ЦИФРОВАЯ КУЛЬТУРА
УНИВЕРСИТЕТ ИТМО

Основы интернета вещей

Высшая школа цифровой культуры
Университет ИТМО
dc@itmo.ru

Содержание

1 Введение **2**

2 Понятие «умной вещи» **3**

3 Примеры IoT решений **5**

4 Умный дом **8**

5 Безопасность и IoT **13**

6 Безопасность умных систем на базе IoT **16**

7 Безопасность самих систем IoT **19**

1 Введение

В этой лекции мы рассмотрим понятие умные вещей, их определение как системы **IoT (Internet of Things)** с переходом в концепцию **IoE (Internet of Everything)**, важность рассмотрения аспекта безопасности как при использовании, так и при проектировании «умных» систем.

Сегодня мы с вами порассуждаем в каком мире мы живем, куда мы движемся и о чем нам стоит думать в нашем техногенном движении. А именно, как соотносятся между собой так привлекающие нас понятия умных вещей, домов, производств, городов и даже стран и такое естественное желание жить безопасно, надежно, приватно, осознанно.

Умные вещи окружают современного человека повсеместно. Например, очень удобно использовать SmartWatch (умные часы) для организации эффективного планирования дня, постоянного доступа к информации (звонки, сообщения, почта), непрерывных коммуникаций – это все исходное предназначение Умных вещей – упростить нам жизнь, сделать ее более удобной, дать больше возможностей и информации о нашем окружении.

Далее, для еще большего удобства нашей жизни умные устройства научились собирать информацию о нас самих. Например, как часто и насколько интенсивно мы ходим, какой у нас пульс, температура, занимаемся ли мы спортом. Обрабатывая эту информацию умные устройства могут давать нам подсказки и советы – «Мой друг, тебе пора прогуляться», или «Вы недостаточно интенсивно бегаете», «SOS! Температура тела 37 Co» и много другое. Устройства из простых «Напоминалок» превращаются в «Умных помощников»!

Чем больше информации знает о Вас и вашей жизни Умное устройство – Кто Вы, Где Вы, Чем занимаетесь, Что любите, С кем общаетесь, Чем интересуетесь, Какой режим дня и т.д. – тем более индивидуальные, подстроенные именно для ваших потребностей сервисы может дать умное устройство. То же рассуждение можно применить и при рассмотрении работы предприятия, жизни города и даже целой страны. Чем больше информации у умной системы, тем более специфическую поддержку она может оказать своему «Хозяину».

Возможность возникновения таких Умных решений появилась с возникновением и развитием целого ряда информационных технологий (Big Data, Artificial intelligence, Neural Networks, Web, Mobile OS, Internet of Things etc.). Мобильные, распределенные и интеллектуальные системы позволяют достигать невероятных результатов в различных областях жизни и деятельности человека.

Однако, современному человеку стоит задуматься, а так ли уж безопасна предлагаемая нам умная система? Можем ли мы полагаться на все 100% на

ее «Советы»? Может ли ошибаться сама система и не приведёт ли слепое доверие к катастрофическим ситуациям в будущем?

Не предоставляет ли она такие же, а то и большие, возможности и информацию не нам в «Плохому парню», который захочет воспользоваться умной системой отнюдь не в нашу пользу? Не окажется ли столь привлекательная умная вещь весьма удобным инструментом в чужих рука?!

О всех этих вопросах стоит задумываться в первую очередь разработчикам Умных решений, но и, конечно, пользователям. Решением поставленных вопросом во многом занимается направление информационной безопасности в рамках решения задач обеспечение конфиденциальности, доступности и целостности.

Именно этих вопросов в контексте разработки и использования умных решений мы с Вами коснемся в данной лекции.

2 Понятие «умной вещи»

Прежде всего давайте подумаем, что же такое «Умные вещи»?

Первая особенность заключается в том, что речь действительно идет о вещах. Важно, что в общем случае ни количество вещей, ни их размер, ни область назначения или иные свойства не ограничены. В идеале умной может стать любая вещь.

Вторая особенность заключается в том, что умная вещь должна иметь возможность работать с информацией. В общем виде это означает, что умная вещь должна уметь:

1. Собирать информацию;
2. Хранить информацию;
3. Обрабатывать информацию;
4. Передавать информацию;
5. Или даже принимать решение на основе информации.

Конечно не каждая вещь может реализовывать весь перечисленный выше функционал. Существуют ограничения по вычислительным возможностям, габаритам и энергоресурсам, но если вещь умеет хотя бы что-то из вышеперечисленного, то существует возможность сделать ее *умной*.

Третья особенность – это то, что работа вещи с информацией не есть самоцель. Информация нужна для принятия глобального решения по управлению процессами реального мира. То есть, умные вещи используются человеком или компьютерными системами для улучшения процессов принятия

решений. Если вещь не может быть полезной для такой задачи, то в ракурсе решаемой задачи она теряет весь свой ум.

Четвертая особенность умных вещей заключается в том, что умные вещи общаются между собой. Результат такого общения передается в центр управления для оптимизации принятия решений. При этом центр принятия решений может быть единым, например, центральный сервер, или распределённым, состоящим из нескольких узлов обработки данных и принятия решений, например, самоорганизующаяся сеть.

Итак, если мы говорим об умных вещах, мы должны понимать, что такие вещи:

1. Собирают информацию, т.е. имеют сенсоры (датчики параметров окружающей среды, камеры, микрофоны и т.д.);

2. Хранят информацию, т.е. имеют встроенную память (такая память может быть постоянной, например, у RFID метки, или перезаписываемой, например, карта памяти видеокамеры);

3. Некоторые обрабатывают информацию (например, для сжатия, шифрования или вычисления некоторых параметров);

4. Передают информацию, т.е. используют сети передачи данных (это могут быть сети общего назначения, такие как WI-FI, или специализированные, такие как ZigBee);

5. Некоторые могут принимать решения и передавать управляющие сигналы (например, Умная розетка может включать или выключать приборы в доме).

Проанализировав свойства умных вещей, мы понимаем, что сами по себе они могут быть как весьма скромного ума, так и весьма сообразительными и самостоятельными.

Однако, при получении возможности общаться для обмена информацией, при получении дополнительных вычислительных возможностей от Центров обработки данных, при получении возможности удаленного управления, даже весьма скромные умные вещи могут быть объединены для получения мощных Умных управляющих систем различного назначения.

В настоящий момент известно множество примеров подобного объединения, например, умные дома, умные производства, умные склады. Такие решения, в свою очередь, могут быть так же объединены. Например, умный дом может общаться с Умным магазином что бы каждое утро у нас на завтрак был свежий бутерброд, доставленный нам умной машиной.

Таким образом, за счет постепенного объединения умных решений мы постепенно переходим от понятия Интернета вещей (IoT- Internet of Things) к понятию Интернета всего (IoE- Internet of Everything).

Возможности, предоставляемые результирующими решениями интернета всего практически безграничны, а существующие решения определяются лишь текущим спросом и фантазией разработчиков.

Но как безграничные возможности Умных решений, настоль же сложны и задачи обеспечения безопасности при их использовании в нашей повседневной жизни.

3 Примеры IoT решений

Рассмотрим примеры различных вариантов умных систем, которые могут нас окружать.

Для начала давайте посмотрим на умные персональные вещи – т.е. те, которыми мы привыкли пользоваться как исключительно собственными.

Начнем рассмотрение носимых устройств (конечно, только части из огромного количества возможных вариантов).

Умный головной убор (умная шляпа, умная кепка, умная шапка и т.д.) - Существует несколько вариантов:

- умная шляпа – шляпа со встроенной камерой для сэлфи. Фотографии сохраняются на карте памяти, встроенной в шляпу или отправляются на смартфон;

- умная кепка – кепка со встроенной камерой для видеотрансляций (также содержит карту памяти для записи результатов и модуль для онлайн трансляции);

- кепка со встроенными датчиками, которая не дает водителю заснуть (имеет несколько встроенных датчиков, например, акселерометров для контроля положения головы водителя, и модуль взаимодействия с внешними устройствами-телефоном или автомобилем. Особенностью является автоматическое включение средств воздействия на водителя-включение света, вибрации и проч.);

- кепка со встроенной музыкальной системой (содержит встроенную музыкальную гарнитуру и модуль коммуникации со смартфоном, а также встроенную панель управления);

- умная шапка – представляет собой шапку со встроенной гарнитурой, которая связывается со смартфоном по Bluetooth.

Умные очки разрабатываются для нескольких направлений.

Повседневная жизнь – очки, которые в удобной форме визуализируют необходимую информацию, например, результаты поисковых запросов, входящие звонки и сообщения, а та же позволяют делать видео и фотосъемку и сохранять результаты на карту памяти либо сразу выкладывать в сеть.

Спортивный аксессуар. Имеет похожее назначение, но со спортивным уклоном. Посредством приложения, установленного на смартфон имеет возможность визуализировать текущие параметры тренировки.

Очки дополненной/виртуальной реальности – предназначены для вывода в поле зрения человека виртуальных объектов.

Умная одежда. В настоящее время многие фирмы думают над производством умной одежды. Для одежды существует также два основных направления.

Для простой жизни – например:

- умные носки с RFID меткой, позволяющей их найти, конечно при помощи специального приложения на смартфоне;
- умные куртки с управляемым подогревом, имеющие встроенные датчики температуры и модуль связи со смартфоном;
- умное белье со встроенным датчиком пульса.

Так же существует и умная одежда для занятий спортом. Она создается из специальных материалов, содержит расширенное число датчиков, таких, как датчик пульса, температуры, акселерометр, GPS и проч., которые передают данные на смартфон, который в свою очередь их анализирует и визуализирует.

Еще одним направление носимых устройств является *умная обувь.* Например:

- кроссовки для спорта, собирающие информацию о динамике тренировки, количестве шагов и потраченных калориях;
- стельки для контроля правильности движений;
- умные стельки с подогревом – температурой которых можно управлять с помощью приложения на смартфоне.

Умные часы. Очень популярным гаджетом среди носимых устройств являются умные часы и браслеты. Их линейка меняется от простых устройств, выводящих информацию о звонках и сообщениях, до весьма сложных устройств, синхронизированных со смартфоном и другими умными системами, например, умной одеждой.

Прочие вещи:

- умные брелоки для ключей и прочих вещей. Такие брелоки содержат встроенный GPS модуль и могут сообщать при помощи приложения о своем местонахождении;

- умная скакалка. Скакалка может быть настолько умна, что способна, синхронизируясь со смартфоном, вести настоящий дневник тренировок, считать потраченные калории и количество прыжков. Кроме того, она позволяет устраивать онлайн-соревнования с друзьями в режиме реального времени;

- умный зонт. Зонт сообщает хозяину о предстоящем дожде, отправляя сообщения на смартфон, о своем местоположении, а также может позвонить, если его забыли.

- Умный кошелек, со следующими функциями:

  – Аккумулятор – в кошелёк встроена батарея на 2600 мАч. С помощью встроенного аккумулятора можно заряжать мобильные устройства как по кабелю, так и с помощью беспроводной технологии;

  – Сигнализация – если вы упустите бумажник из виду, он будет посылать сигналы на ваш смартфон. Если вы потеряете свой смартфон, то он будет посылать сигналы на ваш кошелёк;

  – GPS-локатор. Если Вы потеряете аксессуар, то сможете отследить его положение из любой точки земного шара.

  – Точка доступа. Кошелёк может стать подобием компактного модема.

  – Фотокамера. Если бумажник будет далеко от вашего смартфона в так называемом «lost mode», он сфотографирует каждого, кто его откроет, и вышлет вам фотографии на e-mail. Так вы сможете найти вора или человека, который нашел ваш бумажник.

  – Датчики наличия карт и купюр

Конечно, мы рассмотрели лишь некоторые из возможных вариантов Умных персональных (носимых) вещей и каждый день могут появляться все новые их варианты. Мы видим, насколько удобными они являются и насколько могут упрощать нам жизнь.

Выделим основные общие моменты их работы:

- Умное устройство взаимодействует со смартфоном. Чаще всего такое взаимодействие происходит по протоколу беспроводных коммуникаций Bluetooth или Wi-Fi.

- Умное устройство получает от смартфона управляющие команды. Для управления на смартфон должно быть установлено специализированное приложение, а, так же, должно быть включено беспроводное соединение.

- Умное устройство отдает смартфону информацию о текущем состоянии контролируемых параметров, начиная от уровня заряда батарейки и заканчивая информацией с сенсоров (например, акселерометра, датчика GPS и др.) и устройств (например, микрофонов и камер).

- Умное устройство отдает смартфону информацию о командах пользователя, например, через встроенные панели управления или через микрофон.

- Взаимодействие со смартфоном происходит по беспроводным каналам связи, в настоящий момент чаще всего посредством стандартных протоколов Bluetooth или Wi-Fi.

- Обработка информации происходит на внешнем устройстве – смартфоне или же в облаке.

- Умное устройство имеет автономное питание, т.е. должно периодически заряжаться (в настоящий момент практически каждый день).

- Часть Умных устройств содержит встроенную память, имеет возможность сохранять информацию на установленных картах памяти или же отправлять ее на хранения на внешние устройства: смартфон или облако.

4 Умный дом

Давайте перейдем от рассмотрения нательных носимых устройств к системам интеллектуального управления нашим жилищем, которые носят общее название Умный дом.

Основное отличие заключается в том, что целью создания подобных систем является поддержка качества протекания процессов управления уже не только связанных с жизнью одного человека, как, например, в случае умных часов, но некоего жилого помещения – дома.

В общем случае домом может пользоваться не один человек и даже если в какой-то момент им пользуется один хозяин, то со временем ситуация может измениться – дома живут дольше людей. Кроме того, в доме живут не только люди, а и любимые (наши питомцы) и не очень (непрошенные гости, например, мышки) животные.

Процессы же, протекающие в Доме, эффективное управление которыми необходимо обеспечить для комфортного жилья, в значительной степени отличаются от тех, которые характерны для Человека, т.е. те, примеры которых мы рассматривали при анализе Умных вещей.

Кроме того, дома еще отличаются от Человека по следующим пунктам:

- по размерам (затруднительно будет найти дом размером с его жильца. Даже у космонавтов их космический дом не так уж мал);
- по материалам (мы замечает, что, например, некоторые Дома никак не хотят пускать к себе сигналы мобильной связи, а большинство из них не пускают сигналы GPS);
- по мобильности (большинство домов стационарны, т.е. не очень любят перемещаться. Дом космонавтов, безусловно, является исключением);
- по питанию. (для обеспечения работы систем жизнеобеспечения Дома необходимо электричество, т.е. в доме, почти всегда есть стационарный источник питания. Это важно, поскольку умные системы тоже питаются электричеством, а не морковкой);
- по принципу построения систем. (системы дома не являются биологическими, а значит мы можем или управлять при помощи электрических или механических воздействий. Т.е. можем не только контролировать состояние и сообщать о нем, но и реально управлять подсистемами и отдельными элементами)

Существует еще и ряд других отличий. В любом случае, все эти отличия делают как процесс создания системы умного дома, так и саму систему достаточно сложными.

Рассмотрим пример. В качестве примера рассмотрим обычную городскую квартиру:

Все начинается с двери. Дверь – это вход в наш дом. Дверь нужна, чтобы контролировать доступ в квартиру, т.е. те, кому хозяин (или хозяева) разрешает войти – должный иметь возможность беспрепятственно попасть в помещение. Ну а те, кому это не разрешено (все остальные) – нет.

Проблема заключается в том, что со временем список тех, кого мы хотим пустить в свой дом меняется. Например, к нам приехал друг, или необходимо пустить коммунальные службы, а мы в отпуске, или надо впустить врача, а человек не может дойти до двери, чтобы ее открыть. Кроме того есть и менее экстренные ситуации – в семье стало больше людей.

Мы знаем, что обычная дверь с обычным замком имеет самые обычные ключи. А ведь Эти ключи все одинаковые, и чтобы создать новый ключ или

же забрать ранее выданный, нужно совершить целый ряд действий, растянутых во времени (особенно не приятный момент, если речь идет о корой помощи). Кроме того, нет никакой возможности узнать кто и когда воспользовался ключом и вошел к нам в дом.

Для решения этих проблем можно установить умный замок. Замки бывают различных конструкций: как надстройка над обычным механическим замком и как самостоятельное устройство.

Такой замок устанавливается вместо сердцевины старого замка, механизм может оставаться прежним, либо можно поставить новую систему замка. Управление такими замками может осуществляться:

- со встроенной панели;
- при помощи смартфона с помощью NFC или при помощи специального приложения, установленного на смартфон или компьютер;
- при помощи биометрических датчиков;
- классическим способом при помощи обычного ключа;
- чаще всего в умных замках производители реализуют комбинированный подход.

Часто такой замок имеет подключение к контроллеру или хабу умного дома, через который осуществляется связь с комплексной системой управления.

Удобной функцией является наружная камера, информация с которой отправляется владельцу, что бы он знал, кто хочет зайти в гости. А так же подсистема генерации и распределения ключей, которая осуществляется в специальном приложении. При этом ключи можно выдавать удаленно, на заданное время и контролировать, каким ключом открывается дверь.

Важно отметить, что в качестве двери можно использовать и окна. Так что хорошо бы, что бы контроль доступа в квартиру осуществлялся совместно дверью и окнами. Для этого иногда достаточно подключить в систему умного дома умные датчики открывания, которые по беспроводному каналу сообщат о факте открывания окон.

Поскольку доступ может осуществляться и через окна, то недостаточно просто сообщить о факте открытия, хорошо бы еще знать кто открыл окно - т.е. получить фото гостя.

Для этого в систему умного дома добавляют умные камеры. Наличие таких камер позволяет контролировать не только факт открывания/закрывания, но и следить за тем, что происходит в помещении – это очень удобно.

Итак, у нашего умного дома уже есть умная дверь, окно и камеры. Для эффективной работы они должны работать совместно, а, следовательно, в

системе умного дома появляется новое устройство – хаб. Это устройство собирает и информацию от различных Умных устройств в доме и взаимодействует в внешней средой обработки данных и принятия решений –Облачным сервисом, содержащим интеллектуальную систему, и смартфоном, осуществляющим коммуникации с владельцем/владельцами Умного дома.

Теперь, когда у нас появилась инфраструктура взаимодействия мы можем добавлять в нее и другие умные устройства. Приведем лишь некоторые примеры.

Войдем в прихожую. Здесь нас встретит умное освещение, которое или просто включает свет, или делает это индивидуально, узнав своего гостя. Умный свет может сопровождать нас при перемещении по квартире, учитывая время года и время суток тем самым создавая комфорт и экономя электроэнергию. Подсистема умного света может иметь голосовое управления – это иногда очень удобно.

Так же в прихожей нас может встретить умный пол. Если холодно или влажно, пол включит подогрев. Такой пол может иметь встроенное расписание включения/выключения или же дистанционное управление со смартфона или компьютера.

Умный свет может нас сопровождать и в ванной комнате. Где нас встречает уже Умная система контроля воды: например, регулировки температуры воды (умный термостат), учета количества воды и контроля протечек. Эта подсистема также может управляться удаленно и предоставлять сведения на смартфон. Не говоря уже про умную ванну, которая будет наполнена водой комфортной, именно, для вас температуры и именно тогда, когда это нужно именно Вам.

В уборной же на может встретить умный унитаз. Некоторые из них настолько умны, что сообщат вам не только Ваш вес и температуру, но и проведет экспресс анализ (конечно того, что будет у него в наличии).

Перейдем в комнату. Здесь Вас может встретить умная музыкальная система. Например, сейчас популярными становятся умные колонки с голосовым управлением. Такая система может быть очень точно настроена на индивидуальные вкусы и определять меломана либо биометрически (по лицу или голосу, отпечатку пальца, полученному от умного замка), либо по какому-то персональному носимому устройству (смартфону, RFID брелоку). Музыка, при желании, может сопровождать вас по всему дому!

В комнате можно применить и другие умные вещи – например, умные розетки с дистанционным управлением, умные системы поддержания микроклимата, с контролем состояния температуры и влажности воздуха, освещенности, пыле- и газо-загрязненности. Любители цветов могут даже использовать умные цветочные горшки с дистанционным контролем состояния почвы и воздуха и системой полива.

Отдельно можно упомянуть умный телевизор. Функционал умных телевизоров очень отличается. Многие из них могут быть интегрированы в систему умного дома, например, для вывода информации от умного замка.

Кухня – это царство умных вещей. Умный чайник, кофеварка, тостер, плита и холодильник. Все это сейчас уже не новость. Пожалуй, наиболее многофункциональным можно считать *умный холодильник.*

Например, он имеет возможности:

- Удаленной настройки и контроля параметров температуры в различных его частях;
- Контроля продуктов, а именно, их наличия и срока годности (для этого в холодильник встроены камеры и датчики);
- Подключения к сети Интернет. Для заказа продуктов в Интернет магазинах (холодильник может сам их заказывать, если продукты закончились или их срок годности заканчивается), поиска рецептов (в том числе с учетом имеющихся продуктов);
- Обладает Большой панелью управления на дверце для настройки режимов, отображения информации о продуктах, поиска и просмотра рецептов, просмотра кино и телевизора, а так же, электронной почты и аккаунтов в соцсетях. По сути – это полноценный компьютер, встроенный в холодильник;
- Голосовое общение и управления. Можно поболтать со своим любимым Холодильником.

Все эти умные вещи можно объединить между собой и позволить им общаться. Для организации такого общения используют технологии Интернета вещей и искусственного интеллекта.

Тогда умная кофеварка может узнать от умной кровати, что вы уже почти проснулись, и пора готовить утренний кофе. А выбирая рецепт кофеварка может спросить у умного холодильника, есть ли в доме молоко. Умный же холодильник, в случае отсутствия молока, может предложить кофеварке рецепт кофе со сливками, в тоже время заказав домой молоко и, даже, оплатив его самостоятельно!

Итак, подведем итог! Умный дом реализуется на базе технологии интернета вещей как сеть датчиков, бытовых приборов, гаджетов и устройств управления, которые связываются с хабом при помощи как проводных, так и беспроводных технологий (как общего назначения, так специализированных) через облачный сервер.

Управление всей этой сетью в идеале должно осуществляется с одного приложения на смартфоне, ПК или голосом через умного помощника.

Устройство, несовместимое с хабом, сможет управляться только через отдельное приложение, поэтому необходимо думать о совместимости Умных вещей и подсистем в рамках одного умного дома или же придется управляться с несколькими приложениями. Кроме того, в случае несовместимости, осложняется и интеллектуальная обработка и снижается эффективности принятия решений по управлению Умным домом.

Умные устройства расположены в разных частях дома и должны взаимодействовать друг с другом на расстоянии. При организации такого взаимодействия нужно учитывать свойства материалов (например, непроницаемость для радиоволн или же невозможность прокладки кабеля).

Умные устройства могу иметь автономное питание или же могут быть подключены к собственной сети электропитания дома.

Умные устройства должны общаться между собой (т.е. обмениваться информацией), а значит им нужен общий язык и правила общения.

И последнее, и очень важное - -доступ ко всей информации умного дома и управление всеми элементами Умного дома должны осуществляться только теми лицами, у которых есть на это права, т.е. легальными пользователями.

5 Безопасность и IoT

Давайте рассмотрим, как с умные решения позволяют нам организовать безопасную жизнь.

Прежде всего необходимо обратить внимание на то, что мы можем рассматривать вопросы обеспечения безопасности с различных ракурсов:

Современные технологии позволяют использовать умные решения и Интернет вещей для построения непосредственно систем безопасности. Т.е. таких систем, которые позволяют людям предотвращать опасные ситуации с реальной жизни. Например, мы можем построить интеллектуальную систему защиты от пожаров, задачей которой будет минимизация ущерба (в идеале, конечно, полное избежание ущерба).

В состав таких систем входят средства пожарной автоматики, к которым относятся:

- установки пожарной сигнализации (АУПС);
- установки пожаротушения (АУПТ);
- системы оповещения и управления эвакуацией людей при пожаре (СОУЭ);
- системы противодымной защиты (дымоудаления, или приточно-вытяжной вентиляции);

- системы управления (исполнительные устройства) различным инженерным и технологическим оборудованием зданий и сооружений (лифтами, электроснабжением, СКУД и пр.).

Рассмотрим, например, пожарные извещатели. Пожарные извещатели — это технические устройства (сенсоры), задачей которых является реагировать на изменение характеристик внешней среды, таких как задымление, повышение температуры, при возникновении пожара. И чем раньше сенсор отправит информацию о регистрации повышения контролируемого параметра, тем больше шансов избежать пожар.

В качестве контролируемого параметра в извещателях пожарной сигнализации могут использоваться следующие: дым, газ, тепло, свет, а также их комбинация. Чувствительный элемент сенсора регистрирует уровень параметра, преобразует его в электрический сигнал и передает на приемно-контрольные приборы системы пожарной сигнализации, где происходит дальнейшая обработка поступающих от различных извещателей информации для принятия дальнейших решений.

Давайте проанализируем, обладает ли рассматриваемый сенсор (извещатель), всеми свойствами, необходимыми для построения умных решений.

В качестве примера возьмем простой извещатель пожарный с датчиком дыма оптическим. Принцип работы вкратце можно описать следующим образом.

Извещатели пожарные дымовые срабатывают при попадании на оптико-электронную камеру датчика мельчайших частичек дыма. Принцип работы основывается на том, что посылаемый внутри датчика луч при наличии в воздухе частиц дыма рассеивается. При этом специальный датчик-фотоприемник фиксирует это изменение излучения. Малейшее «затуманивание» приводит к активации системы сигнализации. Для простых автономных извещателей активацией является световая и звуковая сигнализация – т.е. он усиленно моргает и кричит.

Является ли такой прибор Умным?

1. Собирает информацию – да. Содержит чувствительный элемент, который регистрирует уровень контролируемого параметра.

2. Хранит информацию – в простейшем случае нет.

3. Обрабатывать информацию - в простейшем случае нет, поскольку не содержит вычислительного элемента. Под обработкой понимается простое сравнение уровня сигнала на выходе чувствительного элемента с пороговым, заранее установленным значением.

4. Передает информацию - в простейшем случае автономной реализации нет. Извещатель только выдает светозвуковую информацию.

5. Принимает решение на основе информации – нет, извещатель никак не управляет системой пожаротушения.

Итак, простейших извещатель не может рассматриваться как умная вещь, хотя при этом является очень важным и надежным элементом обеспечения пожарной безопасности.

Плохо ли то, что наш извещатель пока что не очень «умен»? В общем случае ДА! Ведь будь он «поумнее», то в случае опасности мог бы не только «моргать и кричать», но и отправить информацию как владельцу помещения, так и в пункт пожарной охраны или же отправить управляющий сигнал на систему пожаротушения.

Примером построения таких поумневших извещателей являются извещатели с GSM модулем. Добавление этого модуля позволило расширить функционал, в результате наш извещатель может реагировать на появление дыма в помещении и оповещать о пожаре:

- громким звуком встроенной сирены;
- отправкой SMS на пультовые охранные системы;
- рассылкой SMS и дозвоном на телефонные номера.

Давайте проанализируем как поменялись свойства нашего извещателя

1. Собирает информацию – да. Содержит чувствительный элемент, который регистрирует уровень контролируемого параметра.
2. Хранит информацию – да, хранит информацию о номерах рассылки сообщений.
3. Обрабатывать информацию - в простейшем случае нет, поскольку не производит обработку согнала с чувствительного элемента для принятия решений. Под обработкой можно рассматривать формирование пакетов GSM.
4. Передает информацию – да. Помимо выдачи светозвуковой информации отправляет еще сигнал тревоги по GSM каналу.
5. Принимает решение на основе информации – нет, извещатель никак не управляет системой пожаротушения.

Есть ли потенциал для дальнейшего усовершенствования нашего извещателя – да. Мы можем подключать его к системе непрерывного мониторинга состояния помещения, использующую совместно информацию от нескольких различных датчиков, позволяющей удаленно настраивать и контролировать

состояние системы, а, так же, анализировать в комплексе состояние контролируемого объекта, что позволит принимать оперативные и точные решения по реагированию на изменения.

Такой системой, например, является система умного дома, в состав которого входит и подсистема обнаружения дыма, от компании Ростелеком.

Интеллектуальный анализ данных и удаленное управление позволит своевременно включать систему пожаротушения, в тоже время снижая вероятность ложных срабатываний. Таким образом повышая безопасность и комфорт нашей жизни. Важно отметить, что подобное рассуждение верно и для иных систем обеспечения безопасности жизни.

Сделаем вывод. Продвигаясь по пути усовершенствования наши умные вещи, например, Извещатели, приобретают все больше свойств по возможности работы с информацией, а самые умные из них обладают всеми, рассматриваемыми выше свойствами. Они интегрируются с системами удаленной обработки данными и управления объектами.

Такое развитие является источником возможностей по увеличению уровня безопасности жизни, постоянного мониторинга состояния как окружающих объектов и так и самого человека, однако, к сожалению, является и источником появления все новых уязвимостей информационной безопасности, в связи с все усложняющейся архитектурой решений.

Далее посмотрим на наш пример Умных решений в пожарной безопасности через призму обеспечения безопасности самих управляющих систем.

6 Безопасность умных систем на базе IoT

Надежность (Safety). Продолжим рассмотрение умных систем с точки зрения обеспечения их безопасности. Одним из важных направлений рассмотрения безопасности является задача обеспечения надежности таких систем.

Представим себе, что у нас есть умный дом, в котором есть несколько подсистем обеспечения безопасности жилища и все они объединены в умную систему управления.

В состав такой системы могут входить, например:

1. Подсистема контроля и управления доступом (умный замок).
2. Подсистема охраны периметра (умные датчики открывания дверей и окон, а также камеры видеонаблюдения).
3. Подсистема пожарной сигнализации.

Для сбора, хранения, обработки и передачи информации пользователям (хозяину и службам реагирования) используется Хаб, который, в свою очередь имеет подключение к Интернет и мобильную связь.

Рассмотрим пример работы. При появлении дыма в помещении, на чувствительный элемент датчика попадает поток отраженного от частичек сажи света, генерируемого внутри корпуса датчика. В результате реакции чувствительного элемента уровень выходного напряжения растет и при превышении заданного порога формируется информационный сигнал – сигнал тревоги, который передается пользователям системы. Передача может проходить как по проводному соединению, так и по беспроводному каналу связи. Сигнал может быть направлен непосредственно к Хабу, а может передаваться посредством сети Умных устройств дома. Хаб (а в некоторых случаях и сам датчик), отправляет сообщение Хозяину Дома и (не всегда) службам реагирования, отправляя смс или сообщения через Интернет.

А что, если с датчиком что-то не так? Что же может быть не так?

Датчик может прислать нам сообщение о задымлении, а его нет. В результате мы: лишний раз понервничаем, или все бросим и приедем навестить свой Умный дом. И совсем плохо, если наш Дом навестят службы реагирования. Такой тип нарушений называется ложным срабатыванием – ложной тревогой.

Другой вариант – датчик при появлении дыма может не сработать, и мы не получим сообщения о задымлении. Это крайне плохая ситуация, а ведь мы рассчитываем на наш Умный дом. Такой тип нарушений называется пропуском цели.

Обе эти ситуации крайне нежелательны, а увеличение вероятности появления таких событий уменьшает надежность системы Умного дома.

Для уменьшения вероятности ложной работы системы и, соответственно, увеличения ее надежности, можно увеличить число датчиков и решении о наличии тревожной ситуации принимать не по сигналу одного датчика, а в результате анализа информации от нескольких таких датчиков.

Рассмотрим упрощённый случай. (полноценно задачи расчёта показателей надежной работы системы рассматриваются в курсе Теории надежности)

Если датчиков два. Допустим они одинаковые и вероятность ложного срабатывания равна 0.1, т.е. вероятность правильного срабатывания равна 0.9%. Тогда, при параллельном подключении и принятии решения о тревожной ситуации при поступлении сигнала хотя бы с одного датчика мы получим вероятность ложного срабатывания равную:

$$0.1 \cdot 0.1 = 0.01,$$

т.е. наша система может сообщать правильное состояние в 99% случаях. А при параллельном подключении трех датчиков:

$$0.1 \cdot 0.1 \cdot 0.1 = 0.001,$$

т.е. наша система может сообщать правильное состояние в 99.9% случаях.

При увеличении числа параллельно подключенный независимых датчиков надежность системы увеличивается (но скорость этого прироста уменьшается)

Если же датчики передают информацию через сеть независимых устройств, то такое подключение уже рассматривается как последовательное. Т.е. при поломке (ложном срабатывании) хотя бы одного из устройств в цепочке, формируется ложное срабатывание датчика (т.к. информация о задымлении не дошла) и, в этом случае, на надежность влияет уже надежность всех элементов цепочки устройств с сети.

В этом случае вероятность ложного срабатывания вычисляется как, например, для двух устройств в сети:

$$0.9 \cdot 0.1 + 0.1 \cdot 0.9 + 0.1 \cdot 0.1 = 0.19,$$

т.е. наша система может сообщать правильное состояние в 81% случаев.

Итак, сделаем вывод:

1. В общем случае для увеличения надежности системы можно увеличить число однотипных узлов, работающих параллельно.

2. При передаче информации через узлы последовательно, надежность системы падает, т.к. поломка (неправильная работа) каждого узла приводит к невозможности доставить информацию.

3. Для получения реальных оценок надежности нужно применять аппарат Теории надежности и проводить расчет с учетом конфигурации подключения, характеристик узлов, и свойств потоков в системе. Потребуется знать вероятность безотказной работы всех компонентов, а также интенсивность отказов в системе.

Следует отметить, что кроме простого дублирования узлов (например, датчиков) в умных системах можно использовать комбинированную обработку информации от различных датчиков. Например, при поступлении сигнала от датчика дыма, мы можем проверить корректность этой информации подключив камеру и проверив изображение. Обработка полученной с камеры информации может позволить снизить вероятность ложных тревог системы умного дома. А вот на сколько – это уже вопрос точных расчетов.

На общий уровень надежности системы умного дома оказывают влияние все его элементы: датчики (узлы), сеть передачи информации внутри дома, Хаб, а также надежность каналов передачи данных (как каналов мобильной или спутниковой связи, так и каналов беспроводной связи).

Расчеты помогают убедиться, что надежность работы системы достигает требуемого уровня. Особенно важно обеспечение надежности для произ-

водственных систем и объектов критической инфраструктуры. Требования и правила расчёта описываются в соответствующих стандартах.

Однако, надо помнить, что современные умные системы - это не просто электро-технические системы, а системы, содержащие программно-аппаратную часть. А значит, кроме вопросов обеспечения надежности компонентов, необходимо также рассматривать вопросы обеспечения надежности работы программного обеспечения. Да и задачи оценки надежности компонентов иногда являются весьма нетривиальными, например, для однокристальных процессоров.

7 Безопасность самих систем IoT

Ранее мы рассмотрели, как влияет на безопасность умных решений надежность ее работы, т.е. надежность спроектированных компонентов, программного обеспечения с учетом конфигурации их объединения.

Мы выяснили, что некорректная работа элементов, а также их поломка могут приводить к весьма неприятным последствиям. Поломки системы могут быть вызваны поломками ее узлов, например, в результате старения компонентов, в результате появления шумов в каналах связи, или же в результате реализации ошибок программного кода. Такие поломки можно назвать естественными.

Однако, помимо естественных поломок, могут возникать и ошибки, связанные со злонамеренными атаками на систему. Анализом данного рода ошибок занимается наука – Информационная безопасность.

Для полноценного обеспечения информационной безопасности необходимо обеспечить следующие свойства информации: **Доступность** – простыми словами означает, что у «правильных» (авторизованных) пользователей системы есть доступ к информации, которая требуется для принятия решения, и именно тогда, когда это необходимо. **Целостность** – означает, что информация, предоставляемая пользователям, является достоверной и полной. **Конфиденциальность** – доступ к информации и любая работа с ней (например, модификация) предоставляется только легальным пользователям.

Существует целый ряд мер по обеспечению информационной безопасности.

Доступность – примером злонамеренных действий по снижению Доступности системы может быть DDoS атаки (distributed denial-of-service (разделенный отказ в обслуживании). Суть таки заключается в том, чтобы скорость поступления новых запросов на какой-либо важный узел в системе превышал скорость обработки этих запросов. Тогда со временем, очередь запросов будет настолько длинной, что фактически новые запросы уже не

будут обрабатываться, а узел станет недоступным (сломанным) для других элементов системы. Это и есть главный принцип ddos атаки.

Реализация такой атаки может привести к значительному, вплоть до критического, снижению надежности работы системы.

В нашем примере, если ddos атака будет проведена на Хаб, то никакая информация от умных устройств умного дома приходить пользователю не будет, конечно в случае, если Хаб – это единственный узел внешней коммуникации.

Источником же многочисленных запросов, приходящих на Хаб могут оказаться, например, домашние умные устройства, подхватившие вирус.

Другим вариантом нарушения Доступности может быть злонамеренное шифрование данных Умного дома. В этом случае, для доступа к данным легальному пользователю предлагается выкупить ключ шифрования для восстановления доступности.

Классическими методами борьбы с указанными выше проблемами являются установка антивирусов и своевременное обновления версий программного обеспечения.

Целостность – в качестве примера атаки на целостность информации можно рассмотреть вариант подмены реальной информации с камеры Умного дома на поддельную.

Такую подмену можно осуществить путем реализации атаки человек по середине (Man in the middle (MITM)). Суть заключается в перехвате и подмене трафика.

В нашем примере, если MITM атака будет проведена на беспроводной канал связи камеры и Хаба (напрмер Wi-Fi), то при получении сигнала тревоги от датчиков охраны периметра и при проверке информации с камеры будет получена недостоверная информация о том, что в помещении никого нет, в то время как злоумышленник уже захватывает наш умный холодильник и доедает последний бутерброд!

Классическими методами борьбы с указанными выше проблемами являются *идентификация* и *авторизация* при осуществлении доступа в систему, формирование контрольных сумм или электронной подписи для передаваемых сообщений, а также шифрование трафика сети.

Конфиденциальность – можно рассматривать как свойство информации по доступности только авторизованным пользователям.

Примером атак на конфиденциальность является атака на взлом учетных записей, например *Брутфорс* (происходит от английского словосочетания: brute force) — разновидность хакерской атаки — способ взлома учётных записей посредством автоматизированного подбора комбинаций паролей и логинов.

В нашем примере, при взломе учетной записи администратора Хаба, зло-

умышленник может получить несанкционированный доступ ко всем элементам Умного дома. В результате, например, через камеру следить, что мы кушаем на завтрак. Или же, заразить все устройства вирусом для проведения хакерских атак. В общем, возможностей у такого злоумышленника появляется очень, и очень много.

Для защиты, например, необходимо устанавливать сложные (соответствующие всем требованиям) пароли на все элементы системы. А установленные пароли «по-умолчанию», заменять на свои! Так же можно использовать счетчики попыток входа, для контроля и блокирования атак.

Подведем итог нашей лекции. Итак:

- Мы разобрали что такое умная вещь и для чего она нужна.
- Какими свойствами обладают умные вещи. Чем умная вещь отличается от любой другой.
- Какие ресурсы нужны, чтобы вещь считалась умной.
- Каким образом набор умных вещей превращается в умное решение.
- Как связаны понятия умное решение и безопасность. А именно:
  - Мы рассмотрели вариант использования умного решения для обеспечения безопасности и удобства нашей жизни и деятельности.
  - Рассмотрели, как связаны понятия умного решения и надежности.
  - Ознакомились с некоторыми аспектами обеспечения информационной безопасности самих умных решений.

Основной вывод:

- Умные вещи и решения – это очень удобный инструмент для повышения качества жизни человека.
- Однако, прежде, чем полагаться на них при принятии важных решений, и уж тем более при автоматизации реальных процессов (например, на производстве), необходимо оценивать и обеспечивать высокий уровень надежности таких систем.
- А, так же, предпринимать постоянные меры по обеспечению информационной безопасности.
- Иначе, умная и полезная вещь может превратиться во вредную и опасную.