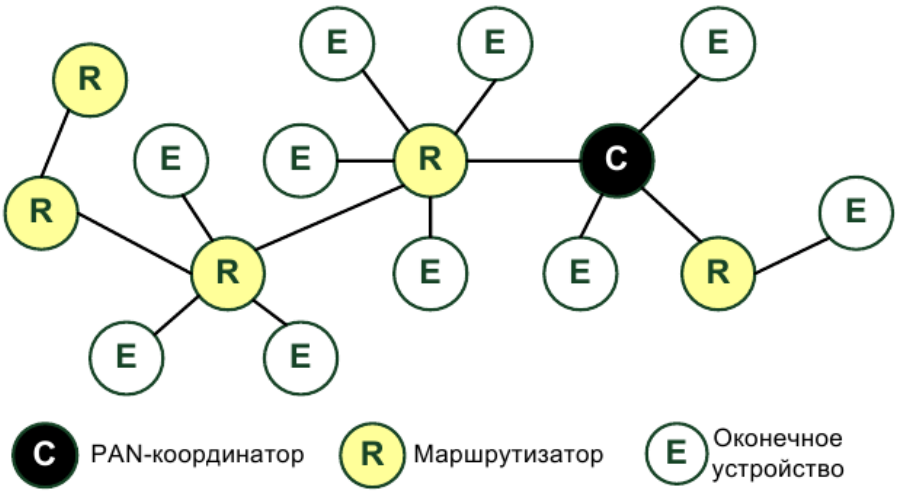


Рис. 7.5. Типовая топология сети ZigBee

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.

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, теле приставки 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.

7.4. 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. 7.6):

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

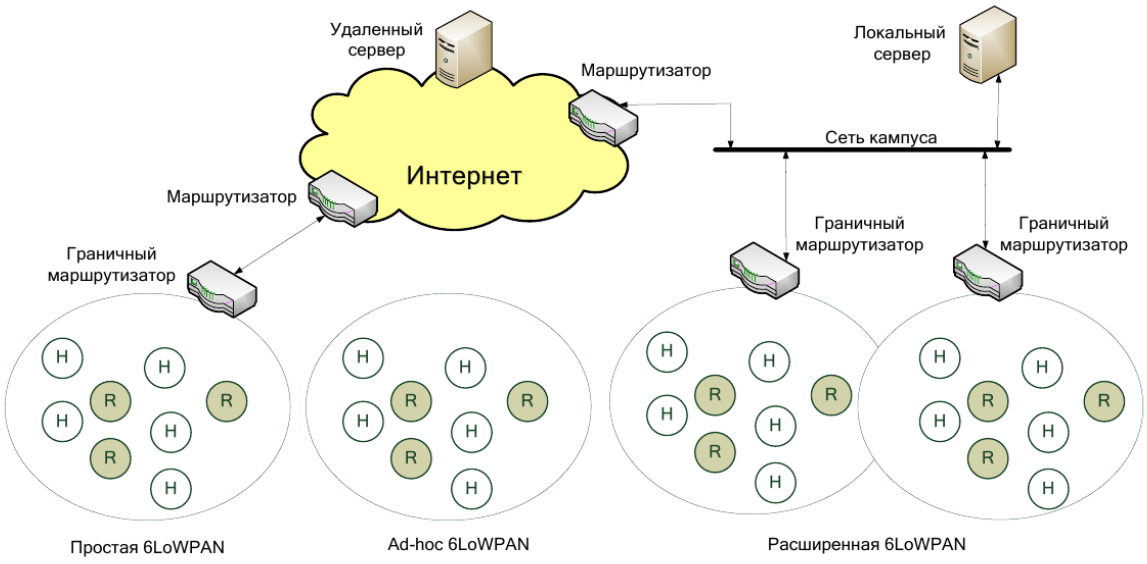


Рис. 7.6. Типы сетей 6LoWPAN (R- маршрутизатор, H – хост)

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).

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.

7.5. 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. 7.7). 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.

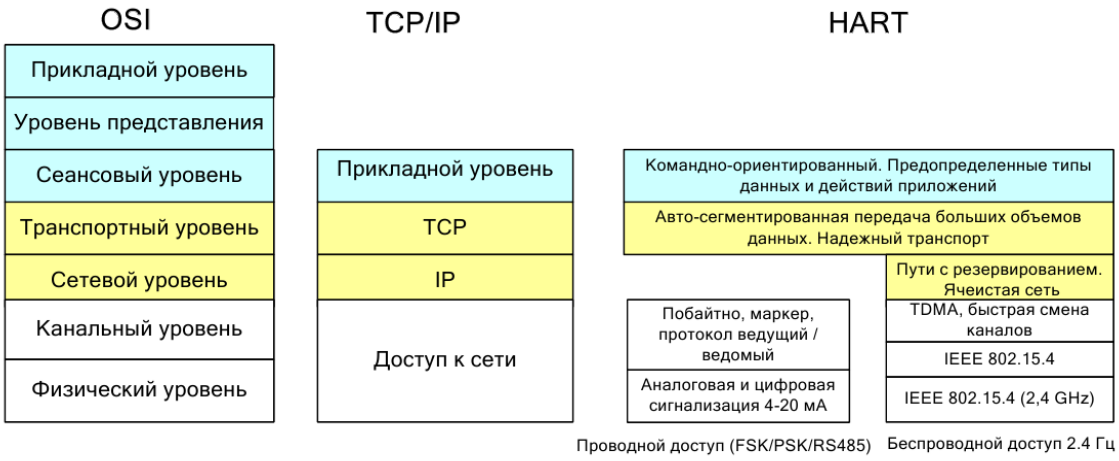


Рис. 7.7. Сравнение стеков протоколов OSI, TCP/IP и HART

Беспроводная сеть WirelessHART состоит из трех основных элементов (рис. 7.8):

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.

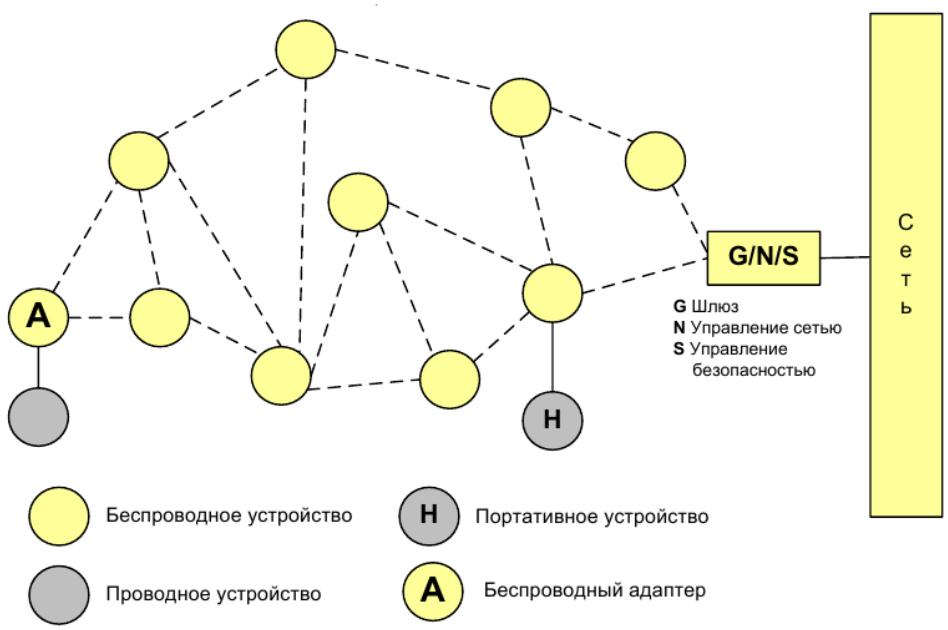


Рис. 7.8. Архитектура сети WirelessHART

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.

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. 7.9).

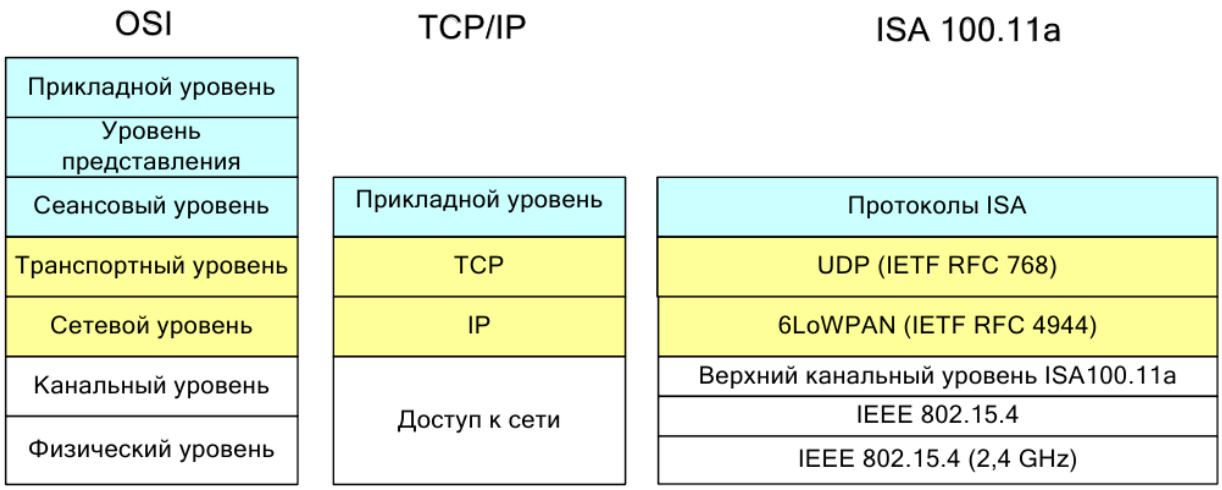


Рис. 7.9. Сравнение стеков протоколов OSI, TCP/IP и ISA100.11a

Беспроводная сеть стандарта ISA100.11a содержит следующие компоненты (рис. 7.10):

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

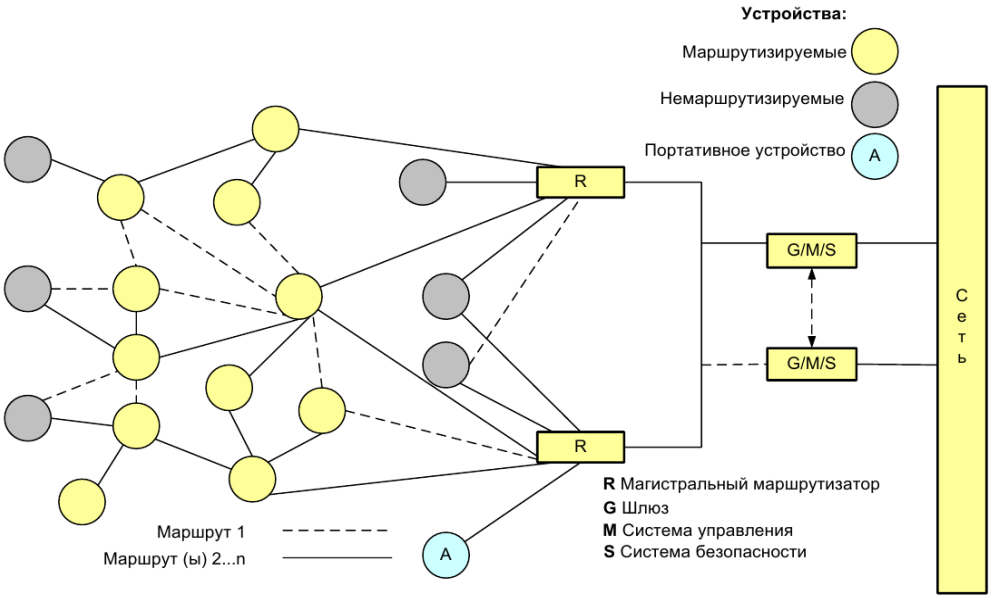


Рис. 7.10. Архитектура беспроводной сети по стандарту SP100.11a

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.

7.6. 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.

Рис. 7.11. Стек протокола Z-Wave

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. 7.11.

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).

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.

7.7. 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. 7.12). 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 программное на микроконтроллере приложений и включает в себя функциональность верхних уровней (рис. 7.12): 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.

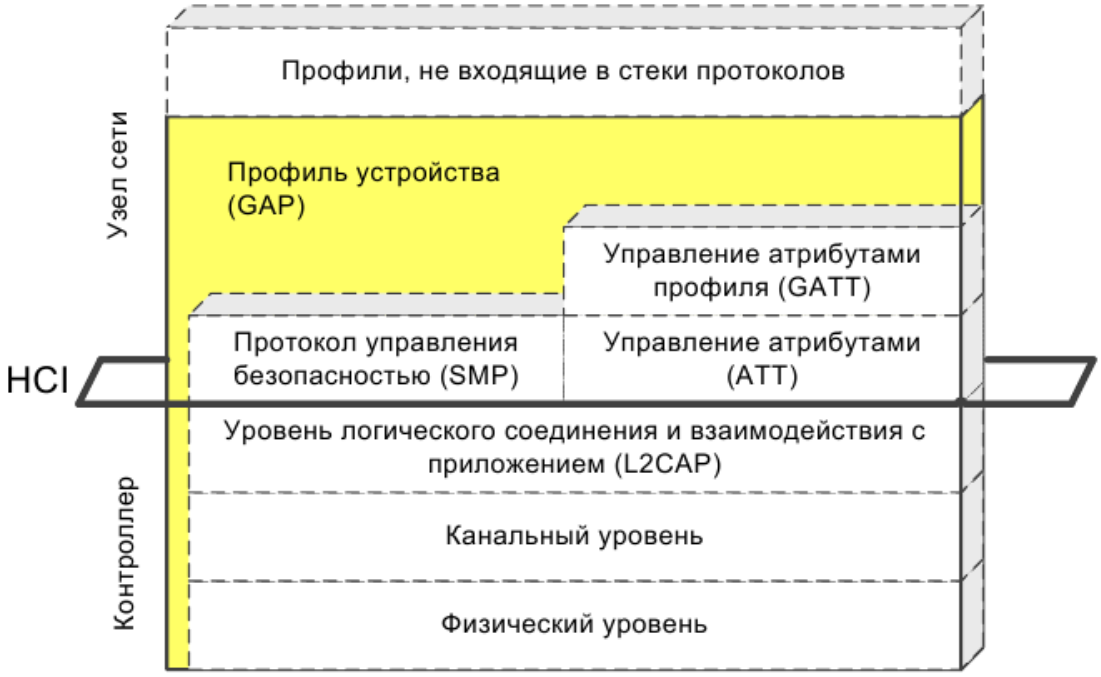


Рис. 7.12. Структура стека протоколов Bluetooth Low Energy

7.8. 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) – лѐгкий 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. 7.13):

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.

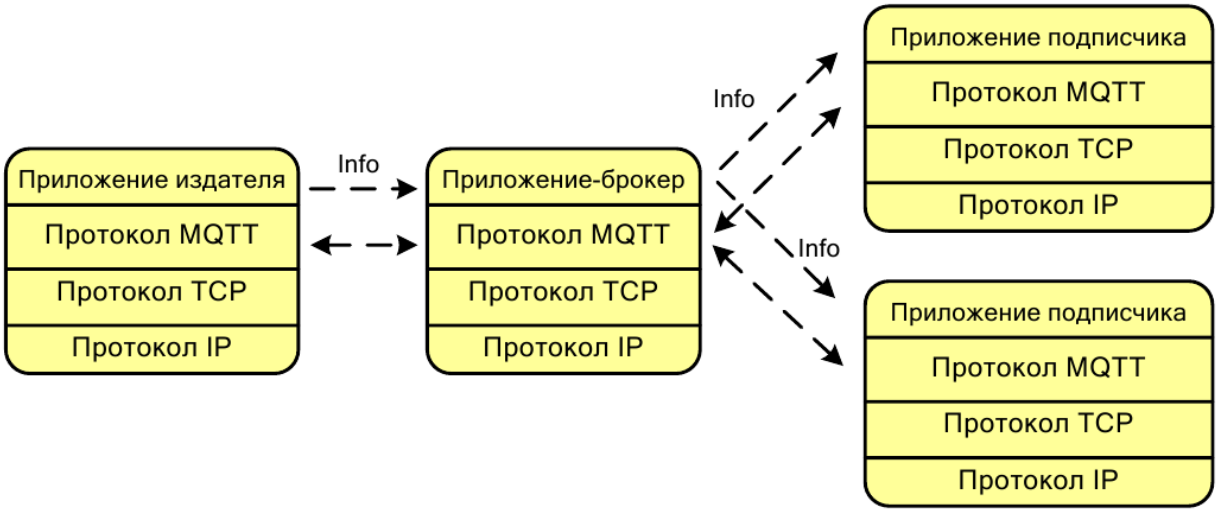


Рис. 7.13. Сеть на базе протокола MQTT

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 радио спектр будет использоваться для нового протокола, но планируется, что само устройство должно быть достаточно экономичным, энерго-эффективным, 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. 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.

Контрольные вопросы по главе 7

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. Какие функции реализует протокол MQTT в контексте реализации услуг IoT и M2M?

ГЛАВА VIII. ИНТЕРНЕТ ВЕЩЕЙ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

8.1. Перспективы и тенденции развития искусственного интеллекта

Цифровые технологии преобразуют все сферы жизни человек, в том числе, структуру рынка труда. Уже сейчас ИТ-сектор испытывает кадровый дефицит ряда специалистов, в частности, аналитиков-математиков (data scientists). Кроме того, большие данные эволюционируют в сторону все более сложных моделей и аналитических возможностей человека становится недостаточно. Некоторые функции будут переданы искусственному интеллекту, который с определенными вида работ стравится намного лучше. Например, Forrester прогнозирует, что в ближайшее десятилетие искусственный интеллект займет 16% рабочих мест в США. Ожидается, что искусственный интеллект станет основой четвертой технической революции. Обсуждается возможность реализации программируемых организаций, в которых преобладающая часть процессов будет автоматизирована и управлять ими будут самообучаемые алгоритмы.

Аналитические компании сформулировали 10 тенденций, стимулирующих развитие глобального рынка искусственного интеллекта. Среди них:

- базовой технологией искусственного интеллекта станет всесторонне обучение;
- искусственный интеллект завершит эпоху доминирования графических процессоров;
- искусственный интеллект окажет влияние на все отрасли. К 2020 году он будет также использоваться в государственном управлении;
- человеческое восприятие станет более важным драйвером для искусственного интеллекта, чем Big Data.

8.2. Инвестиции в искусственный интеллект

В настоящее время инвестиции в искусственный интеллект достигли 500 млн. долл. По данным исследовательских компаний, через 4 года показатель увеличится в 10 раз. Технология машинного обучения (Machine Learning) и распознавания естественного языка должна найти отклик в рекламе, розничной торговле, финансах и здравоохранении.

На пороге бурного развития находится и интернет вещей, который также требует обработки потоковой информации в режиме реального времени. Миллионы подключенных к сети устройств будут генерировать гигантские массивы данных, которые необходимо обрабатывать, анализировать и хранить.

Спектр применения объектов IoT безграничен. Специалисты предсказывают появление зубных щеток с функцией Bluetooth, которые будут отправлять информацию стоматологу, и электронных сигарет с Bluetooth, отслеживающих объем полученного человеком никотина и подающие сигнал о необходимости его сокращения. Уже многочисленные и доступные смарт-часы и смарт-трекеры также относятся к интернету вещей, а все данные поступают в облачные хранилища.

8.3. Интернет вещей для бизнеса

Для бизнеса IoT обещает повышение производительности при одновременном снижении издержек. Перспективны возможности IoT в части мониторинга систем на исправность работы, что позволит предотвращать выход из строя оборудования и оперативно реагировать на мелкие сбои, способствуя их бесперебойному функционированию. Дроны могут стать незаменимым помощником для сельхозпроизводителей, собирая информацию о зрелости урожая и состоянии почвы, уничтожая вредителей и обрабатывая посевы. Рост рынка интернета вещей до 2020 года оценивают в среднем на 21% в год. Но максимальную отдачу он покажет там, где будет сочетаться с аналитическими сервисами на основе Big Data и сервисами машинного обучения (Machine Learning).

Решениям в сфере искусственный интеллект (ИИ) и IoT с каждым годом уделяется все больше внимания во всех мировых IT-компаниях, а продукты в этих сферах становятся все более востребованными на рынке.

По сути, IT-трансформация общества в целом – это уже императив, а не просто одна из возможностей развития. Новый цифровой мир уже воплотился в реальность; концепция интернета вещей распространяется с огромной скоростью. И успешное развитие любого бизнеса в этом новом цифровом будущем требует технологических преобразований.

Так, ИИ позволяет создавать динамичные, гибкие, потенциально автономные системы, обеспечивая полноценное взаимопроникновение виртуального и реального миров.

В то же время большинство компаний не рискуют выходить за рамки узкоспециализированного ИИ, понимая, что на ближайшие несколько лет – это их единственная рабочая перспектива. Роботы по типу Софии представляют скорее научную, чем практическую ценность; у крупных продуктовых компаний они вызывают небольшой интерес, в отличие от ИИ для автомобилей, аналитики либо ритейла.

По словам Майкла Делла, основателя и главы корпорации Dell Technologies, данные – это топливо. В частности, топливо для «ракеты» под названием «искусственный интеллект». Но поскольку ценность данных неуклонно повышается, возникает и потребность в их усиленной защите. Поэтому популярность решений для защиты информации и обеспечения безопасности будет стабильно расти.

По прогнозам консалтинговой компании, Gartner, уже к 2020 году около трети всех сессий просмотра веб-страниц будут осуществляться без участия экранов наших гаджетов, но с участием таких ИИ как Amazon Echo или Google Home.

И эти прогнозы с каждым годом все ближе к реальности. Уже сегодня подростки практически не пользуются текстовым поиском, а следующее поколение переходит от общения в аудио формате к видео чатам и видеомесседжингу.

В условиях активного развития искусственного интеллекта также набирает популярность и концепция интернета вещей. Так,

за последние два года в Украине объемы продаж smart-устройств увеличились более чем в три раза.

А концепция по созданию smart city (систем «умный город») перешла от сугубо теоретической стадии к практическому воплощению. В мире насчитывается уже несколько десятков мегаполисов, которые можно причислить к полноценной IoT-инфраструктуре. Лучшими из них по праву считаются Мельбурн, Амстердам, Токио, Цюрих, Бостон, Сингапур и Копенгаген.

В будущем это поможет снизить нагрузку на коммунальные службы, удешевить обслуживание домов, энергосетей и теплотрасс, а также наладить адекватный транспортный поток внутри города вне зависимости от загруженности дорог.

Если говорить о прогнозах, специалисты той же компании Gartner считают, что уже в 2021 году в мире каждый час будут продаваться более 1 миллиона новых IoT-устройств. Склонен согласиться с этой статистикой, особенно ввиду того, насколько быстро подобные устройства захватывают наш рынок. И речь идет уже не о примитивных фитнес-трекерах или «умных мультиварках», а о системах управления потреблением энергии и энергосбережения в многоквартирных домах, системах управления транспортом и дорожным движением, повышением безопасности и многом другом.

Мы вошли в эпоху четвертой технологической революции, когда в роли топлива выступает не пар и не электричество, а информация. Раньше человек мог распоряжаться данными с относительной легкостью, но теперь, когда их поток увеличивается с каждой секундой, нам приходится все сложнее. Трудно представить себе цифру в 2,5 квинтиллиона, – но именно столько байтов данных производится в мире ежедневно. Этот впечатляющий объем информации открывает перед бизнесом колоссальные возможности.

Исследованиями в области искусственного интеллекта занимаются специалисты из разных стран. Осознавая огромные перспективы высокоинтеллектуальных систем, российские разработчики также уделяют этому направлению особое внимание. В данном обзоре мы собрали информацию о российских компаниях, занимающихся исследованиями в области искусственного интеллекта.

*Компания Яндекс***.** Компания Яндекс уже на протяжении нескольких лет применяет технологии искусственного интеллекта в своих поисковых механизмах. В настоящий момент работа ведется над созданием нейронной сети, способной вывести принцип работы поисковика на новый революционный уровень. Традиционный алгоритм поиска основан на сопоставлении содержания запроса с контентом анализируемых страниц. Безусловно, все это делается с некоторыми дополнениями и расширениями – запросы переформулируются, добавляются синонимы, переводятся на другой язык и т.д.

В новом подходе каждому запросу ставится в соответствие некое векторное число, наиболее точно отражающее его смысл. Далее поиск осуществляется по этому числу. При этом запрос и ответ могут не иметь ни одного общего слова. Все, что их будет объединять – это одинаковый смысл содержимого.

Стоит отметить, что в перспективе в векторное число смогут переводится изображения и видео, что, по словам представителей Яндекс, позволит значительно расширить границы «умного» поиска.

Совсем недавно компания Яндекс выпустила обновленную версию своего браузера, в котором технологии искусственного интеллекта позволяют персонализировать поиск в соответствии с интересами пользователя. Новый сервис получил название Дзэн.

Дзэн не только учитывает то, чем традиционно интересуются пользователи, но и анализирует их текущие предпочтения. Например, если человека заинтересуется анатомией, то материалов, связанных с этой темой, в его новостной ленте станет значительно больше. При этом, Дзен не ограничивается лишь любимыми сайтами и предпочтениями пользователя. Пользователю могут предлагаться материалы из совершенно незнакомых источников, если Дзен посчитает, что они могут его заинтересовать.

Достаточно интересным является применение технологий искусственного интеллекта в сервисе Яндекс.Аудитории. Данный сервис позволяет компаниям найти в Интернете целевых клиентов с целью более эффективного таргетирования рекламных объявлений. Достаточно загрузить в сервис список клиентов с телефонами и/или e-mail адресами, и система, сканируя

социальные сети с помощью искусственного интеллекта, находит этих людей в сети Интернет. Далее можно разбить клиентов по целевым группам и персонализировать для них через Яндекс.Директ рекламные объявления. Например, можно ненавязчиво предлагать целевой аудитории новый товар, или в конце концов склонить пользователей к покупке товара, которым они уже интересовались ранее.

Abbyy. Компания ABBYY является признанные мировым лидеров в области интеллектуальной обработки данных и лингвистики. Компания разработала решения, позволяющие с помощью технологий искусственного интеллекта распознавать текстовые данные, работать с печатными документами и файлами в формате PDF, самостоятельно осуществлять ввод данных в информационные системы компаний, производить корпоративный семантический поиск, а также находить переводы незнакомых слов и фраз.

Одним из главных достижений ABBYY является система Compreno, позволяющая анализировать и понимать текст на естественном языке. Над созданием данной системы специалисты компании работали около 10 лет. Стоимость проекта составила более $80 млн. Принцип работы Compreno представлены на следующем рисунке.

Рис. 8.1. Этапы работы ABBYY Compreno. Источник: ABBYY

1-Этап. Лексико-морфологический анализ. На первом этапе анализируемый текст делится на абзацы, предложения и слова. Для каждого слова определяется часть речи и морфологические характеристики (род, число, падеж и т.д.

2-Этап. Синтаксический анализ. В тексте выделяются предложения. Для каждого предложения определяется структура и принцип организации связи слов.

3-Этап. Семантический анализ. Определяется значение каждого слова и строится семантическая структура предложения, исходя из установленных на прошлом этапе связей.

4-Этап. Прагматический уровень анализа. На этом этапе накладывается прагматический слой анализа текста, применяются онтологии (терминология для конкретной предметной области анализа) и правила извлечения нужных объектов.

В результате, на выходе системы получается универсальный и структурированный набор данных, что позволяет ABBYY Compreno решать задачи по анализу и извлечению важной информации, «умному» поиску и классификации данных.

Технологии компании ABBYY используются по всему миру. Все решения лицензируются крупнейшими международными ИТ-компаниями, такими как EPSON, Fujitsu, Samsung, Panasonic, Sharp, Acer, KnowledgeLake, Microsoft и другие. Заказчиками ABBYY являются российские и международные компании из банковской, энергетической, нефтегазовой, телекоммуникационной и других отраслей, а также из государственного сектора.

Findo. В начале 2016 года Давид Ян, основатель компании ABBYY, объявил о запуске в США нового проекта – Findo. Findo является интеллектуальным помощником, которые предназначен для поиска информации в интернете, в облаке и локальных файлах. Уникальной способностью помощника является распознавание естественной речи (правда, пока только на английском языке).

Для поиска могут использоваться достаточно «сложные» запросы. Например, Findo способен работать с запросами, вида: «найди документы, которые я редктировал в прошлую среду», «покажи письмо, которое мне вчера прислали из Москвы» и т.д.

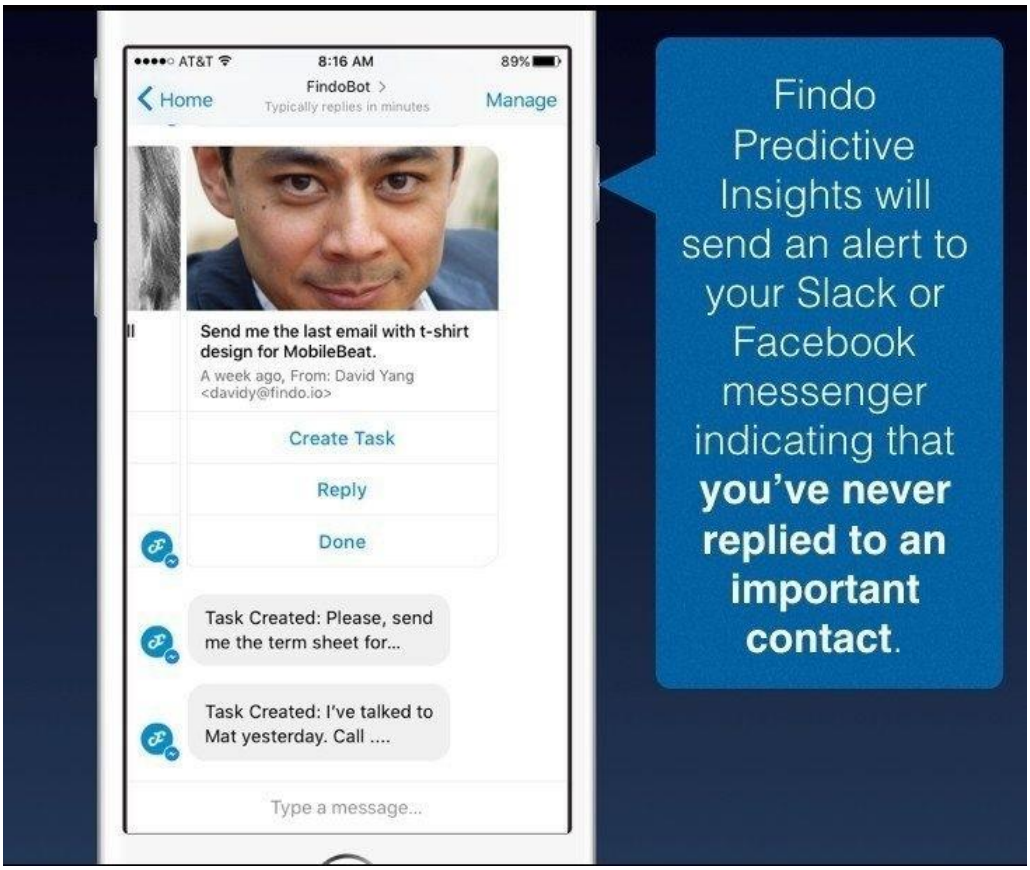


Рис. 8.2. Пример запросов, обрабатываемых Findo.
Источник: finsmes.com

Для более точного «понимания» естественного языка используются наработки технологии ABBYY Compreno. Сама компания ABBYY вложила в стартап около $3 млн.

Головной офис Findo находится в Менло-парк, Калифорния. Пока сервис предоставляется бесплатно. В будущем компания планирует зарабатывать по модели freemium: предоставление базового функционала бесплатно и около $5 в месяц за расширенную версию.

VisionLabs. Компания VisionLabs была основана в 2012 году и является резидентом IT-кластера «Сколково». Компания специализируется на решениях, позволяющих распознавать лица клиентов в самых быстрорастущих сегментах рынка: банковский сектор и ритейл. Массачусетский университет включил VisionLabs в тройку лучших мировых систем в области распознавания лиц для коммерческих целей.

Высокоточные алгоритмы распознавания образов были получены в результате использования нейронных сверточных

сетей, обученных с помощью методов глубокого обучения и многомиллионных массивов данных, что, по словам представителей компании, является существенным преимуществом выпускаемого продукта. Малый размер ключа, извлекаемого из фотоизображения, позволяет проводить сравнения 500 миллионов ключей менее чем за 1 секунду.

Платформа распознавания лиц VisionLabs LUNA - флагманский продукт компании. LUNA позволяет в режиме реального времени анализировать колоссальные объемы фото- и видеоданных с целью определения в них лиц людей и сравнения их с многомиллионными базами данных. На базе данной технологии также создан облачный сервис FACE_IS, который может связывать клиентов с предшествующей историей их покупок и помогать выстраивать взаимодействие с брендом. Решения компании являются plug'&'play, по умолчанию имеют интеграцию с большинством баз данных, CRM и BI-систем, и не требуют от пользователей замены оборудования, так как интегрируются в их существующую IT- инфраструктуру.

В 2014 году компания VisionLabs заключила эксклюзивный контракт с Бюро кредитных историй «Эквифакс» в России по запуску системы распознавания лиц на межбанковском уровне. Система используется в рамках сервиса противодействия кредитному мошенничеству. К данному сервису на базе решения VisionLabs подключено уже более 20 крупнейших банков в России. Крупнейшим реализованным проектом в РФ является проект с «Почта Банк», в СНГ - с Kaspi Bank.

Мивар. Специалисты компании Мивар заложили в основу своих исследований принципиально новую теоретическую базу, и преодолели ограничения, наложенные на разработчиков искусственного интеллекта одной из «задач тысячелетия» – P=NP. Ранее считалось, что логический вывод относится к классу полнопереборных задач. В рамках миварной теории, специалисты Мивар смогли не только снять эти ограничения, но и стали способны решать логические задачи, содержащие несколько миллионов правил, причем, на обычном ноутбуке или бытовом компьютере. Традиционные подходы к созданию искусственного интеллекта такого не позволяют. Это дает возможность создавать более мощные и совершенные системы, перейти в работе с

текстами и изображениями от уровня формальных признаков на семантический уровень. И вообще начать полноценно работать не только с данными, но и со знаниями.

Среди основных направлений, где компания применяет миварные технологии, можно выделить следующие:

- Экспертные системы нового поколения (логически решающие системы, LRS)
- Семантические технологии понимания естественного языка
- Интеллектуальное распознавание образов
- АСУ и системы управления автономными интеллектуальными роботами

Развивать свои решения компания планирует не только на российском рынке, но и на международном.

В ближайшие несколько лет компания Мивар планирует завершить формирование своих продуктовых линеек, создать предпосылки для массовой интеллектуализации роботов, робототехнических комплексов и систем управления. Также планируется сформировать публичный банк миварных моделей, который позволит перейти к повсеместному внедрению логического искусственного интеллекта, виртуальных работников и интеллектуальных программных роботов. Средства на эти цели у компании есть. В прошлом году Мивар смогла привлечь $10 млн от коммерческой организации ITG (INLINE Technologies Group).

Контрольные вопросы по главе 8

1. По каким причинам некоторые функции ИТ сектора будет переданы искусственному интеллекту и какой процент рабочих мест, прогнозируемый в США, замёт ИИ?
2. К чему может послужить создание Smart city?
3. Что подразумевается под выражением «четвертая технологическая революция»?
4. Что представляет собой новый сервис браузера под названием Дзен?
5. Какая система компании ABBYY является более удобной в сфере лингвистики?

6. Чем служит компания VisionLabs в бюро кредитной истории «Эквифакс»?
7. Какие планы имеет компания Мивар в ближайшие несколько лет?

ГЛАВА IX. ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ IOT

Умные решения IoT обеспечивают подключение устройств ко всемирной паутине, возможность сбора и анализа данных, передачу полезной аналитической информации. Стоит ли говорить о том, что все это позволяет сократить затраты (конечно при существенном начальном вложении), повысить эффективность работы предприятий и увеличить их прибыль. Ниже лишь малый список того, в каких сферах и для чего может быть использована технология Интернета вещей:

Новая эра автономного вождения. IoT устройства позволят реализовать полностью автономное вождение. Благодаря этому дороги станут менее загруженными и более безопасными.

Современный автомобиль буквально напичкан всевозможными датчиками и сенсорами: распознавание голоса, индикаторы на лобовом стекле и системы автоматической парковки - это лишь малая часть того, что нас ждет в будущем. Автомобили Tesla – явное тому подтверждение.

Трансформация энергетики. Примененные в энергетике IoT-устройства смогут обмениваться информацией в режиме реального времени, тем самым увеличивая эффективное распределение энергоресурсов, а сами электросети станут более безопасными.

9.1. «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.

9.2. «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. 9.1) 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 u-городов, в которых объекты инфраструктуры и люди тесно связаны. Правительства нескольких стран уже приняли масштабные программы создания интеллектуальных городов U-City.

Рис. 9.1. 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 Ташкенте на улице А. Темура 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.

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.

9.3. «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. 9.2).

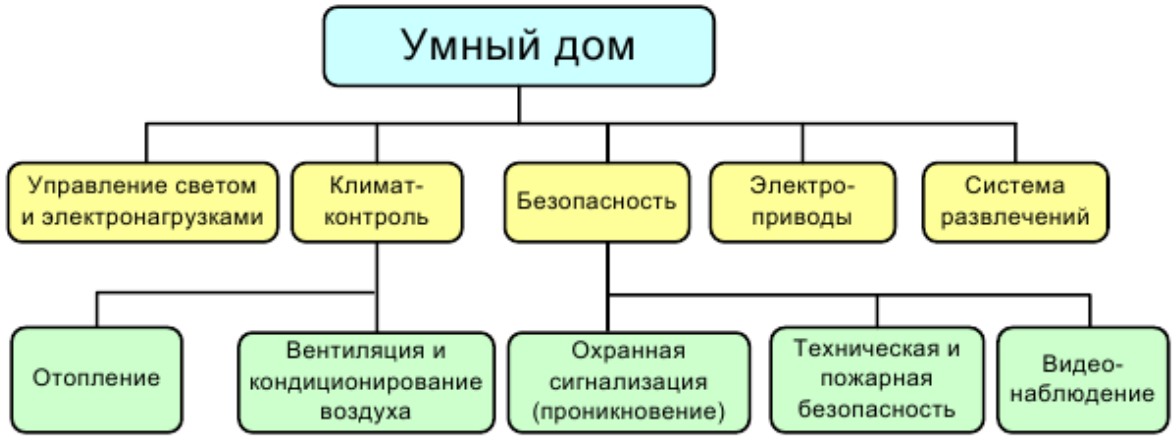


Рис. 9.2. Основные подсистемы «умного дома»

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. 9.3).

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. 9.3. 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 техно шутка 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 интернету.

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. 9.4). 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 видео почту. 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. 9.4. Интернет-холодильник Digital Dios Refrigerator LG Electronics

Робот-пылесос может действовать автономно, программироваться и управляться через Интернет, для чего имеется ряд сенсоров и инфракрасная встроенная камера (рис. 9.5).

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. 9.5. Робот-пылесос VC-RL87W Samsung

Интернет микроволновая печь (рис. 9.6) имеет встроенный модем для выхода в интернет, память для хранения скачиваемой информации и пульт управления. Она выполняет следующие задачи:

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

Рис. 9.6. Микроволновая интернет-печь M-G270IT LG Electronics

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.

9.4. «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. 9.7):

- «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.
-

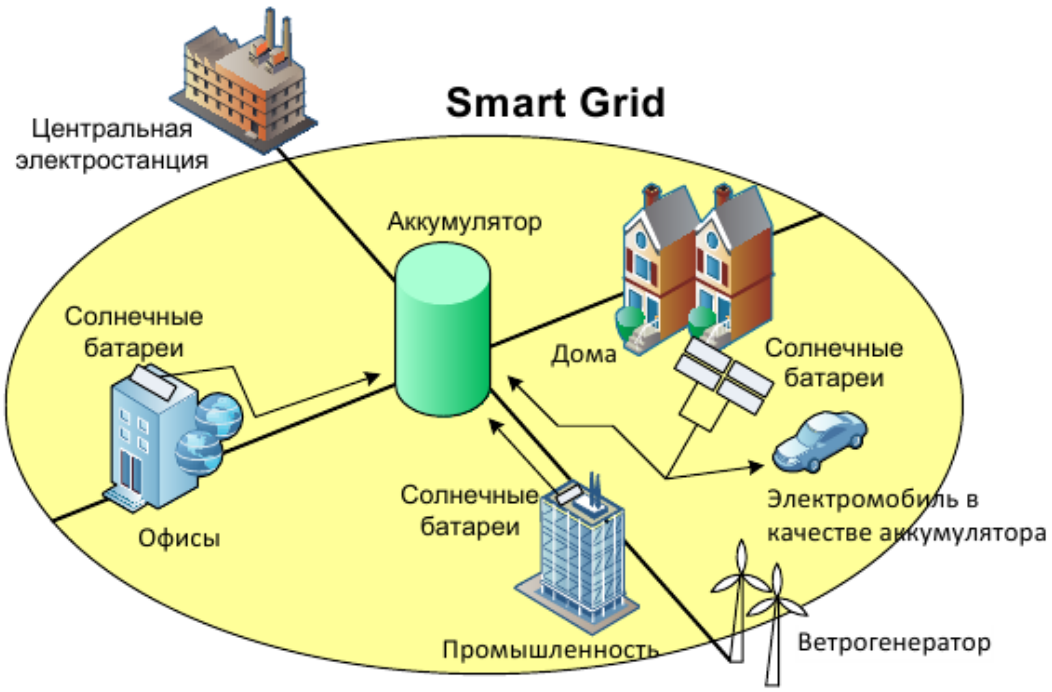


Рис. 9.7. Схема «умной» сети Smart Grid

«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.

9.5. «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 существляют 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.

В качестве примера использования технологий IoT в городах можно привести систему управления автомобильным трафиком (рис. 9.8), 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 своем состоянии, которые могут быть доступны любым другим устройствам и сервисам, будь то ГЛОНАСС/GPS-навигатор, мобильный телефон или специализированные веб-сайты.

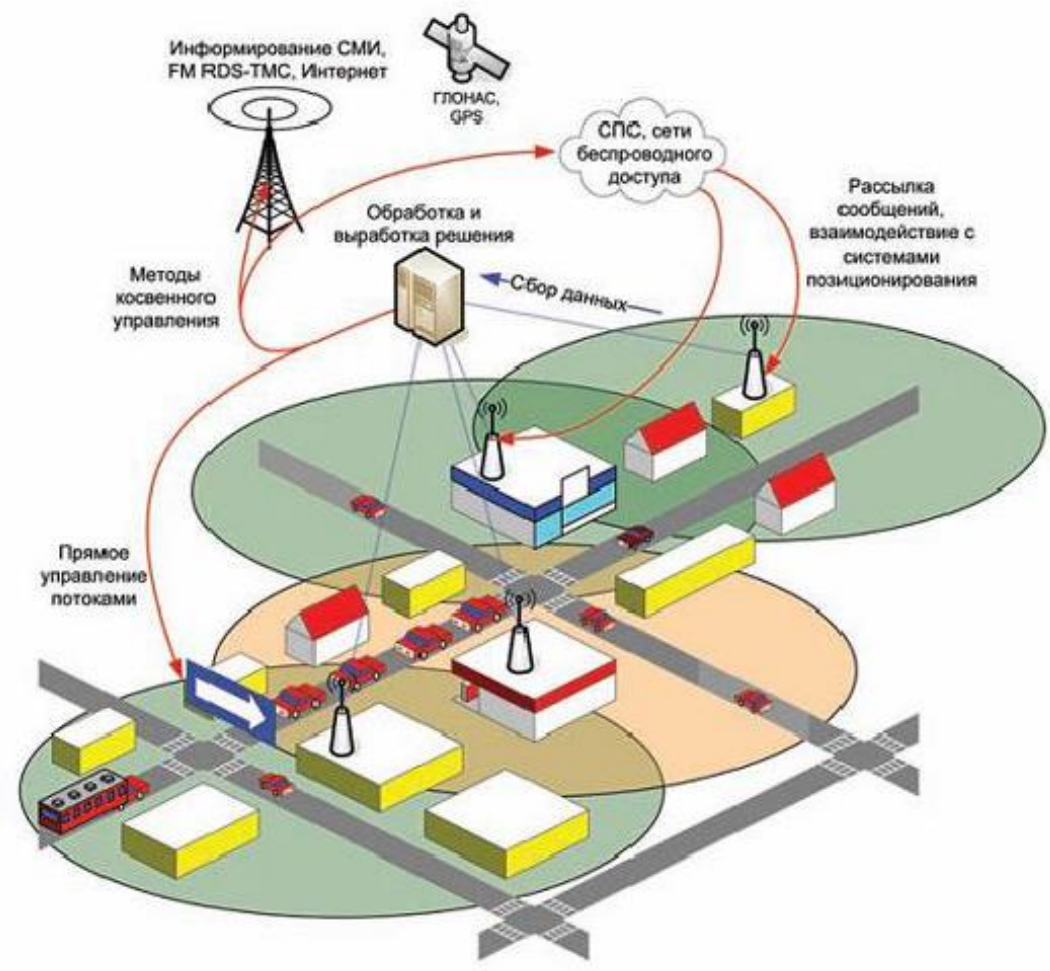


Рис. 9.8. Система интеллектуального управления транспортом

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.

9.6. «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 все - 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 – всѐ 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.

9.7. «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. Видео звонки 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. Развивается «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.

9.8. «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. 9.9), 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 онлайн 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. 9.9. Робот AMMI Electrolux

Компьютеризированная обувь Verb for Shoe («Команда для обуви») компании VectraSense (рис. 9.10) 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.

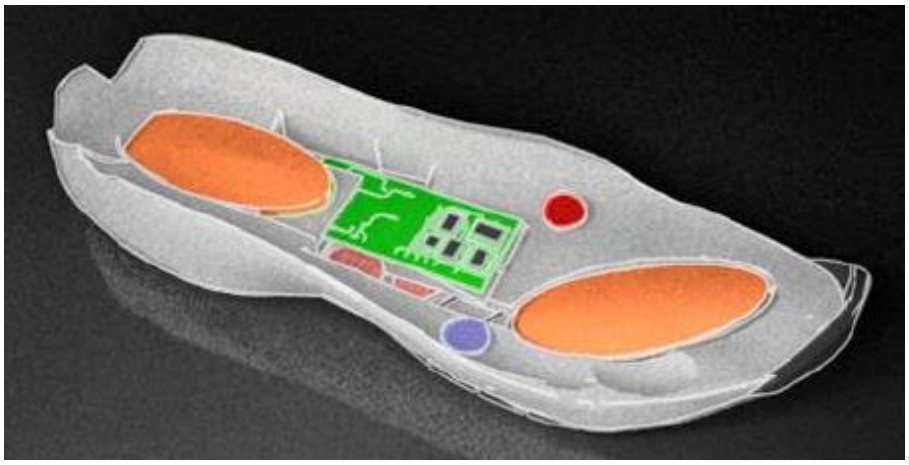


Рис. 9.10. Компьютер, две воздушные камеры, сенсоры и радиопередатчик начинка обуви Verb

Примером умных устройств являются очки Google Glass компании Google (рис. 9.11). 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, видео дневник.

Такие очки позволяют, надев их, получать информацию, дополняющую увиденное. Например, очки смогут распознать местность и подсказать пользователю, что находится поблизости.

Рис. 9.11. Очки-компьютер Google Glass

«Умное» зеркало-гаджет Cybertecture Mirror компании James Law Cybertecture (Япония) (рис. 9.12) 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 стереодинамиками.

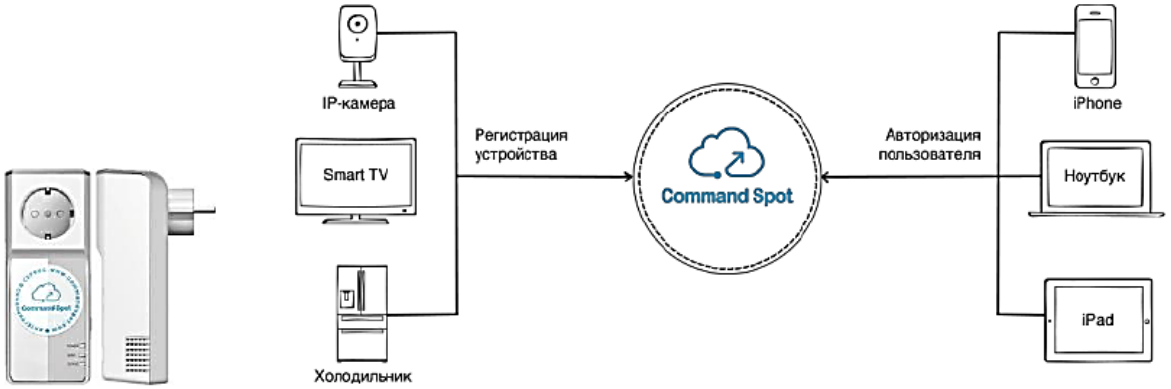
Все необходимые настройки и параметры можно выставить в компьютере и получать на зеркало-экран сообщения с электронной почты, новости с rss-подписки, смотреть фотографии и следить за временем. В перспективе хайтек-зеркало сможет обучаться и подстраиваться под каждого члена семьи, выводя персональные напоминания, календарь и прочую информацию индивидуального характера.

В будущем система сможет получать указания от семейного доктора, считывать RFID-метки и даже демонстрировать видеоролики.

Рис. 9.12. «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. 9.13).

Управление осуществляется с компьютера через интернет-браузер или с мобильных устройств через загружаемое из интернет-магазина облачное приложение.



а) б)

Рис. 9.13. Управление электроприборами через интернет:
а) «умная розетка»; б) схема управления

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

Контрольные вопросы по главе 9

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.

ГЛАВА X. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ IOT

Интернет вещей (IoT) находится только в начале своего пути, но уже развивается с огромной скоростью, и все вводимые новшества добавляют серьёзные проблемы, связанные с информационной безопасностью.

Помимо нарушения конфиденциальности традиционных сетей связи (повторы, подслушивания, искажения информации и т. д.), возникают проблемы с защитой потребительской составляющей. Они обусловлены:

- отсутствием серьёзного ущерба;
- отсутствием стандартов не только защиты, но и взаимодействия;
- отсутствием в наши дни интереса у производителей, как у первой ступени реализации.

Большую угрозу несёт управление устройств с помощью межмашинного взаимодействия. Ни одну написанную человеком программу нельзя считать стопроцентно точной; для неё пишутся различные патчи для исправления ошибок. Такая же участь ждёт датчики в интернет устройствах. И с углублением роли данных устройств в жизни людей будет увеличиваться угроза безопасности всех данных, даже самых незначительных на первый взгляд. Необходимо оценивать любую утекающую информацию, так как резюмирование её составляющих может

представлять опасность для жизни как физических, так и юридических лиц (крупнейших компаний).

В таком случае ещё оказывается важным защищать критически важную инфраструктуру, такую как сеть электропередачи. Необходимо подготовить базу для неожиданного аварийного случая, а также правильное соотношение для открытости и встроенной избыточности.

Одним из самых опасных направлений атаки, на которые стоит обратить внимание, является DDoS-атака. Её цель представляет из себя захват системных ресурсов и затруднение доступа к ним добросовестных пользователей.

Так 21 октября 2016 года в США была совершена серия DDoS-атак, которая привела к глобальному нарушению интернет-деятельности. Поскольку она была направлена на систему доменных имён (DNS), которая получает информацию о доменах, многие повседневные активности, такие как социальные сети или онлайн покупки, стали недоступны на некоторое время. Основные информационные потоки злоумышленников были направлены на сервера компании Dyn, являющейся главным поставщиком DNS-услуг для таких крупнейших компаний, как Twitter, Pinterest, Reddit, GitHub, Etsy, Tumblr, Spotify, PayPal и Verizon. Осуществление таких атак стало возможным благодаря подключению к незащищённым цифровым устройствам: роутерам и камерам видеонаблюдения. Хоть они и не являются мощными компьютерами, но способны генерировать огромные объёмы паразитической информации для серверов, особенно при одновременном подключении.

Эксперты настойчиво заявляют о том, что поставщики услуг и устройств рынка IoT нарушают принцип сквозной информационной безопасности (ИБ), который рекомендован для всех ИКТ-продуктов и услуг. Согласно этому принципу, ИБ должна закладываться на начальной стадии проектирования продукта или услуги и поддерживаться вплоть до завершения их жизненного цикла.

Но что же мы имеем на практике? Вот, например, некоторые данные исследований корпорации HP (лето 2014 года), целью которых было не выявить какие-то конкретные небезопасные

интернет-устройства и уличить их изготовителей, но обозначить проблему ИБ-рисков в мире IoT в целом.

Исследователи HPE обращают внимание на проблемы как на стороне владельцев устройств, так и на проблемы, над которыми должны подумать разработчики. Так, в самом начале эксплуатации пользователю обязательно нужно заменить фабричный пароль, установленный по умолчанию, на свой личный, поскольку фабричные пароли одинаковы на всех устройствах и не отличаются стойкостью. К сожалению, делают это далеко не все. Поскольку не все приборы имеют встроенные средства ИБ-защиты, владельцам также следует позаботиться об установке внешней защиты, предназначенной для домашнего использования, с тем чтобы интернет-устройства не стали открытыми шлюзами в домашнюю сеть или прямыми инструментами причинения ущерба.

В ходе проведенного HP исследования обнаружено, что примерно в 70% проанализированных устройств не шифруется беспроводной трафик. Веб-интерфейс 60% устройств эксперты HP посчитали небезопасным из-за небезопасной организации доступа и высоких рисков межсайтового скриптинга. В большинстве устройств предусмотрены пароли недостаточной стойкости. Примерно 90% устройств собирают ту или иную персональную информацию о владельце без его ведома.

Всего же специалисты HP насчитали около 25 различных уязвимостей в каждом из исследованных устройств (телевизоров, дверных замков, бытовых весов, домашних охранных систем, электроразведок...) и их мобильных и облачных компонентах.

Вывод экспертов HP неутешителен: безопасной экосистемы IoT на сегодняшний день не существует. Особую опасность вещи Интернета таят в себе в контексте распространения целевых атак (APT). Стоит только злоумышленникам проявить интерес к кому-либо из нас, и наши верные помощники из мира IoT превращаются в предателей, нараспашку открывающих доступ в мир своих владельцев.

10.1. Слабые места IoT

- Переход на IPv6.
- Питание датчиков.
- Стандартизация архитектуры и протоколов, сертификация устройств.
- Информационная безопасность.
- стандартные учётные записи от производителя, слабая аутентификация
- отсутствие поддержки со стороны производителе для устранения уязвимостей
- трудно или невозможно обновить ПО и ОС
- использование текстовых протоколов и ненужных открытых портов
- используя слабость одного гаджета, хакеру легко попасть во всю сеть
- использование незащищённых мобильных технологий
- использование незащищённой облачной инфраструктуры
- использование небезопасного ПО.

Насколько безопасны «умные дома будущего».

Ниже компания Panda собрала несколько идей о способах, благодаря которым хакеры могли бы получить беспрецедентный доступ к Вашей повседневной жизни через комплексные устройства, которые расположены у Вас дома.

Т.к. Интернет вещей продолжает интегрировать, казалось бы, бессмысленные и несвязанные объекты, то полноценная домашняя операционная система выглядит вполне вероятной. Хотя это превратит Ваш дом в оптимизированное жизненное пространство, полностью предназначенное для обеспечения Вашего комфорта, тем не менее, она может также нести Вам серьезные риски стать жертвой кибер-атаки в Вашем собственном доме.

Центральное звено любой системы безопасности умного дома будущего – это его замок.

Кстати, недавнее исследование показало, что умные замки пугающе легко можно взломать, в результате чего они не могут

гарантировать выполнение своей основной функции, для которой, собственно говоря, они и существуют.

Выкуп за вход домой?

Существующие системы достаточно просты для кибер-хакеров и не являются препятствием для того, чтобы проникнуть в Ваш дом.

И мы решили подумать дальше: а что если хакеры в будущем смогут использовать это технологическое достижение против Вас?

Если умный замок можно взломать, чтобы его открыть, возможно, хакеры найдут способ, как полностью его закрыть, чтобы Вы не могли его открыть.

В этом случае в будущем можно будет достаточно тихо проникать в чужой дом: хакер сможет контролировать все

события удаленно. Более того, он сможет запрашивать у своих жертв какой-нибудь разумный выкуп за то, чтобы они могли попасть в свои собственные дома.

Кстати, это может быть идеей для сценария какого-нибудь страшного фильма (Совсем один дома), но это ужасная мысль. Если все Ваши устройства безопасности взаимосвязаны, то кибер-преступники потенциально могли бы получить доступ также к Вашей домашней сигнализации и даже ключам от Вашего автомобиля.

Задымленный экран – тревога о пожаре.

Одна функция безопасности, которая уже встроена в некоторые доступные на рынке детекторы дыма, - это возможность, позволяющая умному дому получать информацию (и использовать ее в дальнейшей работе) от других смарт-устройств, что позволяет системе реагировать соответствующим образом в случае опасности. Данная функция внедрена для безопасности пользователя, позволяя домашней системе, которая обнаружила пожар, например, разблокировать все двери в доме, чтобы помочь выбраться из него как можно быстрее.

Это отличный пример того, как производители IoT-решений работают над прозрачной интеграцией и взаимодействием смарт-устройств внутри умного дома.

Однако есть одна оговорка: если эта технология будет использоваться кибер-преступниками, то существует вероятность создания нежелательной цепной реакции, которая в конечном итоге может, наоборот, снизить уровень безопасности умного дома.

Еще один способ, когда хакер мог бы потенциально издалека навредить, - это создание ложной тревоги о пожаре, которая отправляется в пожарные службы. Хаотическая сцена может выглядеть в виде задымленного экрана, что также в итоге может сделать Вас легкой добычей для других потенциально вредоносных кибер-атак.

Пылесос смерти.

Наверное, это одна из наших «уайлдеровских» идей, но если вспомним про фурор, который произвел на всех самовзрывающийся смартфон, то не будем удивляться и тому, что IoT-устройства все чаще ставят нас в такое положение,

которое предоставляет хакерам доступ к потенциально взрывоопасным устройствам!

Можно ли использовать IoT-устройства для кибер-атаки? Легко.

Злоумышленники, как правило, работают на массы: например, распределенные атаки на отказ в обслуживании (DDOS), когда тысячи электронных писем или запросов отправляются на какой-то сервер, чтобы замедлить его работу или вообще вывести его из строя.

В этом случае в будущем мы можем столкнуться с ситуациями, когда хакеры попытаются «завалить» как можно больше машин в надежде на то, что какая-то их часть будет работать неправильно, что приведет к тяжелым последствиям. Вообще-то, пугающая перспектива. Возможно, как раз по этой причине правительственные органы говорят о потенциальных опасностях Интернета вещей, связанных с кибер-атаками.

Остерегайтесь холодильника.

Помните эпизод в «Симпсонах», когда Мардж нападает на домашнюю операционную систему с искусственным интеллектом, озвученную Пирсом Броснаном, которая готовит еду, но тайно планирует «избавится» от остальных членов семьи? Да, конечно, это забавная пародия, но смущает то, что нам потребуется всего несколько технологических достижений, чтобы эти события уже перестали быть смешными, а оказались ужасной действительностью.

Хорошо, допустим, что Ваш холодильник пока не ведет с Вами интеллектуальных бесед, и уж тем более, не прорабатывает какие-то убийственные схемы в отношении Вашей семьи. Однако еще два года назад ЦРУ отметили угрозу со стороны смарт-холодильников в умных домах. К чему бы это?

ЦРУ всполошилось от того, что холодильник использовался как часть бот-сети для выполнения DDOS-атаки. И все это происходило совершенно незаметно для хозяина этого холодильника, который даже и понятия не имел о том, что его смарт-устройство может выполнять какие-то дьявольские действия, кроме как охлаждать и сохранять еду.

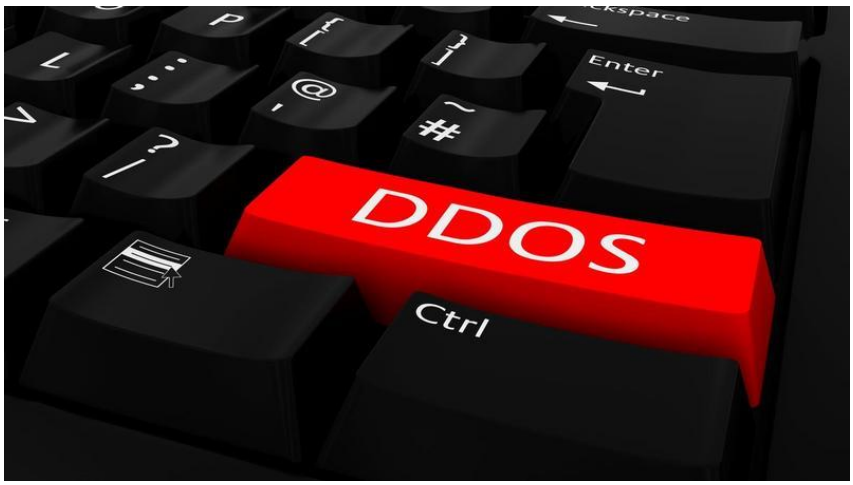
Что дальше?

Т.к. смарт-устройства становятся все умнее, отслеживая Ваши покупательские предпочтения и осуществляя заказы на дом, мог бы хакер получить доступ к Вашим банковским данным или вмешаться в Ваши покупки? Мы все знаем, что искусственный интеллект и холодильники лучше оставить как жуткое видение в мультиках, а не ужас в реальной жизни!

10.2. Сертификация устройств IoT для защиты от хакеров

11 октября 2016 года стало известно о планах Еврокомиссии - ввести обязательную сертификацию или другую аналогичную процедуру всех приборов, подключаемых к интернету вещей. Предполагается принять меры на государственном уровне, что должно помешать хакерам использовать интернет вещей для создания ботнетов.

Как вариант, не исключается установка на устройства сети специальных унифицированных чипов, которые обезопасят их от атак хакеров. Эти меры, по мнению чиновников Еврокомиссии, должны повысить уровень доверия к интернету вещей в обществе и помешать хакерам создавать ботнеты из подключаемой техники.



В группу приборов, подключаемых к интернету, входят видеокамеры, телевизоры, принтеры, холодильники и другая техника. Большая часть этих устройств неудовлетворительно защищена от хакерских атак. Сами по себе эти устройства могут не представлять интереса для преступников.

Однако хакеры взламывают их, чтобы использовать в качестве роботов для создания ботнетов, посредством которых можно атаковать более серьезные системы. Большинство владельцев взломанных устройств даже не подозревают, как используется их техника.

В качестве примера приведена масштабная DDoS-атака на интернет-ресурс Krebs On Security, в сентябре 2016 года.

По данным Gartner, к интернету вещей подключено около 6 млрд приборов, а к 2020 году их число достигнет 20 млрд, что создаст хакерам более широкие возможности для проведения масштабных атак посредством ботнетов.

На сайте National Institute of Standards and Technology (NIST) можно обнаружить документ «Draft NISTIR 8200. Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)». Версия датирована февралем 2018, и пока все еще носит статус драфта. Там проводится анализ существующих стандартов, распределенных по следующим 11 областям: Cryptographic Techniques, Cyber Incident Management, Hardware Assurance, Identity and Access Management, Information Security Management Systems (ISMS), IT System Security Evaluation, Network Security, Security Automation and Continuous Monitoring (SACM), Software Assurance, Supply Chain Risk Management (SCRM), System Security Engineering.

Перечень стандартов занимает больше ста страниц! Значит, там содержатся сотни наименований, это десятки тысяч страниц, на изучение которых могут уйти годы, к тому же, многие документы являются платными. При этом идентифицированы множественные пробелы в стандартизации отрасли, которые, очевидно, будут заполняться.

Думаю, читатель уже понял, на стороне какого подхода находится здравый смысл и симпатии автора. Поэтому, вернемся к лучшим практикам ENISA. Они базируются на анализе около сотни уже выпущенных документов. Однако, нам не надо читать все эти документы, поскольку эксперты ENISA уже собрали в своем отчете все самое важное.

Ниже на рисунке представлена структура документа, и мы с ней сейчас детально ознакомимся.

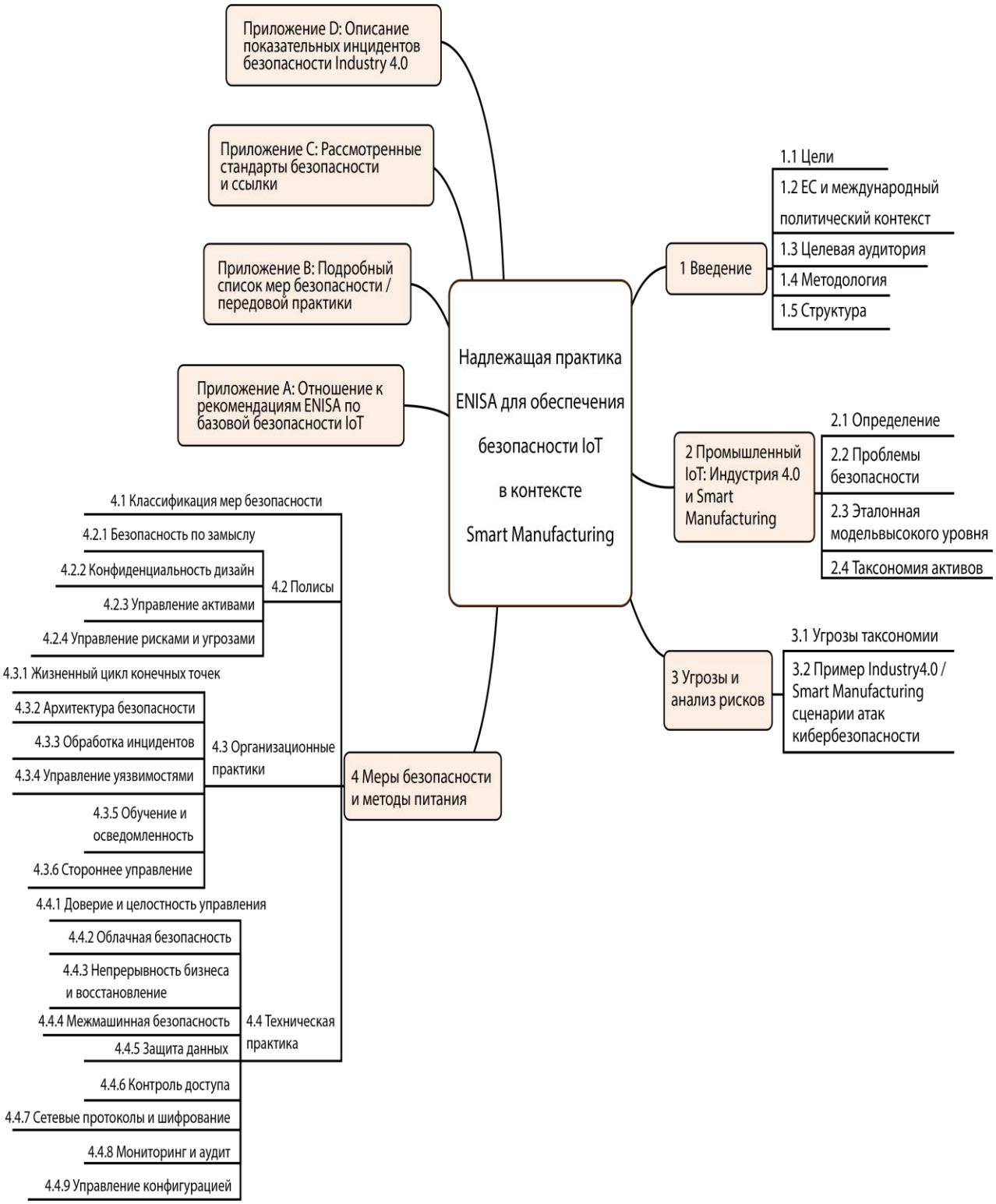


Рис. 10.1 Структура документа «Good Practices for Security of Internet of Things in the context of Smart Manufacturing»

Первая часть является вводной.

Во второй части сначала приводится базовая терминология, а затем вызовы в обеспечении безопасности, к которым относятся:

- уязвимые компоненты (Vulnerable components);
- недостатки в управлении процессами (Management of processes);
- возрастающее количество коммуникационных связей (Increased connectivity);
- взаимодействие операционных и информационных технологий (IT/OT convergence);
- наследование проблем АСУ ТП (Legacy industrial control systems);
- небезопасные протоколы (Insecure protocols);
- человеческий фактор (Human factors);
- избыточная функциональность (Unused functionalities);
- необходимость учета аспектов функциональной безопасности (Safety aspects);
- реализация обновлений, связанных с ИБ (Security updates);
- реализация жизненного цикла ИБ (Secure product lifecycle).

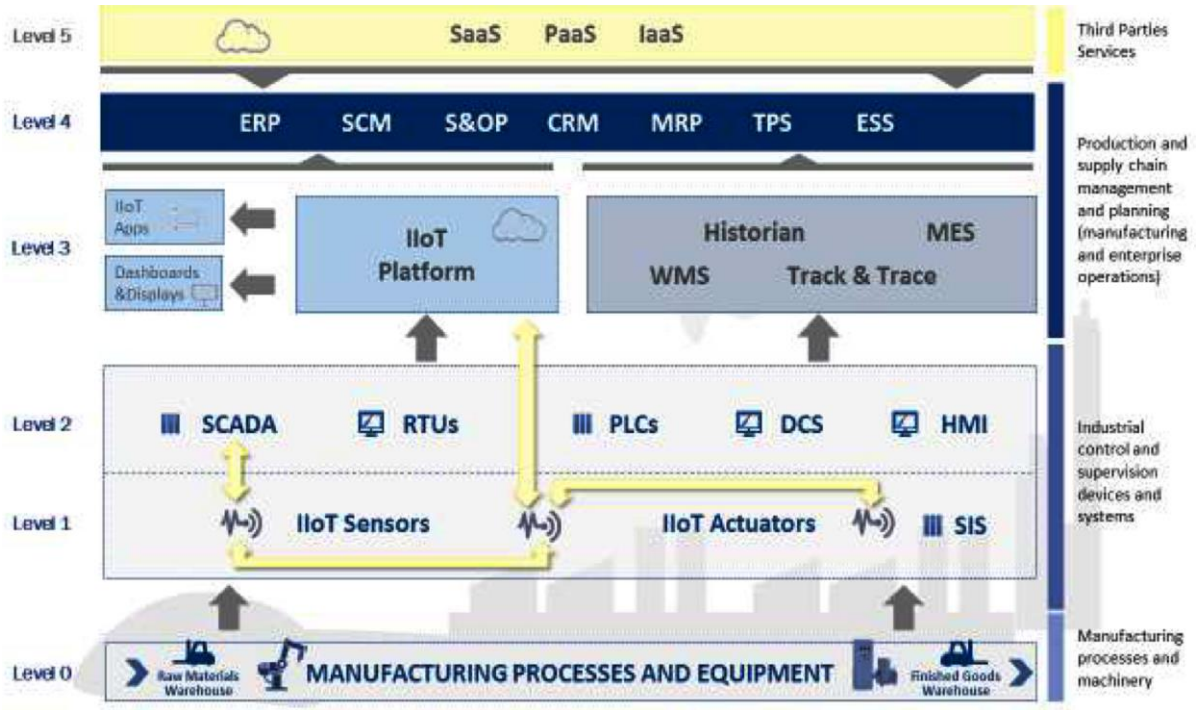


Рис. 10.2. Референсная архитектура IIoT

Референсная архитектура является входом для формирования таксономии активов. На основании экспертных данных оценена критичность активов с точки зрения их влияния на ИБ.

О репрезентативности речь не идет (в отчете сказано, что участвовали эксперты от 42 различных организаций), и можно воспринимать эту статистику, как «некоторое мнение». Проценты на диаграмме означают процент экспертов, которые оценили тот или иной актив, как наиболее критичный.

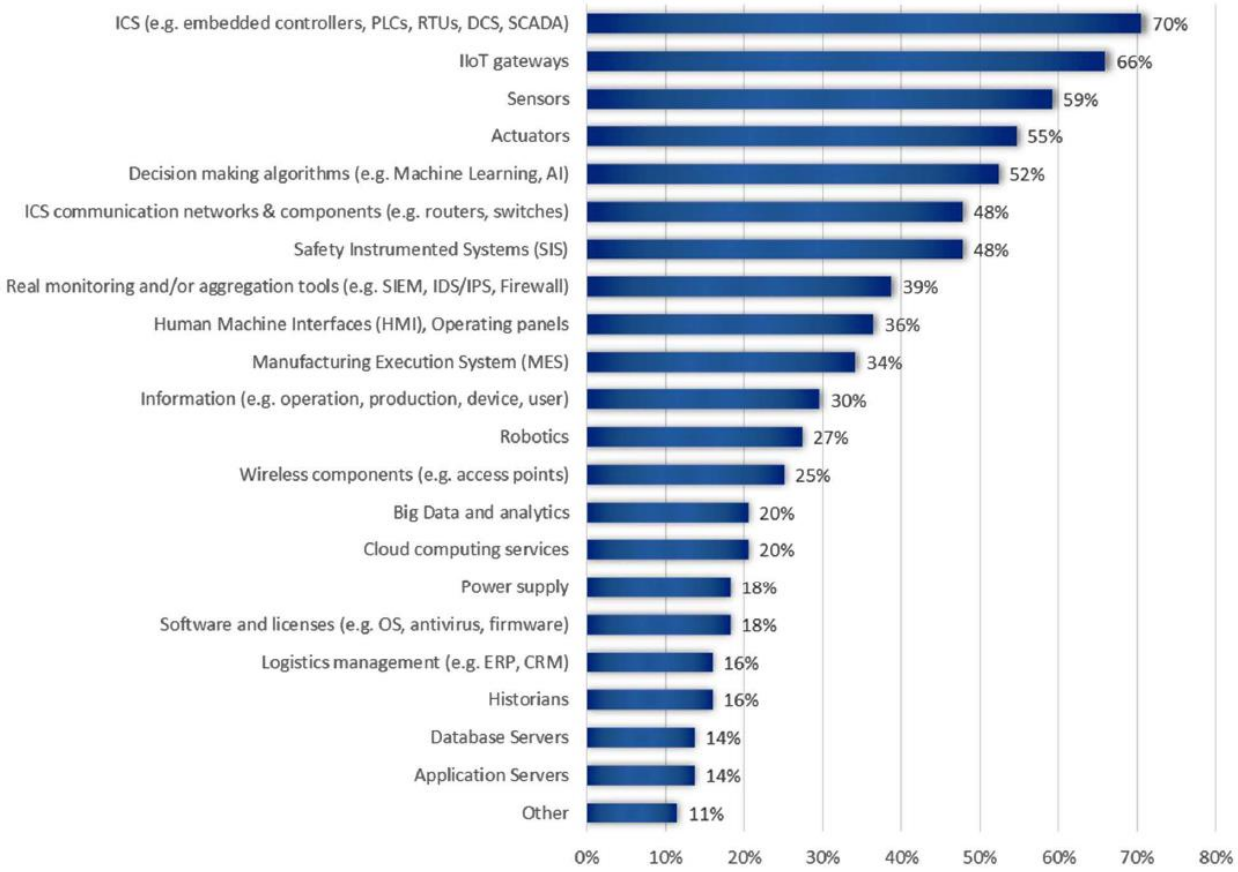


Рис. 10.3. Результаты экспертной оценки критичности активов IIoT

В разделе 3.1 выполнена классификация и описание возможных угроз, применительно к области IIoT. Кроме того, к каждой из угроз привязаны классы активов, которые могут быть затронуты. Выделены основные классы угроз:

- Nefarious activity / Abuse (недобросовестная деятельность и злоупотребления) – различного рода манипуляции, производимые с данными и устройствами;

- Eavesdropping / Interception / Hijacking (прослушивание / перехват / хакинг) – сбор информации и взлом системы;
- Unintentional damages (accidental) (непреднамеренные случайные повреждения) – ошибки в конфигурировании, администрировании и применении;
- Outages (отключения) – перебои в работе, связанные с потерей электропитания, коммуникаций или сервисов;
- Disaster (катастрофы) – разрушительные внешние воздействия природного и техногенного характера;
- Physical attack (физические атаки) – воровство, вандализм и саботаж (вывод из строя), производимый непосредственно на оборудовании;
- Failures / Malfunctions (отказы и нарушения в работе) – могут происходить по причине случайных отказов аппаратных средств, по причине отказов сервисов провайдера, а также из-за проблем в разработке программного обеспечения, приводящего в внесение уязвимостей;
- Legal (правовые вопросы) – отклонения от требований законов и контрактов.

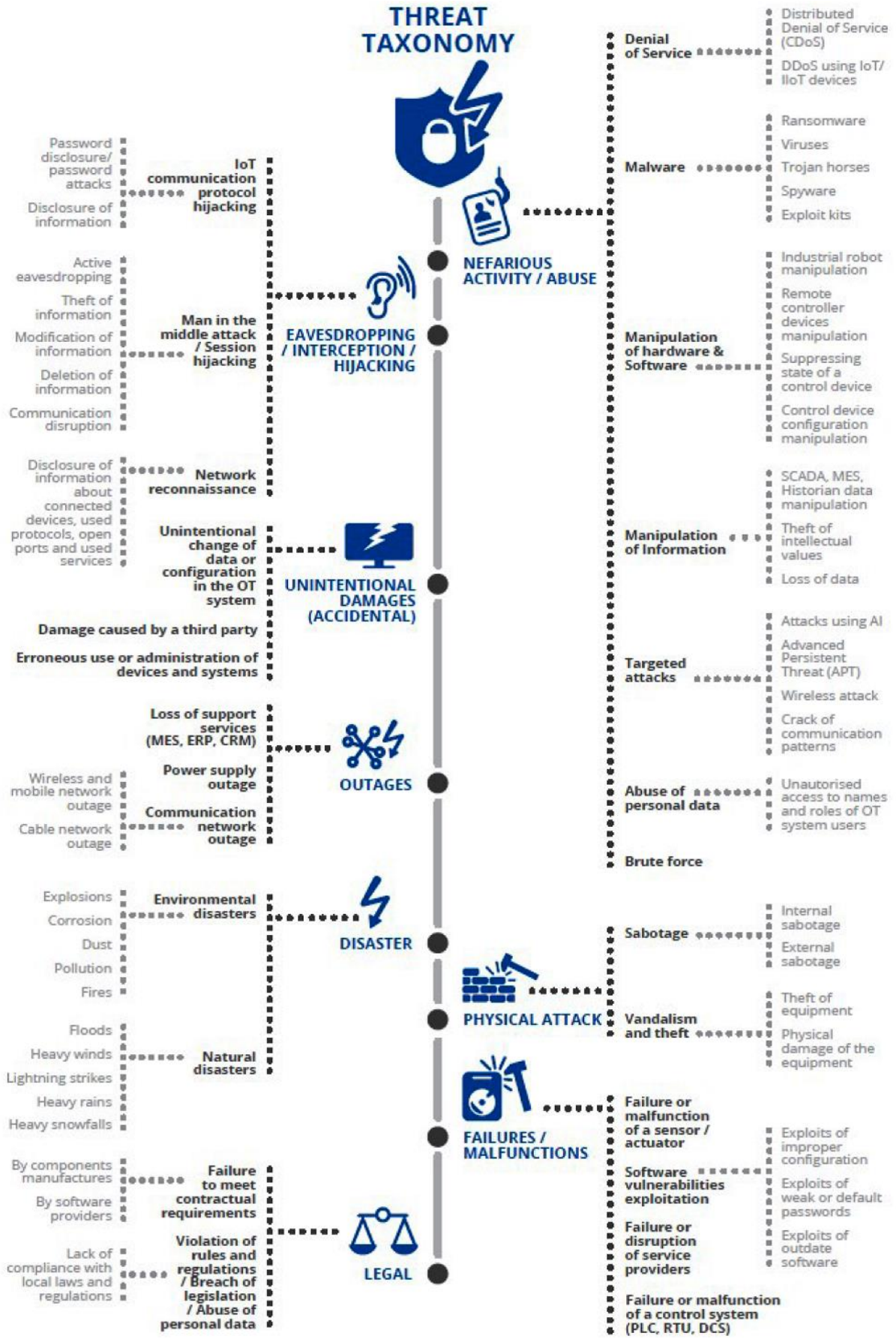


Рис. 10.4. Таксономия угроз

В разделе 3.2 рассмотрены типовые примеры атак на компоненты систем IIoT.

Самый важный раздел в документе – это 4-й, в котором рассмотрены лучшие практики, направленные на защиту компонентов IIoT. В практики включены три категории: политики, организационные практики и технические практики.

Рис. 10.5. Структура лучших практик обеспечения ИБ IIoT

Принципиальное различие политик и организационных практик не объяснено, а процедурный уровень присутствует в обоих случаях. Например, Risk and Threat Management попали в политики, а Vulnerability Management – в организационные практики. Единственное различие, которое можно уловить, это то, что политики применяются, в первую очередь, для разработчиков, а организационные практики – для эксплуатирующих организаций.

В составе политик (4.2) описаны 4 категории и 24 практики. В организационном разделе (4.3) описано 27 практик, разделенных на 6 категорий, а в техническом (4.4) – 59 практик, разделенных на 10 категорий.

В Приложении А отмечено, что настоящим документом ENISA продолжает исследования, задекларированные в 2017 г. в

документе «Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures». Конечно, IoT более широкое понятие, чем IIoT, и, с этой точки зрения, можно было бы взять прошлогодний документ за основу этого обзора, однако, всегда хочется иметь дело с более новым материалом.

Приложение B – эта основная смысловая часть документа. Перечень практик из раздела 4 изложен в виде таблиц, где сделана привязка к группам угроз и даны ссылки на документы, поддерживающие применение той или иной практики, правда, к сожалению, без указания конкретной страницы или параграфа. Вот, например, несколько пунктов, относящихся к безопасности облачных сервисов.

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
Cloud security	TM-10: Locate critical systems and applications within the private or at least hybrid deployment models. If you consider utilisation of a public cloud, precede this decision with risk analysis.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Failures / Malfunctions	• Cloud Security Alliance - Future Proofing the connected world • Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • Online Trust Alliance - IoT trust framework 2.5
Cloud Security	TM-11: To mitigate the risk related to cloud attacks, adopt a zero-knowledge security approach. It means that providers of services should store and manage data without access to encryption keys. Protect all the data within the cloud and data in transfer. Ideally, all data should be encrypted. Application and interfaces should be secured as well.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking	• Federal Office for Information Security (BSI) - BSI-Standards 100-4 - Business Continuity Management • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements • NIST - NIST Advanced Manufacturing Series 300-1 Reference Architecture for Smart Manufacturing Part 1: Functional Models • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile

Рис. 10.6. Фрагмент описания лучших практик обеспечения ИБ IIoT

В Приложении C дан перечень цитируемых документов (их всего около 100), которые были проработаны и легли в основу разработанных лучших практик.

В Приложении D перечислены самые значимые инциденты, связанные с нарушением ИБ в промышленных приложениях.

Прогноз развития устройств IoT был экспоненциальный, и, согласно оценкам, к 2020 году свыше 50 миллиардов устройств будут подключены к Интернету. При таком темпе роста очень критично встаёт вопрос безопасности устройств в случае

отсутствия процессов, обеспечивающих целостность и шифрование данных.

Все сведения, которые хранят устройства IoT являются высоко востребованными, потому что показывают целостную картину повседневных действий и привычек пользователей. А наличие баз данных такого содержания является полезным для различных компаний, которые могут направить свои ресурсы на производство товаров и услуг, сосредоточенных на привычках и предпочтениях масс. То, что может помочь свести к минимуму проблемы — это шифрование и специальные системы защиты для загрузки и хранения данных в облаке.

Контрольные вопросы по главе 10

1. Перечислите слабые места IoT.
2. Насколько безопасны «умные дома будущего»?
3. Можно ли использовать IoT-устройства для кибер-атаки?
4. Перечислите основные классы угрозы.

ГЛАВА XI. ПЕРСПЕКТИВЫ РАЗВИТИЯ IOT В УЗБЕКИСТАНЕ

Интернет вещей является одной из наиболее перспективных ИТ-отраслей. По данным компании Microsoft, к 2020 году в мире ожидается появление до 30 млрд устройств интернета вещей, а экономическая выгода обществу и бизнесу от цифровой трансформации к 2025 году оценивается в 100 трлн долларов.

Одним из наиболее перспективных направлений повышения эффективности корпораций является интернет вещей наряду с корпоративной мобильностью, так как IoT-инвестиции отличаются сравнительно невысокими капитальными затратами, позволяя значительно улучшить финансовые показатели организаций даже при их установке на имеющееся оборудование.

Экономия происходит за счет исключения человека из определенных фаз бизнес-процесса. Примерами может служить модернизация с помощью IoT инфраструктуры ЖКХ или сетей электроснабжения, повсеместное внедрение умных датчиков в АСУ ТП и т.д.

По прогнозам аналитиков, Gartner, к 2020 году технологии IoT будут использоваться в 95% отраслей – от электроники для разработки новых продуктов.

Аналитическая компания прогнозирует, что программно-аппаратные продукты с поддержкой IoT с активацией со смартфона появятся в начале 2019 года.

Жизненный цикл интернета вещей в отличие от многих других ИТ-инноваций продлится значительно дольше, чем просто несколько лет.

По данным всемирного исследования PwC Digital IQ® за 2017 год, IoT занимает первое место среди восьми прорывных технологий, способных изменить бизнес-модели компаний или целых индустрий, опережая в этом рейтинге искусственный интеллект, дополненную реальность, технологию, связанную с созданием дронов и управлением ими, блокчейн и ряд других.

IoT также находится на первом месте в рейтинге, учитывающем уровень инвестиций в новые и перспективные технологии.

Рис. 11.1. Рейтинг технологий, составленный с учетом степени их влияния на бизнес-модели компаний или целых отраслей (представлена доля респондентов, участвовавших в опросе и выделивших определенную технологию)

Рис. 11.2. Рейтинг технологий, составленный с учетом их инвестиционной привлекательности

У IoT есть важные преимущества перед другими прорывными технологиями. Во-первых, IoT-технологии могут широко применяться как для обслуживания потребителей, так и в бизнесе в целом.

С другой стороны, для начала использования IoT уже есть в той или иной степени готовая инфраструктура – мобильные и фиксированные сети, а дальнейшее внедрение (сенсоры, приложения, платформы) достаточно дешево.

Распространение IoT в мире стало возможным благодаря четырем технологическим трендам:

• снизилась стоимость вычислительных мощностей (процессоров, памяти и систем хранения данных);

• снизилась стоимость передачи данных;

• благодаря развитию «облачных» технологий и «больших данных» становятся доступными гибкие системы хранения и анализа данных, несмотря на постоянное увеличение объема получаемой информации;

• быстро растет число «подключенных» устройств.

Однако развитие IoT связано не только с новыми технологиями, но и с созданием технологической экосистемы и разработкой ряда предложений для сбора, передачи и агрегации данных и платформы, позволяющей обработать эти данные и использовать их для реализации «умных решений». «Интернет вещей» уже становится реальностью.

Бизнесу IoT позволяет получить конкурентное преимущество за счет снижения затрат и развития новых источников дохода. Потребительский рынок все активнее заполняют «умные» технологии: например, по результатам опроса PwC в США, устройства с технологией «умного дома» использует каждый четвертый потребитель.

Мы считаем, что за счет применения технологий IoT взаимодействие объектов, среды и людей будет крайне активным, благодаря чему можно надеяться на то, что мир станет «умным» и более благоустроенным для человека. Постоянный и увеличивающийся обмен данными требует развития новых сервисов, которые должны соединить нас с физическим миром вокруг.

Эти сервисы также должны быть построены на полностью новых бизнес-моделях и обеспечить новые финансовые потоки.

Применение технологий IoT в Узбекистане сопряжено с рядом особенностей и ограничений, связанных с экономической, технологической, законодательной, географической и культурной спецификами страны.

На потребительском рынке сдерживающим фактором является низкий уровень дохода населения, на рынке коммерческих компаний – длительность процесса принятия решений о внедрении новых технологий, короткий горизонт планирования компаний, сложность изменения внутренних процессов, регламентов, документооборота и подходов к получению и обработке информации, сложность интеграции технологий IoT в существующую IT-среду.

По нашему мнению, важно учитывать мультипликативное воздействие, которое технологии IoT окажут на отрасли экономики за счет повышения производительности труда и сокращения затрат. Достижение данного эффекта зависит от системности подхода к внедрению IoT в Узбекистане.

Важную роль в этом процессе должно выполнять государство, в распоряжении которого есть различные инструменты: совершенствование регуляторной базы, развитие механизмов поддержки IoT, создание условий для развития кадрового потенциала, продвижение российского опыта за рубежом. В случае продуманного и системного подхода IoT может стать одним из факторов роста экономики Узбекистана в долгосрочной перспективе.

Применение технологий IoT изменит облик многих индустрий и областей жизнедеятельности – как с учетом экономической составляющей, так и с точки зрения потребительского опыта.

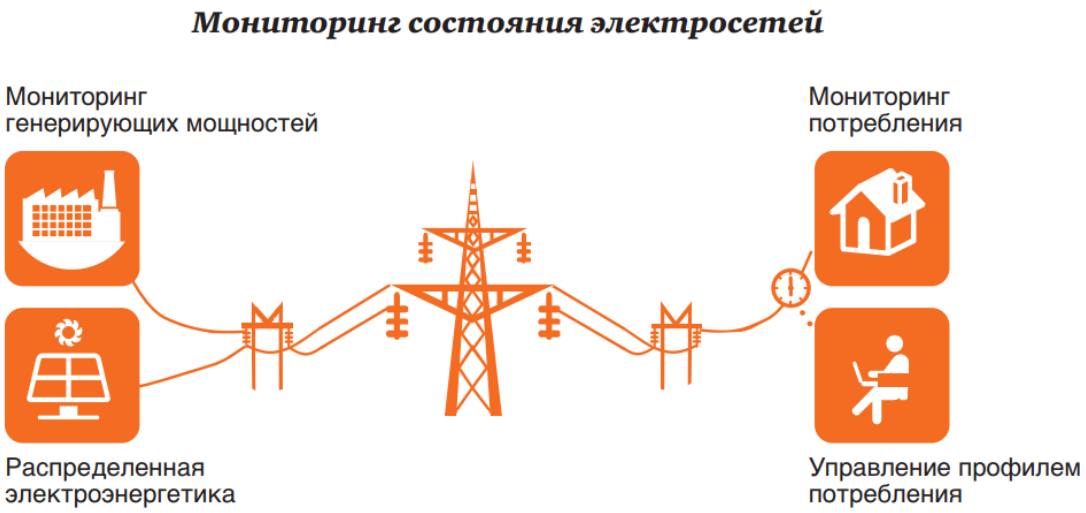
В ряде областей человеческие трудозатраты и ошибки будут сведены к минимуму. Так, IoT в электроэнергетике кардинально изменит технологии, обеспечит экономию средств и создаст новые продукты во всех звеньях энергосистемы. В сельском хозяйстве IoT позволит внедрить точное земледелие и значительно усовершенствовать управление сельхоз транспортом.

Решения IoT в логистике помогут сократить затраты, повысить прозрачность цепочки доставки товаров и сократить использование человеческого труда. Технологии «умного города» позволят создать более привлекательную городскую среду с эффективно работающей транспортной системой, ЖКХ, удобной инфраструктурой и обеспечить безопасность населения.

Среди компонентов «умного дома» наибольшей популярностью у потребителей пользуются устройства повышения безопасности, контроля потребления воды и энергии, «умные» бытовые приборы и термостаты.

В ходе подготовки настоящего исследования специалисты PwC опросили более десяти руководителей энергетических компаний, и большинство из них сошлись во мнении о том, что в будущем все три звена электроэнергетики – генераторы, сети и потребители – должны стать «умными».

Глубокая интеграция всех участников рынка, к которой ведут технологии IoT, позволит в каком-то смысле преобразить электроэнергетику. На смену иерархичной системе «производство – передача – сбыт», в которой все процедуры жестко определены регламентами, согласованность достигается за счет государственного регулирования, а участники узнают о действиях друг друга из новостей, придет гибкая система продуктивного взаимодействия в режиме реального времени. Каждый элемент системы будет «видеть» другие элементы, понимать их возможности и потребности и использовать свой потенциал наилучшим образом. Данное изменение позволит выйти на принципиально новый уровень надежности и эффективности в работе энергетической системы.



При этом важно понимать, что процессы цифровизации сетей, генерации и потребительского сектора должны идти параллельно. «Умная сеть» без «умного потребителя» работать не будет.

Ключевыми сферами во всех элементах электроэнергетики, на которые повлияет внедрение IoT, являются:

• технологии, в том числе повысится их надежность;

• экономичность, в том числе сократятся затраты;

• появление новых рынков, создание новых свойств и бизнесов.

Рис. 11.3. Ключевые области выгод от применения IoT в электроэнергетике

11.1. IoT в здравоохранении

Решения, разработанные при помощи IoT, начинают занимать свою нишу в сфере здравоохранения. Технологии IoT помогают повысить эффективность работы медицинских учреждений, сократить время пребывания в стационаре, предоставить пациентам новые сервисы для контроля здоровья, собирать и анализировать дополнительную информацию о ходе лечения и т. д., например, дистанционный мониторинг здоровья помогает снизить затраты за счет оперативного контроля медицинских показателей и упростить взаимодействие между врачами и пациентами.

Медицинская диагностика включает различные инструменты измерений, и потенциал IoT в этой области практически безграничен. Помимо методов «традиционной» визуализации (например, ультразвуковой, магнитно-резонансной и компьютерной томографии) и лабораторной диагностики все большее распространение в области клинической диагностики приобретают микродатчики и нано сенсоры.

Сегодня уже доступны нано масштабные биочипы, которые позволяют проводить сверхчувствительный анализ как in vivo, так и в лабораторных условиях. Уже достигнут значительный прогресс при использовании наносенсоров, которые помогают обнаружить биомаркеры рака и инфекционные микроорганизмы при проведении молекулярной диагностики и геномики.

Рис. 11.4. Области применения IoT в здравоохранении

Большой потенциал применения есть у IoT в области мониторинга пациентов в операционных, отделениях неотложной помощи, отделениях интенсивной терапии и послеоперационной помощи стационаров. В этом случае могут использоваться датчики для измерения широкого спектра клинических признаков (ЧСС, артериальное давление, пульс, активность головного мозга и т. п.).

В режиме реального времени данные передаются на мониторы сотрудников, которые осуществляют уход за больными. Современные интеллектуальные системы дистанционного мониторинга состояния пациентов способны не только отслеживать и отображать широкий спектр измерений, поступающих из различных не инвазивных и имплантируемых датчиков, но и анализировать эти данные в реальном времени и прогнозировать неблагоприятные события.

На рынке уже представлены приборы, позволяющие идентифицировать и мгновенного предупреждать об изменениях показателей, которые могут указывать на такие осложнения, как инсульт или сердечная недостаточность. Для мониторинга приема лекарственных средств хорошо зарекомендовали себя встроенные в таблетки микродатчики, которые помогают отслеживать прием лекарств и соответствие установленному графику. При контакте с желудочным соком микродатчик передает сигнал на носимое устройство пациента, а оттуда – на мобильное устройство и далее в электронную медицинскую карту.

Помимо этого, проглатываемые микродатчики дают возможность отслеживать ряд других показателей, таких как ЧСС, температура и параметры физической нагрузки. Устройства IoT также участвуют в решении ряда управленческих, административных и логистических задач, таких как мониторинг и управление человеческими ресурсами, удаленная диагностика медицинского оборудования, локальное позиционирование персонала, пациентов и переносных устройств, управление запасами медикаментов и расходных материалов и пр.

Например, представленные на рынке решения могут осуществлять контроль остатков медикаментов и в реальном времени сообщать о необходимости пополнить запасы. Системы

локального позиционирования могут отслеживать и сообщать текущее местоположение переносного оборудования и других объектов. Кроме того, они могут отслеживать перемещение персонала, пациентов и посетителей медицинских учреждений.

11.2. Применение IoT в сельском хозяйстве

По прогнозам ООН, к 2050 году будет необходимо производить на 70 % больше продуктов питания, чем сейчас, чтобы прокормить растущее население Земли.

Для сельского хозяйства это означает регулярный и постоянно растущий спрос на сельскохозяйственную продукцию, а также появление ряда новых вызовов и принципиально новых требований к уровню производительности в целом. «Умное сельское хозяйство» ставит перед собой цель максимально автоматизировать сельскохозяйственную деятельность, повысить урожайность и качество продукции. Точное земледелие (GPS, датчики, дроны) – это широкий спектр технологий от планирования посева и подготовки почвы, мониторинга состояния и управления посевом, контроля уровня влажности, минерализации почвы и температурного режима до сбора самого урожая.

Точное земледелие призвано оптимизировать операционные расходы и повысить урожайность (в среднем на 15–20 %), которые достигаются путем:

• сокращения объемов используемых семян, агрохимикатов, удобрений и воды (использование «по потребности»);

• более эффективного использования земли: с учетом особенностей того или иного участка определяется агрокультура с наибольшей урожайностью, а также оптимальная методика выращивания и ухода для максимизации урожайности.

При использовании «умных теплиц» (датчики, устройства и ПО для удаленного управления теплицами) операционная экономия достигается путем более эффективного расхода удобрений, химикатов, а также воды. Технология также позволяет оптимизировать количество персонала, который нужен для ухода за культурами, и снизить потери, возникающие из-за человеческого фактора.

Рис. 11.5. Области применения IoT в сельском хозяйстве и животноводстве

«Умные фермы» (датчики, устройства и ПО для мониторинга) позволяют повысить производительность животных и качество продукции. По оценке экспертов рынка, автоматизированные системы откорма, дойки и мониторинга здоровья поголовья скота могут повысить надои на 30–40 %.

11.3. Применение IoT в городской среде

Технологии IoT глубоко проникли в городскую среду в рамках инициатив по развитию «умного города», позволяя повысить уровень жизни и безопасности населения и, таким образом, улучшить экономику города. В России такие технологии уже начинают массово внедряться в мегаполисах. Внедрение IoT в городскую среду повышает эффективность управления транспортной системой, городской инфраструктурой и объектами жилищно-коммунального хозяйства, обеспечивает сохранение здоровья и безопасность населения.

Рис. 11.6. Области применения IoT в городской среде

Транспортная система Транспортная система города может увеличить пропускную способность дорог за счет адаптивного управления дорожным движением: видеокамеры и датчики движения в режиме реального времени передают данные в единый диспетчерский центр, благодаря чему формируется динамическая модель транспортных потоков.

«Умные светофоры» автоматически регулируют продолжительность «красного» и «зеленого» сигналов, перенаправляя транспортные потоки с загруженных участков. Вдоль дорог устанавливаются электронные табло для информирования участников движения о текущей дорожной обстановке. Кроме того, осуществляется мониторинг парковочного пространства.

Контрольные вопросы по главе 11

1. Расскажите применение технологий IoT в Узбекистане.
2. Перечислите ключевые области выгод от применения IoT в электроэнергетике.
3. Расскажите области применения IoT в здравоохранении.
4. Расскажите области применения IoT в сельском хозяйстве и животноводстве.
5. Расскажите области применения IoT в городской среде.

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.

«Всеохватывающему Интернету» (Internet of Everything, IoE) превращает информацию в конкретные действия, создающие новые возможности, расширяющие опыт пользователя и формирующие благоприятные условия для развития стран, компаний и пользователей.

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
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
RFD (Reduced Function Device) – устройство с ограниченным набором функций
RFID (Radio Frequency IDentification) – радиочастотная идентификация RO (Read Only) – только чтение
SMS (Short Messaging Service) – служба коротких сообщений
SOA (Service-Oriented Architecture) – сервис-ориентированная архитектура 129
SOAP (Simple Object Access Protocol) — простой протокол доступа к объектам
SOP (Self-Organization Protocol) – самоорганизующийся протокол
SPA (Simple Power Analysis) – простой анализ мощности
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
ИК – инфракрасный
КПД – коэффициент полезного действия
КПК – карманный персональный компьютер
ЛВС – локальная вычислительная сеть
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

СПИСОК ЛИТЕРАТУРЫ

1. Богородицкая, И.А. M2M – новые возможности для развития сотового бизнеса [текст] /И.А. Богородицкая // Электросвязь. – 2012. – №1. – С. 38-39.
2. А. В. Росляков, С. В. Ваняшин, А. Ю. Гребешков - Интернет вещей /учебное пособие/Самара – 2015.
3. Бхуптани, М. ID-технологии на службе вашего бизнеса [текст] / М. Бхуптани, Ш. Морадпур. – М.: Альпина Паблишер, 2007. – 290 с.
4. Васильков, А. Микрокомпьютеры для интернета вещей: от умного дома к поумневшему окружению [текст] / А. Васильков // Компьютерра, 14 июня 2013г.
5. Гиббс, М. Интернет вещей – не только для «умных» [текст] / М. Гиббс // Сети/network world. – 2013. – №3
6. Голышко, А. Строим «интеллектуальный городок» [текст] / А. Голышко // Мобильные телекоммуникации. – 2013. - №10. – С. 46-51
7. Гудин, М. Технология RFID: реалии и перспективы [текст] / М. Гудин, В. Зайцев //Компоненты и технологии. – 2003. – №4.
8. Дроздов, С. Eurotech, «интернет вещей» и «облако устройств» [текст] / С. Дроздов, С. Золотарев // Control Engineering Россия. – 2012. - № 8(78). – С. 18-24.
9. Каледин, В.В. NFC в мобильных сетях: перспективы и пути развития [текст] / В.В. Каледин, В.М. Полионов // Электросвязь. – 2011. – №5. – С. 10-14.
10. Коржов, В. Опасный Интернет вещей [текст] / В. Коржов // Открытые системы. СУБД. – 2013. – №4. – С. 29-30.
11. Круз, Л. Сотовые телефоны станут датчиками? [текст] / Л. Круз // Мобильные телекоммуникации. – 2013. – №4-5. – С. 36-38
12. Кучерявый, Е.А. Интернет нановещей и наносети [текст] / Е.А. Кучерявый, С. Баласубраманиям // Электросвязь. – 2014. – №4. – С. 24-26.
13. 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.

14. Лахири, С. RFID. Руководство по внедрению [текст] / С. Лахири. – М.: Кудиц-Пресс, 2007. – 312 с
15. Майская, В. Беспроводные сенсорные сети, малые системы – большие баксы [текст] / В. Майская // Электроника: Наука, Технология, Бизнес. – 2005. – №10. – С. 18–22.
16. Рекомендация МСЭ-Т Y.3001. Будущие сети: целевые установки и цели проектирования, 2011 [электронный ресурс]. – 26 с.
17. Рогов, В.Г. Инфокоммуникации для «умного» города [текст] / В.Г. Рогов // Вестник связи. – 2013. – №8. – С. 39-41.
18. Рынок M2M-коммуникаций в России и мире: ноябрь 2013 года и прогноз развития [текст] // Мобильные телекоммуникации. – 2013. – №9. – С. 32-33.
19. Самсонов, М. Интернет вещей в умном городе [текст] / М. Самсонов, А. Гребешков, А. Росляков, С. Ваняшин // ИнформКурьер-Связь. – 2013. – №10. – С. 58-61.
20. 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.
21. Сергиевский, М. Беспроводные сенсорные сети [текст] / М. Сергиевский – М. Сергиевский // КомпьютерПресс. – 2007. – №8. – С. 4-10.
22. Черняк, Л. Интернет вещей: новые вызовы и новые технологии [текст] / Л. Черняк // Открытые системы. СУБД. – 2013. – №4. – С. 14-18
23. Черняк, Л. От первых радиометок до Интернета вещей [текст] / Л.Черняк // Открытые системы. СУБД. – 2005. – №07-08. – С. 92-94
24. Шарфельд, Т. Системы RFID низкой стоимости [текст] / Т. Шарфельд / Под ред. С. Корнеева. – М., 2006. – 197 с.
25. Шнепс-Шнеппе, М.А. Задачи производства изделий M2M: от простого к сложному [текст] / М.А. Шнепс-Шнеппе // Вестник связи. – 2013. – №9. – С. 11-16.
26. ETSI TS 102 690 «Machine-to-Machine communications (M2M); Functional architecture» [электронный ресурс], V1.1.1. – 2011
27. ISO/IEC 18092:2004. Information technology – Telecommunications and information exchange between systems –

Near Field Communication – Interface and Protocol (NFCIP-1) [электронный ресурс].
28. ITU-T Rec. Y.2060 (06/2012): Overview of the Internet of things [электронный ресурс].
29. RFID-метки [электронный ресурс]. – Режим доступа: http://rfid-m.ru, свободный. – Загл. с экрана
30. Wi-Fi Alliance [электронный ресурс]. – Режим доступа: http://www.wi-fi.org/, свободный. – Загл. с экрана.
31. P. Bowen et al., "Choosing the Right Platform for the Industrial IoT," 2017,
32. M. Kranz, Building the Internet of Things, 2017, Hoboken, New Jersey: JohnWiley & Sons, Inc.
33. M. Kranz, "Success with the Internet of Things Requires More Than Chasing
34. the Cool Factor," 2017, https://hbr.org/2017/08/success-with-the-internet-ofthings-requires-more-than-chasing-the-cool-factor.
35. H. Antunes, "The Future of IoT is Clearly in the Fog," 2017, http://www.maciejkranz.com/future-iot-clearly-fog/.
36. G. Corser et al., Internet of Things (IoT) Security Best Practices, 2017, https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf.
37. C. Tom, "Security and IoT in IEEE Standards," IEEE Standards University, 2016, 6, https://www.standardsuniversity.org/e-magazine/march-2016/security-andiot-in-ieee-standards/.
38. Standard for an Architectural Framework for the Internet of Things (IoT), 2016; http://grouper.ieee.org/groups/2413/Intro-to-IEEE-P2413.pdf.
39. J. Scholze, "Mining Industry Strategically Protects Assets with IoT," 2017, https://blogs.sap.com/2017/08/25/mining-industry-strategically-protects-assets-with-iot/.
40. M. C. O'Connor, "At Goldcorp's Éléonore Mine, the IoT Is Worth Gold," IOT Journal, 2015, http://www.iotjournal.com/articles/view?12790.
41. J. Perkins, "Internet of Things Improving Goldcorp Operations," Mining Innovation News, 2015, https://republicofmining.com/2015/03/13/internet-of-things-

improving-goldcorp-operations-by-james-perkins-mining-innovation-news-march-12-2015/.
42. Business Insider, “Retiring Cisco CEO Delivers Dire Prediction: 40% of Companies Will Be Dead in 10 Years,” June 8, 2015, http://www.businessinsider.com/chambers-40-of-companies-are-dying-2015-6.
43. E. Bertino and N. Islam, “Botnets and Internet of Things Security,” Computer, 50.2, 2017, pp. 76–79.
44. A. Velosa, W. R. Schulte, and B. J. Lheureux, Gartner Hype Cycle for IoT, 2017.
45. J. P. Albrecht, “How the GDPR Will Change the World,” Eur. Data Prot. L. Rev., 2, 2016, p. 287.
46. A. Nosko, E. Wood, and S. Molema, “All About Me: Disclosure in Online Social Networking Profiles: The Case of FACEBOOK,” Computers in Human Behavior, 26.3, 2010, pp. 406–18.
47. K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” IEEE Access, vol. 4, 2016, pp. 2292–303.
48. J. Ploennigs, A. Ba, and M. Barry, “Materializing the Promises of Cognitive IoT: How Cognitive Buildings are Shaping the Way,” IEEE Internet of Things J., 2017.
49. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660.
50. Li, S., Da Xu, L., & Zhao, S. (2015). The internet of things: a survey. Information Systems Frontiers, 17(2), 243-259.
51. Guo, B., Zhang, D., Wang, Z., Yu, Z., & Zhou, X. (2013). Opportunistic IoT: Exploring the harmonious interaction between human and the internet of things. Journal of Network and Computer Applications, 36(6), 1531-1539.
52. Banafa, A. (2014). IoT Standardization and Implementation Challenges. IEEE. org Newsletter.
53. Banafa, A. (2015). „What is next for IoT and IIoT”. Enterprise Mobility Summit. International Journal of Computer Science & Information Technology (IJCSIT) Vol 10, No 2, April 2018 24
54. Cai, H., Da Xu, L., Xu, B., Xie, C., Qin, S., & Jiang, L. (2014). IoT-based configurable information service platform for product

lifecycle management. IEEE Transactions on Industrial Informatics, 10(2), 1558-1567.
55. Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012, December). Future internet: the internet of things architecture, possible applications and key challenges. In Frontiers of Information Technology (FIT), 2012 10th International Conference on (pp. 257-260). IEEE.
56. Sadeghi, A. R., Wachsmann, C., & Waidner, M. (2015, June). Security and privacy challenges in industrial internet of things. In Proceedings of the 52nd annual design automation conference (p. 54). ACM.
57. Banafa, A. (2014). IoT and Blockchain Convergence: Benefits and Challenges. IEEE Internet of Things.
58. Marjani, M., Nasaruddin, F., Gani, A., Karim, A., Hashem, I. A. T., Siddiqa, A., & Yaqoob, I. (2017). Big IoT data analytics: Architecture, opportunities, and open research challenges. IEEE Access, 5, 5247-5261.
59. Desai, P., Sheth, A., & Anantharam, P. (2015, June). Semantic gateway as a service architecture for iot interoperability. In Mobile Services (MS), 2015 IEEE International Conference on(pp. 313-319). IEEE.
60. Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). Vision and challenges for realizing the Internet of Things. Cluster of European Research Projects on the Internet of Things, European Commision, 3(3), 34-36.
61. Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., ... & Doody, P. (2011). Internet of things strategic research roadmap. Internet of Things-Global Technological and Societal Trends, 1(2011), 9-52.
62. Sheng, Z., Yang, S., Yu, Y., Vasilakos, A., Mccann, J., & Leung, K. (2013). A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities. IEEE Wireless Communications, 20(6), 91-98.
63. Theoleyre, F., & Pang, A. C. (Eds.). (2013). Internet of Things and M2M Communications. River Publishers.
64. Coetzee, L., & Eksteen, J. (2011, May). The Internet of Things-promise for the future? An introduction. In IST-Africa Conference Proceedings, 2011 (pp. 1-9). IEEE. International Journal of

Computer Science & Information Technology (IJCSIT) Vol 10, No 2, April 2018 25
65. Ji, Z., & Anwen, Q. (2010, November). The application of internet of things (IOT) in emergency management system in China. In Technologies for Homeland Security (HST), 2010 IEEE International Conference on (pp. 139-142). IEEE.
66. James Kirkland , “Internet of Things: insights from Red Hat” , Website: https://developers.redhat.com/blog/2015/03/31/internet-of-things-insights-from-red-hat/ , Accesed : 2nd February 2018

СОДЕРЖАНИЕ