Internet of Trash Things: какие проблемы принесет "Интернет вещей"

К 2021 году IoT принесет 50 миллионов тонн электронных отходов

Концепция "Интернета Вещей" предполагает добавление вычислительных способностей и радиопередающих модулей тем устройствам, которые ранее в этом не нуждались. Организация Объединенных Наций подсчитала, что к 2021 году люди произведут 52,2 миллиона тонн электронных отходов, не подлежащих переработке.

Причины стремительного увеличения отходов заключаются в том, что IoT устройства относительно просты и дешевы. Добавление полупроводниковых элементов и батарей питания в устройства ограничило их срок службы. Если раньше некоторые бытовые приборы могли работать десяток лет, то теперь их срок службы сократился в 2-3 раза. Также большинство современных электронных устройств не предполагает замены, а в некоторых случаях и подзарядки батарей. Предполагается, что после выхода из строя батареи устройство нужно утилизировать.

Например, компания Wilson производит баскетбольные мячи со встроенной интеллектуальной системой, позволяющей подключать устройство к смартфону по Bluetooth. Через приложение можно отслеживать время тренировки, и даже количество закинутых в сетку мячей:



После выхода батареи из строя компания Wilson перекладывает заду по утилизации этого "гаджета" на плечи пользователей. Тех же взглядов придерживаются некоторые производители электронных трекеров и браслетов. Количество IoT-устройства стремительно растет, и они становятся частью нашей жизни. Например, компания Tile производит брелки, облегчающие поиск часто теряющихся предметов:

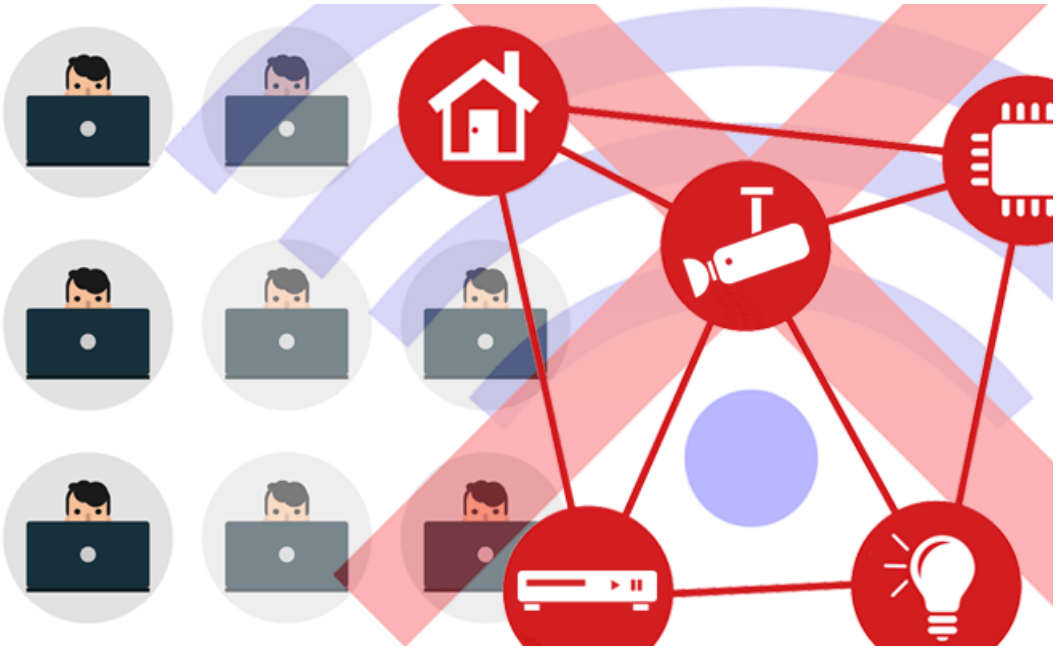


Компания Spire создает устройства для отслеживания активности человека и ритмов его дыхания в процессе тренировок. Все компоненты устройства находятся внутри плоского корпуса размером 5.3 на 3.2 сантиметра:



Некоторые компании, разрабатывающие IoT-устройства одновременно создают и программы по утилизации. Например, Dell перерабатывает свою продукцию и экономит благодаря этому до 3000 килограммов золота при изготовлении новых компьютеров и серверов. По мере того, как во все больше устройств внедряются драгоценные и токсичные металлы, людям нужно начинать заботиться об их повторном использовании, ну а производителям следует увеличивать срок службы IoT-устройств.

Безопасность в IoT-сетях



Интернет вещей мало похож на традиционную IT-инфраструктуру и это затрудняет защиту IoT-сетей. Каждое новое подключение физического устройства к сети становится источником угрозы безопасности. Таким образом, с появлением IoT, проблем с кибербезопасностью становится больше.

На предприятиях сотрудники служб безопасности и администраторы сетей принимают меры по защите данных в сети, запрещая подключение личных USB-устройств к машинам компаний, ограничивая доступ к информации для разных категорий пользователей.

Но предполагается, что IoT-устройства будут автоматически получать доступ к сети, и в случае взлома, подключение большого количества вредоносных устройств по беспроводной связи создаст тяжелые последствия. Проблема усугубляется тем, что большинство устройств IoT напрямую взаимодействуют с человеком и берут на себя ответственность за его жизнь как в прямом, так и в переносном смысле.

Чайник, которым можно управлять со смартфона - конечно круто! Но сколько вреда он принесет, когда управление даже этим безобидным устройством попадет в чужие руки. А в случае широкомасштабных взломов у пользователей будет пропадать доверие к фирме и рынку умных устройств в целом.

Даже сегодня не редки случаи, когда хакеры предлагают выкупить пароль от взломанного iPad’a. А сколько может стоить "пароль" от системы управления умным домом?

В настоящее время наблюдается сильное несоответствие цены IoT устройств и их качества. С одной стороны "Интернет вещи" требуют высокой степени безопасности и защиты данных, а с другой - низкой стоимости товаров. Но высокие требования к безопасности и низкая стоимость - вещи несовместимые.

Еще одна важная проблема безопасности заключается в том, что интеллектуальная часть IoT-устройств существует в уникальных операционных системах, а значит дыр в системах управления может быть бесчисленное множество. Интернет вещи нужны для решения разного круга задач, поэтому их физическая реализация и логика взаимодействия в сети сильно отличаются для разных типов устройств. Например, кардиостимулятор имплантируется в организм человека и должен незамедлительно среагировать тогда, когда это потребуется. Пока не существует никаких мер безопасности и строгих нормативных требований. Пользуясь таким "интеллектуальным" устройством человек сам несет ответственность за свое здоровье.

IoT и новый взгляд на частотные ресурсы

Так сложилось, что компании, покупающие частотные ресурсы, оценивают стоимость спектра исходя из того, сколько людей он сможет обсуживать. Таким образом, цены определяются величиной MHz pops (мегагерц на одного человека). Например, если ширина спектра составляет 3 МГц, в которой будет обеспечена связь для 2 миллионов человек, то получится значение 6 миллионов МГц/чел.

С появлением сетей связи пятого поколения и концепции "Интернета вещей", это представление изменится. Так FCC (Федеральная Комиссия Связт США) предлагает пересмотреть эту оценку и

считать не количество людей, которых будет обслуживать сеть, а целую экосистему технических вещей, которых ранее не было в сети: датчики, бытовые приборы, беспилотники и пр. Эти устройства также будут нуждаться в сотовой связи.

Например, ВМС США использует спектр частот в диапазоне 3,550 - 3,700 МГц. В 2014 году FCC предложила открыть этот диапазон шириной в ~150 МГц для LTE сетей. Диапазон привлекал внимание большого количества сотовых операторов. Например, американская компания GE Digital (ссылка: https://www.ge.com/digital/), которая разрабатывает программное обеспечение и оказывает консультационные услуги по инфраструктурным решениям связи, попросила FCC предоставить разрешение на создание новых типов Wi-Fi сетей диапазона 3,550 – 3,700 МГц.

Когда появляются новые частоты, то сразу встает вопрос лицензирования и стоимости. В связи с этим в США для таких лицензий есть конкретное название Priority Access Licenses или PAL. До недавнего времени PAL лицензии распределялись по разным районам страны и чем более населенным был район – тем дороже продавалась лицензия, из расчета МГц/чел.

Но с учетом появления 5G и IoT, FCC будет брать во внимание количество работающих устройств в сети, а не количество людей. Очевидно, что это сделано для того, чтобы поднять стоимость на дефицитные радиочастоты. FCC теперь разрабатывает нормативные документы к различным правилам, связанным с распределением PAL. Скорее всего FCC учредит новую схему аукционов с двумя различными видами PAL.

"Один из них может быть основан на охвате населения, тогда как другой, основанный на IoT, может смотреть на количество подключенных клиентов, обслуживаемых за точку доступа", Dave Wright, the president of the CBRS Alliance.

Таким образом, при продаже частот, малонаселенная сельская местность с огромной связанной фермерской инфраструктурой, построенной на сотнях тысяч сетевых датчиков, может быть оценена также как и крупный мегаполис. В общем, при продаже радиочастот настало время определить, насколько сильно используется спектр и продать лицензии по завышенной цене даже там, где это не нужно. По мнению FCC такая система распределения спектра будет более эффективной. Ну а для операторов это может стать началом новой эры в борьбе за дефицитные частотные ресурсы.