ОГЛАВЛЕНИЕ

Глава 1

ТЕХНОЛОГИИ, ВОЗМОЖНОСТИ И ПЕРСПЕКТИВЫ ИНТЕРНЕТА ВЕЩЕЙ

В этой главе мы поговорим об истории возникновения, особенностях облачной технологии, возможностях и перспективах интернета вещей, а также о проблемах или сбоях, связываемых именно с этой технологией взаимодействия современных электронных устройств и передачей данных на расстоянии.

1.1. Из истории интернета вещей

Так или иначе, полезные модели (изобретения) всегда с чего-то начинаются, кем-то, пусть даже в непривычных и неусовершенствованных формах, разрабатываются и запускаются в серийное производство. Мало кому верится сейчас, но концепция популярного сегодня интернета вещей предугадана в начале XX века Николой Теслой. Известный физик и, как бы сказали сегодня, талантливый электроник предполагал свойства проникающих радиоволн в роли нейронов «большого мозга», управляющего различными окружающими человека предметами. По замыслу Теслы, инструменты контроля должны умещаться буквально в кармане повседневной одежды. Великий и проницательный изобретатель не был фантастом, он понимал то, что его современники не могли и представить.

Концепция интернета вещей базируется на принципе межмашинного общения: без вмешательства человека электронные устройства «общаются» между собой. Интернет вещей – это автоматизация, но более высокого уровня. В отличие от «умных» домов, узлы системы используют TCP/IP-протоколы для обмена данными через каналы глобальной сети интернет. Рассматриваемый метод коммуникации дает преимущество – возможность объединять системы между собой, строить «сеть сетей», что позволяет изменить бизнес-модели отраслей и даже экономики целых стран.

Спустя 100 лет после Теслы термин интернет вещей ввел в широкий оборот сотрудник исследовательского агентства при Массачусетском технологическом институте Кевин Эштон, предложивший увеличить эффективность логистических процессов без вмешательства человека в производстве: с помощью электронных (радио)датчиков с автономным питанием собирать информацию о наличии товаров на складах и отслеживать их движение к торговым точкам. Каждая метка отправляла в сеть данные о своем местонахождении в каждый момент времени. Использование RFID-меток ускорило реакцию поставщиков и ритейлеров на изменение спроса и предложения: товары не лежали на складе, а отправлялись туда, где они действительно необходимы. Эффект от введения маркировки оценили, и вскоре все поставщики торговой сети производили товары только с радиометками. В наши дни «интернет вещей не только меняет существующие правила, но и формирует новые правила экономики совместного использования» (shared economy), исключая посредников из бизнес-модели.

Менее чем за 20 лет интернет вещей, или Internet of Things (IoT), стал трендом рынка информационных технологий. Аналитики прогнозируют колоссальное количество IoT-устройств через несколько лет – свыше 50 млрд. Развитие производства электронных компонентов позволяет «штамповать» миллионы дешевых чипов для всевозможных устройств. От радиочипов, нанесенных на складские коробки, IoT трансформировался в глобальную «интернетизацию» окружающих нас предметов и воспринимается людьми как глобальная «оцифровка» реальности.

Внимание, важно!

Уже сейчас, говоря об интернете, можно разделять его, разумеется условно, на интернет вещей и интернет людей, то есть получение, анализ информации с целью контроля процессов, передачи данных и управления исполнительными устройствами и всемирную паутину массовой коммуникации, которая подчас «высасывает» не только деньги, но и время. Некоторые пользователи проводят по нескольку часов в неделю в соцсетях, онлайн-играх или на сайтах, покупают в интернет-магазинах вещи, которые не нужны, просто потому, что это легко и доступно, буквально в два клика. В отличие от традиционного «человеческого» интернета, IoT применяется для рационального и практичного подхода. Его ключевая задача – автоматизация, оптимизация, сокращение материальных и временных затрат.

IoT стал всемирным трендом, и скоро возможность «интернетизации» станет обязательным требованием для продуктов и услуг широкого потребления. Новые устройства выходят с конвейера с уже встроенными интеллектуальными и коммуникационными возможностями. И вряд ли кто в точности мог бы предполагать такое прогрессивное развитие технологии еще 20–30 лет назад.

Применение IoT в промышленной индустрии и транспорте сокращает затраты за счет снижения аварийности, уменьшения потерь сырья и количества использованных ресурсов. В сфере энергетики – повышает эффективность выработки и распределения электроэнергии. Интернет вещей экономит не только деньги, но и время: машины заменили человека на рутинной работе и освободили от выполнения рискованных или стандартных задач. Интеллектуальные системы следят за промышленным конвейером, считают товар на складах и регулируют движение вместо человека – в любую погоду, круглосуточно и без выходных.

Кругом людей окружают разнообразные «подключенные» устройства: на улице работают системы безопасности и экомониторинга. Интернет вещей начинает использоваться в быту, в ЖКХ и индустриальной сфере, транспорте, сельском хозяйстве и медицине. Но мало кто вне цеха специалистов задумывается о том, что же на самом деле скрывается за этими двумя направлениями прогрессивного развития общества – интернетом вещей и интернетом людей. В нашей книге мы будем говорить об интернете вещей, поскольку всего знать невозможно и охватить всё также невозможно. Будем конкретны.

1.2. Технологии IoT

IoT (Industrial IoT, IIoT) объединяет концепцию межмашинного общения, использование BigData и проверенные технологии автоматизации производства. Ключевая идея IIoT – в превосходстве «умной» машины над человеком, в точном, постоянном и безошибочном сборе информации.

Технологии, которые присутствуют в IoT, можно рассматривать в нескольких значимых аспектах:

- RFID (радиочастотная идентификация), EPC (электронный код продукта);

- NFC («коммуникация ближнего поля»). Обеспечивает двусторонние взаимодействия между устройствами. Эта технология присутствует в смартфонах и служит для бесконтактных транзакций;
- Bluetooth. Широко применяется в ситуациях, когда достаточно связи ближнего радиуса действия. Чаще всего присутствует в носимых устройствах;
- Z-Wave. Низкочастотные RF-технологии. Чаще применяются для домашней автоматики, управления освещением и пр.;
- Wi-Fi. Самая популярная сеть для IoT (передача файлов, данных и сообщений).

Именно в этом ключе мы будем в дальнейшем излагать материал: прежде всего по теме книги, нас интересуют видеокамеры и аудиодиктофоны – эти инновационные модели, работающие в системе интернета вещей, следовательно, в книге мы будем опираться на все эти пять направлений, особенно на Wi-Fi, Z-Wave, Bluetooth.

Для читателя, не причисляющего себя к разработчикам радиоэлектронных устройств, интернет вещей понятен прежде всего на бытовом уровне – это холодильник, публикующий фото продуктов, к примеру, в Instagram, или стиральная машина, которая «постит» в Facebook: «у меня была сегодня чумовая стирка».

Примерно из 50 млрд ожидаемых подключений менее половины придется на пользовательские гаджеты, которые составляют «customer IoT»: смартфоны и планшеты, диктофоны и камеры, стационарные носимые и возимые датчики различного направления и контроля, в том числе для фитнеса и амбулаторной медицины. Более 15 млрд устройств будут работать в бизнесе и промышленности: разнообразные датчики для оборудования, терминалы для продаж, сенсоры на производственных агрегатах и общественном транспорте. Именно поэтому интернет вещей уже стал инструментом, с помощью которого можно дешево, быстро и масштабно решать конкретные задачи контроля, безопасности, бизнес-задачи в разных отраслях. Интернет вещей повысит уровень контроля качества продукции, выстроит процесс бережливого и экологичного производства, обеспечит надежные поставки сырья и оптимизирует работу заводского конвейера.

1.3. Примеры IoT

Знакомый всем пример – «Яндекс-навигатор». Водители нередко пользуются этим сервисом. Смартфоны и планшеты передают координаты, направление движения и скорость в службу Яндекс, а принятая от пользователей информация анализируется на сервере компании. Получив сведения о заторе, приложение автоматически предлагает водителю варианты объезда и отображает маршрут на экране телефона или планшета. Мобильные устройства, центры обработки данных и приложение Яндекс обмениваются данными без вмешательства человека, являя собой отличный пример интернета вещей. Как результат – водители тратят меньше времени в пробках, выбирая оптимальные маршруты объезда. Искусственный интеллект Яндекса уже пытается перераспределять нагрузку на дорогах мегаполисов. Учитывая накопленную статистику, он предлагает маршруты, которые оптимально загрузят магистрали и минимизируют пробки.

В спорте интернет вещей используют для накопления статистики и анализа данных. Применение IoT-решений разнообразно: от мобильных приложений для любителей утренних пробежек, следящих за расходом калорий, до производительных информационно-вычислительных систем в профессиональном спорте.

Командное IoT-решение отслеживает состояние отдельных спортсменов и всего коллектива. Причем браслеты и брелоки могут быть используемы не только спортсменами, но и для контроля лиц, отбывающих наказание в системе ФСИН, для военизированной охраны объектов – для контроля состояния часового и в других случаях с подобным спектром задач. Информация о перемещении, пульсе считывается датчиками, встроенными в одежду. Координаты и медицинская телеметрия отправляются на облачную платформу, снабжая оперативной информацией руководство и вспомогательные службы команды. Тренер строит тактику игры, не дожидаясь тайм-аута для оценки состояния коллектива, и переигрывает соперников за счет быстрого реагирования на окружающую обстановку. Ранее у тренерского состава и спортивных аналитиков не было иного выбора, кроме как просматривать после игры заметки и десятки часов видеозаписи для оценки поведения игрока на поле и его работоспособности. Теперь информация предоставляется онлайн, и голевой момент

матча всегда можно «вытащить» из хранилища и проанализировать. Интернет вещей обрел популярность не только среди тренеров, но и у медиков – бригады оказания первой помощи мгновенно реагируют на критические показания здоровья подопечных.

Дистанционное снятие показаний со счетчиков водо- и энергоресурсов в домах возможно благодаря IoT-решениям – беспроводной автоматизированной диспетчеризации. В жилищно-коммунальном хозяйстве IoT нашли применение в системах интеллектуальной диспетчеризации – «умных» приборов учета ресурсов. Подключенные к интернету счетчики передают показания в «облако», а диспетчер видит расход воды (электричества, газа) в отдельном доме, квартале или городе. Это дает возможность, не заглядывая в квартиры собственников, в режиме реального времени иметь информацию о потреблении ресурсов, удаленно управлять приборами учета, оперативно выставлять счета жильцам. Без обходчиков, без обработчиков и без временных потерь. За счет точного учета, оповещения о перерасходе ресурсов или авариях подключенные к интернету приборы учета ЖКХ сохраняют до 30% ресурсов в каждом многоквартирном доме. А помимо удобства, дополнительное преимущество для конечного потребителя – сэкономленные на содержании ненужной «прослойки» деньги. Организации, внедрившие IoT-решения для управления многоквартирными жилыми домами, получили эффективный инструмент контроля и учета ресурсов. Такая система автоматизирует трудоемкие операции по сбору и обработке показаний, которые ранее требовали участия половины штата сотрудников. Имея на руках прозрачные данные, управляющая компания выявляет потери и минимизирует расходы на общедомовые нужды (ОДН).

Аналогично – UBER, который за счет концепции IoT исключил таксомоторные компании из бизнес-модели частного извоза. Это дало возможность минимизировать посредников между клиентом и водителем.

Еще один пример. Наиболее продвинутые компании в России (по всему миру это давно вошло в обиход) используют систему для мониторинга влажности, температуры грунта и других характеристик почвы. Она работает как в частных, так и в государственных хозяйствах, где выращивают овощи и фрукты. Датчик, «закрепленный» за отдельным растением или участком с посевами, отправляет информацию на облачный сервер, отку-

да данные поступают оператору, выводя на экран контрольного дисплея состояние саженца (группы растений) и рекомендации по улучшению их плодоносных свойств. Этот комментарий иллюстрирует рис. 1.1.

Рис. 1.1. Датчик контроля роста томата передает данные беспроводным способом на пульт контроля

Как мы поговорили выше, интернет вещей (или IoT) – сеть соединяющая в себе множество объектов: транспортные средства, домашнюю автоматику, медоборудование, микрочипы и т. д. Все составные элементы накапливают и передают данные. Посредством такой технологии пользователь управляет устройствами удаленно.

Примеры IoT-устройств можно рассматривать в нескольких отдельных и связанных единой концепцией группах, таких как:

1) *носимые технологии*.

   К примеру, фитнес-браслеты Fitbit и умные часы Apple Watch легко синхронизируются с другими мобильными устройствами. IoT-часы и браслеты позволяют оперативно в режиме реального времени собирать сведения о здоровье: частота пульса, активность организма во время сна и др.;

2) *инфраструктура и разработка*.

   К примеру, приложение CitySense в онлайн-режиме анализирует данные об освещении и автоматически включает или выключает фонари. Существуют приложения, которые управляют светофорами или сообщают о доступности парковок;

3) *здоровье*.

   Некоторые системы, которые отслеживают состояние здоровья, используются в больницах. В основе их работы – ори-

ентировочные данные. Эти сервисы контролируют дозировку лекарств в различное время дня. К примеру, приложение UroSense отслеживает уровень жидкости в организме и, если нужно, повысит этот уровень. А врачи узнают сведения о пациентах по беспроводной связи. Рассмотрим пример: медицинская система, которая следит за состоянием здоровья, частотой сердцебиений, содержанием жидкости и отправляет отчеты медработникам. Данные отображаются в системе; доступны архивы. Проанализировав информацию, врачи решают, принимать ли пациенту медикаменты, удаленно.

Интересный симбиоз такой «пахучей» сферы агротехники, как удобрение полей и IoT. Фермер оснастил трактора-распрыскиватели, обслуживающие угодья в радиусе 1 км от станции, решением на базе беспроводных технологий. Водитель-оператор насосной установки удаленно отслеживает и распределяет подачу органических удобрений на поля, а владелец контролирует расход с экрана своего смартфона.

С помощью IoT-технологий операторы морских ветрогенераторов удаленно контролируют износ роторов и турбин, отслеживают их производительность. За счет своевременного обслуживания минимизируется риск остановки «ветряков» и отпадает необходимость в отправке бригад на удаленные морские платформы.

Оборудования на производственных площадках подключили к IoT-платформе, сигнализирующей о необходимости ТО для профилактики возможной поломки. «Проактивный» мониторинг сократил расходы за счет снижения издержек и ликвидации простоев. Традиционно ППР (планово-предупредительные ремонты) требовали остановки производственных линий и организовывались по графику, независимо от того, была в них необходимость или нет. Поэтому важно, чтобы внедрение IoT-технологии позволило проводить упреждающее техобслуживание тогда, когда оно действительно нужно, и ремонтировать оборудование до того, как оно сломается. Интернет вещей обеспечил не только непрерывность производства, но и сэкономил на планировании предупредительных работ (как правило, затраты на планирование составляют 30–40 % от объема ремонтного фонда предприятия).

Кроме того, новые технологии оптимизируют производственный процесс и уберут из него человеческий фактор, а вместе с ним и лишние риски.

Одно из решений в сегменте IoT отслеживает динамику болезни и выздоровления пациентов в режиме 24/7 посредством носимого на теле датчика. Мониторинг происходит в режиме реального времени, начиная от сбора показаний в стационаре и дома, завершая направлением данных лечащему врачу и в лаборатории для анализа и принятия решений. Есть проекты, развернутые в рамках лечебного учреждения и предупреждающие персонал об истощении запаса медикаментов или инструментов.

В обеспечении физической безопасности применение IoT-концепции скорее экзотично, чем привычно. В октябре 2016 года технологию интернета вещей начали использовать военные – для охраны Крымской военно-морской базы Министерство обороны закупило комплекс охраны «Часовой-1». Как уже было отмечено выше, комплекс, в состав которого входят вибробраслеты, гарантирует безопасность бойцов, охраняющих объекты и проверяющих автотранспорт на «блоках». Каждый браслет оснащен датчиком «неподвижности». Как только часовой прекращает движение более чем на 30 с, система посылает на его браслет вибросигнал. Если в течение 15 с после предупреждения боец не «оживет» – в караульном помещении объявляется тревога.

1.4. Перспективы для IoT

Перспективы для развития интернета вещей и новых, с расширенными возможностями протоколов IoT связывают с несколькими аспектами, в числе которых особенности проникающей способности сигнала XNB. Если удастся решить эту проблему в ближайшие годы (а над ее решением работают довольно эффективно), то фундаментом новых масштабных проектов в рассматриваемой теме станет энергоэффективная сеть, удовлетворяющая запросы промышленников, сельхозпроизводителей, государственные компании в масштабности и невысокой стоимости эксплуатации. Интернету вещей сегодня, как воздух, нужен стандарт связи с возможностью широкого территориального охвата, высокой энергоэффективностью, дешевой инфраструктурой и не требующей высоких эксплуатационных расходов. В этом, пожалуй, заинтересованы все стороны. Поэтому можно ответственно заявлять, что будущее IoT-концепции за LPWAN.

1.4.1. Особенности LPWAN

С учетом перечисленных требований и ограничений решением проблемы видится использование технологии на стыке высокой дальности и низкого энергопотребления. Она называется Low-Power Wide-Area Network (сокращенно – LPWAN), или энергоэффективная сеть дальнего радиуса действия. LPWAN разрабатывался специально для межмашинного общения и стал двигателем дальнобойного интернета вещей (далее – ИВ). Отсутствие относительно высоких требований к объему передаваемой информации позволило сконцентрироваться на важных параметрах технологии и обеспечить 50-километровую дистанцию взаимодействия между разнесенными устройствами, высокую энергоэффективность, проникающую способность и масштабируемость. Преимущества LPWAN вписываются в потребности масштабного внедрения IoT в промышленности, транспорте, сфере безопасности и других отраслях. Относительно большой радиус действия, высокая автономность конечных устройств, относительная простота развертывания LPWA-сети и низкая стоимость инфраструктуры дают импульс крупномасштабным проектам и развитию ИВ.

«Дальнобойная» и энергоэффективная LPWAN отлично подходит для IoT как в бытовом, так и в промышленном секторе, где имеется потребность в автономной передаче телеметрии на дальние расстояния, потому что LPWAN гораздо лучше соответствует запросам M2M-сетей, чем ее слабый аналог (в теме передачи данных) сотовая связь – тысячи квадратных километров будут покрыты лишь одной базовой станцией. Построение такой сети проще, а обслуживание – дешевле. Сей подход становится единственной альтернативой в случае, когда датчики разнесены по большой территории. К примеру, счетчики воды в пределах одного квартала или датчики влажности почвы, размещенные сразу на нескольких полях.

IoT проник в недоступные ранее сферы, улучшив качество жизни людей и увеличивая эффективность бизнеса, экономики. Технологии ИВ применяют там, где они выгодны бизнесу и удобны людям.

За счет увеличения масштаба производства и удешевления компонентной базы стоимость «умных» электронных устройств снизится еще более. IoT проник в автомобили, грунт, море и реки, в тело человека. Датчики стали миниатюрными, помещаются в бытовых предметах или продуктах питания. Соответственно, в

перспективе устройства еще уменьшатся в размерах, уменьшится и форм-фактор аккумуляторов, а затем они и вовсе исчезнут – «умные» датчики научатся получать энергию из окружающей среды: от вибрации, света или воздушных потоков, и станут полностью автономными. Если Господь благоволит, то и мы застанем то время, когда интернет вещей станет гетерогенной средой, существующей как живой организм.

Если оставить неблагодарные прогнозы о «количестве устройств интернета вещей к 2020 году», станет ясно, что IoT-индустрия растет. Порядок роста примерно понятен, как и цель – подключение «армии» устройств к интернету.

1.5. Перспективы разработки новых датчиков для IoT

В 2019 году разработчики ставят перед собой следующие перспективные задачи, чтобы обеспечить:

- небольшой объем данных: датчикам и сенсорам не нужно передавать мега- и гигабайты, как правило, это биты и байты;
- энергоэффективность: бóльшая часть датчиков автономна и должна работать годами без смены элемента питания или подпитываясь естественной энергией (солнце, ветер, иные виды альтернативной энергии);
- масштабируемость: в сети должны уживаться миллионы различных устройств, чтобы при необходимости оперативное добавление одного-двух миллионов не вызывало сложностей;
- глобальность: работа на перспективу широкого территориального охвата и, как следствие, передача информации на значительные расстояния;
- проникающая способность: электронные устройства под землей и водой должны передавать сигнал наружу;
- конкурентная стоимость устройств: устройства должны быть относительно дешевы и доступны для пользователя, а готовые решения рентабельны для бизнеса;
- относительная простота: принцип «поставил и забыл»: пользователь выберет понятные и дружелюбные устройства.

Не так давно люди убедили себя, будто бы сети сотовой связи – наиболее перспективные кандидаты на построение развернутой на сотни километров беспроводной IoT-среды. Однако ни стандарт GSM, ни инфраструктура мобильных операторов изначально не создавались для M2M-диалога. Протоколы сотовой связи предназначены для общения людей: этому способствуют большой объем трафика и высокая скорость обмена данными в густонаселенных районах, и это же является проблемой для безупречной качественной связи. Те ошибки или «сбои» аналоговой (речевой) или цифровой связи, которые пусть и скрепя сердце допустимы в общении между частными корреспондентами (в быту), не могут быть признаны приемлемыми в радиоэлектронных устройствах в промышленном производстве с высокими требованиями к техногенной безопасности и (или) передаче данных. К сожалению, в этом вопросе еще не все так гладко, как хотелось бы, ибо ограничить сигнал Wi-Fi с частотой 2,4 ГГц, забить его помехой можно даже на бытовом уровне – такие устройства существуют, – чем привести в полную негодность всю IoT-сеть. Однако и над этой проблемой профессионалы работают, что дает надежду либо на трансформацию протоколов в будущем, либо на обеспечение их безопасности от несанкционированного внешнего воздействия. Подробнее о методах защиты и возможных методах воздействия на сигналы в системе интернета вещей мы поговорим во второй главе книги.

1.6. Сравнение беспроводных технологий в интернете вещей

Разработчики изначально не предполагали возможности обмена небольшими объемами данных между разнесенными «умными» сенсорами. Датчику с Wi-Fi необходимо постоянное питание, а элемент умного GSM-устройства продержится 2–3 недели. Не многие пока готовы ежемесячно менять элементы питания в десятках устройств или монтировать к ним проводную систему питания. Подключение всевозможных устройств к мобильным сетям еще можно представить в населенных пунктах, но за пределами оживленных трасс и урбанизированных территорий протоколы GSM, 3G, LTE не позволяют создавать масштабные IoT-проекты – слишком дорого разворачивать и обслуживать инфраструктуру сотовой сети.

Внимание, важно!

В населенных пунктах с большой плотностью населения (городах, мегаполисах) сотовая связь ограничена низкой проникающей способностью сигнала. А «умные» датчики или счетчики находятся за несколькими стенами, в технических колодцах или на цокольных этажах, где связь GSM может быть неустойчива по определению распространения радиоволн на соответствующих частотах.

В наши дни сложности с компонентной базой ушли в прошлое, появился новый вызов: необходимо объединить миллиарды «умных» приборов в единую сеть. Интеллектуальный станок, датчик температуры масла на промышленном агрегате, смарт-холодильник – всем этим устройствам необходима среда для общения. В противном случае они так и останутся «немыми»: обычным счетчиком или датчиком, отличающимся от своих собратьев только «космическим» дизайном.

К примеру, «Яндекс-навигатор» может работать через GPRS/3G/4G, и пока другая связь для сего приложения не подходит. Можно подключить смартфон к Wi-Fi и запустить «Навигатор», но как только автомобиль отъедет на 150 м от точки доступа – приложение «закончится». А в «умном» доме не «приживутся» автономные GPRS-датчики – через несколько дней активного использования датчиков в них «сядут» батарейки. Поэтому в интеллектуальном жилище лучше всего подойдет энергоэффективный ZigBee.

Действительно, для передачи данных разрабатывалось множество протоколов, но каждый из них был «заточен» под определенную задачу: GSM для голосового общения, GPRS для обмена данными с мобильных телефонов, ZigBee для создания локальной сети и управления «умными» домами, а Wi-Fi для беспроводных локальных сетей с высокой скоростью передачи данных. Все эти технологии интернета вещей могут быть применены для решения нецелевых задач и по-разному с ними справляться. Сейчас разработчики работают над тем, как это все конфигурировать и объединять для взаимодействия именно с высокой степенью надежности.

И наконец, открытый пока вопрос возможности глушения «полезных» сигналов как Wi-Fi, так и GSM, а также спутниковой связи на бытовом уровне. Это действительно проблема, подробно она хорошо описана в современной литературе.

1.7. IoT-архитектура

Существует несколько подходов для тестирования архитектуры IoT.

Необходимо достаточно продуманное оборудование, которое бы отправляло не только уведомления, но и сообщения об ошибках, предупреждения и др. В системе должна присутствовать опция, которая фиксирует события, чтобы конечному пользователю было понятнее. Если такая возможность не предусмотрена, сведения о событиях сохраняются в базе данных. Тщательно проверяется и возможность обработки данных и обмена задачами между устройствами. Необходимо обеспечить юзабилити тестирование каждого из устройств, и желательно при тестах, чтобы тестируемые устройства были портативными.

Безопасность IoT

Данные лежат в основе работы всех подключенных устройств. Потому не исключен несанкционированный доступ во время передачи данных. С точки зрения тестирования ПО необходимо проверять, насколько защищены/зашифрованы данные. Если есть UI, нужно проверить, защищен ли он паролем.

Эффективность и сетевые возможности

Крайне важны возможность подключения к сети и функциональность IoT. Ведь речь идет о системе, которая используется в целях здравоохранения.

Проверяются два главных аспекта:

- наличие сети, возможности передачи данных (передаются ли задания с одного устройства на другое без каких-либо заминок);
- сценарий, когда подключение отсутствует.

Независимо от уровня надежности системы существует вероятность, что статус системы будет офлайн. Если сеть недоступна, сотрудникам больницы или другой организации необходимо об этом знать (уведомления). Таким образом, они смогут следить за состоянием пациента сами, а не ждать, когда система заработает. С другой стороны, в подобных системах обычно присутствует механизм, который сохраняет данные, если это офлайн-система. То есть потеря данных исключается.

Возьмем здесь за пример медицинскую сферу. Необходимо учитывать, насколько решение для сферы здравоохранения применимо в конкретных условиях. В тестировании участвуют от 2 до 10 пациентов, данные передаются на 10–20 устройств. Если вся больница подключается к сети, это уже 180–200 пациентов. То есть фактических данных будет больше, чем тестовых. Также необходимо протестовать утилиту для мониторинга системы: текущая нагрузка, потребление электроэнергии, температура и пр.

Тестирование совместимости

Этот пункт всегда присутствует в плане по тестированию IoT-системы. Совместимость разных версий операционных систем, типов браузеров и их соответствующих версий, устройств разного поколения, режимов связи, к примеру Bluetooth 3.0, крайне важна для IoT.

Пилотное тестирование

Пилотное тестирование – обязательный пункт тест-плана. Только тесты в лаборатории позволят сделать вывод о том, что система функциональна. При пилотном тестировании число пользователей ограничено. Они совершают манипуляции с приложением и высказывают свое мнение. Эти комментарии оказываются весьма кстати, позволяют сделать надежное приложение.

Проверка на соответствие

Система, которая отслеживает состояние здоровья, проходит множество проверок на соответствие. Бывает и так, что программный продукт проходит все этапы тестирования, но проваливает финальный тест на соответствие (тестирование проводит регулирующий орган). Поэтому, целесообразнее проверить на предмет соответствия нормам и стандартам перед стартом цикла разработки.

Тестирование обновлений

IoT – это комбинация множества протоколов, устройств, операционных систем, встроенного ПО, аппаратного обеспечения, сетевых уровней и т. д. Когда происходит обновление – будь то система или что-то еще из перечисленного выше, – требуется

тщательное регрессионное тестирование. В общую стратегию вносятся поправки, чтобы избежать сложностей, связанных с обновлением.

1.8. Особенности тестирования IoT

IoT – это архитектура, в которой тесно переплетаются компоненты ПО и аппаратной части. Важно не только программное обеспечение, но и качество устройств и взаимодействие: датчики, сенсоры, шлюзы, проводка питания и др. Одного лишь функционального тестирования будет недостаточно, чтобы сертифицировать систему. Все составные компоненты взаимозависимы. IoT сложнее, чем отдельно ПО или только аппаратная часть.

Модель взаимодействия устройств

Составные части сети должны взаимодействовать в режиме реального времени или близкого к реальному. Все это становится единым целым – отсюда дополнительные сложности, связанные с IoT (безопасность, обратная совместимость и обновления).

Тестирование данных, поступающих в реальном времени

Получить такие данные непросто. Дело усложняется тем, что система, как в описанном случае, может относиться к сфере здравоохранения.

Сеть IoT обычно состоит из разных устройств, которые управляются разными платформами iOS, Android, Windows, Linux. Тестирование возможно только на некоторых устройствах, поскольку тестировать на всех возможных устройствах практически невозможно.

Доступность сети

Сетевое соединение играет важную роль в IoT. Скорость передачи данных постоянно увеличивается. IoT-архитектура должна тестироваться в различных условиях соединения на разной скорости. Эмуляторы виртуальных сетей в большинстве случаев используются, чтобы разнообразить сетевую нагрузку, возможности соединения, стабильность и прочие элементы нагрузочного тестирования. Но фактические данные – это всегда новые сценарии, и тестировщик не знает, где в будущем возникнут сложности.

1.8.1. Инструменты тестирования IoT

Существует множество инструментов, которые применяются в тестировании IoT-систем. Их классифицируют в зависимости от предназначения.

Особенности программного обеспечения

Wireshark: инструмент с открытым исходным кодом. Используется для мониторинга трафика в интерфейсе, адреса источника/заданного хоста и др.

Tcpdump: этот инструмент выполняет похожую работу. У утилиты нет GUI, ее интерфейс – командная строка. Она дает возможность пользователю высвечивать TCP/IP и другие пакеты, которые передаются по сети.

Особенности аппаратного обеспечения

JTAG Dongle: инструмент, аналогичный отладчикам в приложениях для ПК. Позволяет найти дефекты в коде целевой платформы и показывает изменения шаг за шагом.

Digital Storage Oscilloscope: проверяет различные события с помощью временных отметок, перебои с электропитанием, целостность сигнала.

Software Defined Radio: эмулирует приемник и передатчик для различных беспроводных шлюзов.

Подход к тестированию IoT может отличаться в зависимости от конкретной системы/архитектуры. Тестировать IoT для неподготовленного пользователя непросто, но вместе с тем это интересная работа, благо есть где «размахнуться»: устройств, протоколов и операционных систем множество. Особо интересен тестовый формат TAAS («тесты с точки зрения пользователя»), он позволяет творчески подходить к делу, основываясь на вариативном и опциональном выборе функций, а не просто выполнять формальные требования.

1.9. Облачные технологии беспроводной передачи данных

Доступ через интернет к видеонаблюдению UControl по облачной технологии P2P для пользователя осуществляется бесплатно. Облачная технология P2P (англ. peer-to-peer) создана для удобства