ИНТЕРНЕТ ВЕЩЕЙ

Вадим Подольный

Что такое Интернет вещей (IoT)?

На сегодняшний день существует несколько определений такого явления, как Интернет вещей. Зачастую многие вендоры и интеграторы также склонны интерпретировать данный термин по-разному, несколько видоизменяя трактовку. Несмотря на то, что сам термин и направление появились только в 1999 году, идея витала в воздухе достаточно давно. К примеру, еще в далеком 1926 году Никола Тесла в интервью для журнала «Collier's» сказал, что в будущем радио будет преобразовано в «большой мозг», все вещи станут частью единого целого, а инструменты, благодаря которым это станет возможным, будут легко помещаться в кармане. Одной же из самых первых «умных вещей» можно назвать тостер выпускника MIT Джона Ромки (одного из отцов-основателей протокола TCP/IP), подключенный к сети в 1990 году.

В качестве наиболее простого и оптимального для понимания определения Интернета вещей (IoT) можно привести следующее:

IoT — это совокупность устройств, обладающих интерфейсами сетевого взаимодействия, и самой объединяющей их сети. Важно отметить, что устройство может подсоединяться к данной сети через промежуточное сопряжение — или даже через цепочку сопряжений. Простейший пример: сопряжение фитнес-трекера с внешней сетью через мобильный телефон.

IoT — сеть физических объектов, обладающих встроенными технологиями взаимодействия с внешней средой с возможностью передачи данных о своём текущем состоянии и приеме данных извне.

Gartner https://www.gartner.com

IoT — концепция вычислительной сети физических предметов («вещей»), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой, рассматривающая организацию таких сетей как явление, способное перестроить экономические и общественные процессы, исключающее из части действий и операций необходимость участия человека.

Википедия https://ru.wikipedia.org

Наряду с термином IoT, часто также используется и другой термин, который появился существенно раньше – **M2M (Межмашинное взаимодействие, Machine-to-Machine)**, общее название технологий, которые позволяют приборам обмениваться информацией друг с другом. Это проводные и беспроводные системы датчиков, которые передают информацию от одного устройства другому. Одной из первых разработок в области мобильного межмашинного взаимодействия является OmniTRACS — решение Qualcomm, разработанное в 1989 году для отслеживания коммерческого транспорта.

Фактически M2M позволил технологиям АСУ ТП в режиме онлайн получать доступ к объектам, которые ранее были недоступны — не было возможности наладить с ними постоянное кабельное соединение. Такие объекты можно разделить на два класса: удалённые от кабельных сетей объекты и подвижные объекты. Ключевым фактором роста технологий M2M стало существенное развитие систем глобального позиционирования GPS/ГЛОНАСС и др.

Концепция IoT, появившись в 1999 году, в год представления технологии радиочастотной идентификации физических предметов (RFID), сразу получила мощный толчок к развитию. В 2008 и 2009 годах состоялся переход от «Интернета

людей» к «Интернету вещей», т.е. количество подключенных к сети предметов превысило количество людей.

Активная реализация и развитие технологических платформ на основе концепции продолжаются и сейчас. Ключевыми факторами развития IoT стали технологии межмашинного взаимодействия (M2M), развитие технологий связи 4G, распространение протокола IPv6, облачных технологий (SaaS, PaaS, IaaS и др.), программно-определяемых сетей (SDN) и программно-определяемых дата-центров (SDDC).

В первом десятилетии XXI века получила распространение доступная беспроводная связь, став важным фактором для развития технологий межмашинного взаимодействия.

Основными отраслями применения IoT стали:

1. Системы мониторинга и управления транспортом, ЖКХ, медицинскими устройствами.
2. Системы мониторинга и управления безопасностью автомобилей (противоугонные системы), судов, домов, квартир и офисов, людей и животных.
3. Системы мониторинга промышленного оборудования и т.п.

Промышленный интернет вещей (IIoT)

Отдельного рассмотрения заслуживает вопрос применения IoT в промышленности, где данное направление образует отдельный широкий кластер технологий, который получил название индустриального (промышленного) интернета вещей (Industrial IoT, IIoT).

Промышленный интернет вещей — это совокупность устройств (датчиков, контроллеров, установленных на узлах и агрегатах промышленного объекта), средств передачи, сбора, обработки, визуализации и интерпретации информации, объединенных в единую сеть.

Фактически, такое определение можно дать и автоматизированной системе управления технологическими (производственными) процессами (АСУ ТП, АСУ ПП).

АСУ ТП и IIoT

Корни концепции АСУ ТП уходят к середине XX века и начинаются с таких технологий, как тепловая автоматика, релейная защита и автоматика (РЗА). На этих системах строились первые схемы управления промышленным оборудованием в концепции жёсткой (не программируемой) логики — зарождалось первое поколение АСУ ТП. Человек, обслуживающий такие системы, называется главным механиком, главным технологом; его роль заключается в том, чтобы обойти все устройства, проконтролировать их корректную работу, снять показания и занести в таблицу.

При развитии технологий микроэлектроники появляются программно-логические контроллеры (ПЛК, Programmable Logic Controller, PLC), позволяющие

задавать алгоритмы управления в виде программ, что, в свою очередь, обеспечивает высокую гибкость, стандартизацию и формирование отрасли — появляется АСУ ТП второго поколения. Развитие сетевых коммуникационных технологий вкупе с объединением ПЛК в сети образуют АСУ ТП поколения 2+.

Третье поколение АСУ ТП связанно с появлением мощных микропроцессорных систем, серверов на их основе, рабочих станций, коммутаторов и маршрутизаторов. Логика ПЛК существенно разгружается, часть функций низовой автоматики забирают на себя системы верхнего уровня (СВУ). Появляются сложные промышленные сети, большое разнообразие контроллеров и программного обеспечения. Выделяются следующие направления:

- средства (сквозного) проектирования АСУ ТП в целом;
- средства программирования ПЛК;
- SCADA/HMI.

В начале XXI века компьютерные технологии продолжают развиваться, процессоры — усложняться, их мощность растёт, и в это же время цены на них существенно падают. Спектр задач, решаемых на микропроцессорной технике, расширяется, появляются методы обеспечения надёжности (резервирования, диагностики, безопасности) такой техники. Появляются алгоритмы функционально-группового управления (ФГУ) совокупностью исполнительных механизмов и производством в целом, построенных по принципу обратной связи. Такие АСУ ТП принято называть «Поколением 3+».

Важно отметить, что в АСУ ТП поколения 2, 2+, 3, 3+ присутствует роль человека — оператора АСУ ТП, получающего информацию и осуществляющего оперативное управление через СВУ.

Во втором десятилетии XXI века появляются интеллектуальные технологии и методы, которые принято называть технологиями «искусственного интеллекта» (ИИ), под которыми понимается совокупность следующих методов и технологий:

- нейронные сети (neural networks);
- нечёткая логика (fuzzy logic);
- генетические алгоритмы (genetic algorithm);
- машинное обучение.

Пункты списка определяет их суть — они являются оптимизирующими (аппроксимирующими, уточняющими) методами решения математических (алгоритмических) задач.

Появляется ряд технологий, которые сильно меняют подход к построению АСУ ТП:

1. Контроллеры с нейропроцессорами, обеспечивающие мгновенную идентификацию состояния узла или подсистемы.
2. Контроллеры с нечёткой логикой, обеспечивающие автономное принятие решения.
3. На мощных серверах локальных ЦОД появляются технологии построения аналитических инструментов для идентификации и прогнозирования состояния систем, управляемых АСУ ТП. Те, в свою очередь, используют технологии

машинного обучения на структурированных и не структурированных данных (Big Data).

4. Появляются математические сопроцессоры, ускоряющие решение базовых уравнений, описывающих наиболее распространённые технологические процессы:

- волновое уравнение (радиоэлектронная аппаратура, связь, РЭБ);
- уравнение непрерывности, Эйлера, Навье-Стокса, диффузии и др. (гидродинамика, движение жидкости, газа, аэродинамика, двухфазные потоки);
- вероятностные уравнения (метод Монте Карло, перенос частиц, нейтронно-кинетические расчёты);
- уравнения химии и радиохимии (расчёт химических процессов, в т.ч. испытывающих радиоактивный распад);
- уравнения физики прочности (расчёт сопротивления, прочности и надёжности материалов), и др.

	Промышленность		Автоматизация	+
Индустрия 1.0	Сила воды и пара	Поколение 1	Тепловая автоматика	РЗА
Индустрия 2.0	Сила электричества	Поколение 2	ПЛК	Сети
Индустрия 3.0	Сила ЭВМ	Поколение 3	ЭВМ	ФГУ
Индустрия 4.0	Сила IoT	Поколение 4	IIoT	СУУ ТП

Табл. 6.2.1. Этапы совершенствования АСУ ТП.

Моделирование технологических процессов в режиме реального времени становится реальностью, нейросетевые аппроксиматоры позволяют в режиме увеличенного пространственно-временного шага решать сложнейшие системы дифференциальных уравнений, описывающих технологические процессы с достаточно высокой точностью в рамках задачи прогнозирования управления на 30-60 секунд вперёд, что раньше занимало достаточно длительное время счёта и требовало серьёзных вычислительных ресурсов.

Таким образом, оператор получает мощнейшие инструменты, помогающие идентифицировать (оценить) ситуацию и предлагающие (в режиме советника) пространство вариантов для действий. Класс таких решений называется **системами поддержки принятия решения (СППР)**.

Не исключено, что повторяемые действия оператора, выполняемые по совету СППР можно, в свою очередь, автоматизировать — таким образом оператор становится супервайзером (наблюдателем). Часть функций управления отдаётся машине, и тогда для контроля крупного объекта автоматизации требуется меньше операторов. Например, АСУ ТП современной АЭС, которая обрабатывает информацию с десятков тысяч датчиков и управляет множеством исполнительных механизмов, оперируя сотнями тысяч рассчитываемых в режиме онлайн переменных, управляется всего двумя операторами и одним начальником смены.

Многие современные устройства низовой автоматики (датчики, контроллеры) стали интеллектуальными, они самостоятельно идентифицируют шум и отделяют его от реального изменения параметров, тем самым снижая общий поток данных в СВУ; они стали обладать коммуникационными интерфейсами, которыми сопрягаются с системой в целом, а не с «сухими» контактами, как в предыдущих поколениях. Много конечного оборудования — турбины, насосы, задвижки — изначально оснащены контроллерами диагностики и управления, и эти устройства также следует отнести к IIoT.

Такие решения классифицируются как АСУ ТП четвёртого поколения и напрямую лежат в пространстве концепции «Индустрия 4.0».

В целом концепция «Индустрия 4.0» обеспечивает возможность построения «бережливого производства»; в рамках концепции ставится задача оптимизации управления технологическими процессами для снижения аварийности и продления ресурса эксплуатируемого оборудования, что иногда формулируется как «переход от планово-предупредительного ремонта к ремонту по состоянию». Таким образом, к задачам управления АСУ ТП четвёртого поколения добавляется задача оптимизирующего (усовершенствованного) управления. Такие АСУ ТП называются **системами усовершенствованного управления технологическими процессами (СУУ ТП, Advanced process Control, APC)**. В состав СУУ ТП должны входить достаточно мощные средства долгосрочной предиктивной аналитики. На промышленных производствах анализируются такие параметры, как появление дефектов, охрупчивание, изменение химического состава стали элементов конструкций (что может привести к их разрушению), осаждение, стенозис частиц, уменьшение толщины стенок трубопроводов из-за абразивной полировки (что может привести к разрыву), оценивают вибрацию и её влияние на свойства конструкций, их соединений и многое другое. Если производство целиком управляется СУУ ТП, такое решение называется АСУ ТП поколения 4+.

Технологический прогресс не стоит на месте, и «машина» так или иначе забирает на себя всё больше функций управления промышленным предприятием. С одной стороны, это хорошо — снижается количество ошибок из-за «человеческого фактора», с другой стороны, одной ошибки в алгоритме ФГУ достаточно, чтобы появились существенные проблемы.

Сегодня на предприятиях лёгкой и тяжелой промышленности внедряется множество решений, включающих в себя стек технологий промышленного интернета вещей. К примеру, вновь закупаемые/обновляемые парки производственно-технологического оборудования и аппаратуры с поддержкой технологий промышленного интернета вещей уже сейчас могут самостоятельно контролировать текущее состояние производственного процесса (состояние конвейера, его подвижных частей и т.д.) и предсказывать возможные проблемы (отказ отдельных сегментов конвейерной линии). Масштабное внедрение оборудования и аппаратуры такого класса на производстве позволяет достичь существенного сокращения времени простоев технологического оборудования, влекущего за собой издержки и финансовые потери для производства, а также общее повышение эффективности производства и уровня контроля за состоянием — как отдельных компонентов технологического оборудования, так и производственного процесса в целом.

Надёжность и безопасность IIoT зависит от многих факторов, которые могут найти своё отражение на каждом из этапов жизненного цикла любого из компонентов системы в целом. Построение надёжной и безопасной IIoT-системы зависит от проработанности технологий проектирования и эксплуатации отдельных компонентов и системы в целом, что определяется технологической платформой, в которой разрабатывается и эксплуатируется система.

Связь в IoT

Особая роль в проектировании и последующей реализации и сопровождении архитектуры IoT уделяется вопросам обеспечения сетевого взаимодействия всех аппаратных компонентов. Это во многом обусловлено тем, что развитие технологий IoT требует высокого технологического разнообразия средств и каналов связи, обеспечения их стандартов, надёжности и безопасности связи в целом.

Проводная связь

Исторически самый надёжный и простой способ передачи данных между устройствами — это физическое соединение кабельным каналом связи.

С развитием технологий автоматизации и существенным удешевлением микроэлектроники, датчики все чаще обретают дополнительный функционал за счет использования микроконтроллеров в своей конструкции, что обеспечивает возможность обмена цифровой информацией с устройствами сбора данных и/или иными датчиками, в том числе с использованием шлюза/маршрутизатора, и зачастую штатно имеют в своей конструкции разъёмы Ethernet, обеспечивающие подключения в том числе и по оптическому каналу.

Современные проводные сети используют, как правило, витую пару и порты стандарта RJ-45. Работа проводных сетей описываются стандартами IEEE 802.3. На сегодняшний день используются следующие стандарты:

- IEEE 802.3u с максимальной пропускной способностью 0,1 Гбит/сек.
- IEEE 802.3ab с максимальной пропускной способностью 1.0 Гбит/сек. и др.

Существует также стандарт IEEE 802.3an с максимальной пропускной способностью 10 Гбит/с, разъем SFP+.

Однозначным плюсом применения проводных сетей являются их надёжность и безопасность. Для осуществления вмешательства нарушителю необходим физический доступ к кабелю. Указанные выше стандарты сохраняют свои характеристики при длине медного кабеля до 100 м (при использовании оптического кабеля расстояния могут быть гораздо больше).

Рис. 6.2.1. Бытовой Power Line контроллер TP-Link.

Power Line Communication (PLC)

Важнейшей современной технологией проводной связи для IoT является возможность передачи данных по линиям электропередачи (ЛЭП, Power Line Communication, PLC). Такая сеть может передавать данные, накладывая аналоговый сигнал поверх стандартного переменного тока частотой 50 Гц или 60 Гц. PLC включает BPL (англ. **Broadband over Power Lines** — широкополосная передача через линии электропередачи), обеспечивающий передачу данных со скоростью до 1 Гбит/с, и NPL (англ. **Narrowband over Power Lines** — узкополосная передача через линии электропередачи) — со значительно меньшими скоростями передачи данных, до 1 Мбит/сек.

Технология PLC удобна для подключения узлов к сети Интернет, объединения в сеть бытовых устройств в офисе, а также в ЖКХ и в системах безопасности.

Беспроводная связь

И всё же основным фактором развития технологий IoT является появление и повсеместное распространение доступной беспроводной радиосвязи. В большинстве случаев устройства IoT зависимы от автономного питания, и встаёт вопрос об энергии, затрачиваемой на коммуникации — чем более энергоэффективным окажется используемый устройством модуль передачи данных, тем дольше прибор сможет оставаться автономным.

Помимо очевидных задач обеспечения максимальной энергоэффективности модулей передачи данных, присутствуют требования к мощности приемопередатчика, например в случае размещения устройства на географически отдаленном объекте, не имеющем прямого подключения к сети.

В соответствии с данными требованиями, можно классифицировать применяемые модули по радиусу действия:

- малый — NFC, Bluetooth, «нательная» компьютерная сеть;
- средний — WiFi, ZigBee, мобильная связь, LTE, 5G;
- дальний — спутниковая связь, LPWAN, LoRa, СТРИЖ.

NFC (ISO 14443)

NFC (**Near Field Communications**, Ближняя бесконтактная связь) — технология беспроводной передачи данных малого радиуса действия, предоставляющая возможность обмена данными между устройствами, находящимися на расстоянии около 10 см, анонсирована в 2004 году. Особенность данной технологии — отсутствие постоянного соединения.

Применяется в основном для считывания данных со смарт-карт, смартфонов, смарт-часов и прочих носимых с собой устройств для осуществления бесконтактных платежей, идентификации и прочих задач, требующих краткосрочного соединения.

Считыватель NFC может работать только с одним источником данных на расстоянии не более 0,2 м. Скорость установки соединения — менее 0,1 сек. NFC полностью совместим с системой меток RFID.

Bluetooth (IEEE 802.15.1)

Протокол относится к беспроводным персональным сетям (Wireless Personal Area Network, WPAN).

Bluetooth — распространённый стандарт, обеспечивающий обмен информацией между периферийными устройствами ПК (POS-терминалы, клавиатуры, принтеры и прочие устройства), мобильных (мобильные телефоны, планшеты и пр.) и носимых устройств (смарт-часы, трекеры, гарнитуры).

Bluetooth позволяет этим устройствам осуществлять обмен данными, когда они находятся в радиусе до 10 м друг от друга (дальность сильно зависит от условий эксплуатации и размещении устройств — преград и помех). Скорость установки соединения — от 5 сек.

На сегодняшний день наиболее распространённым является стандарт Bluetooth 4.X, скорость передачи информации в котором может достигать 3,125 МБ/сек с возможностью осуществления соединения с устройствами на расстоянии до 50 м (в идеальных условиях, с отсутствием явных препятствий). В стандарте Bluetooth 5.0 скорость увеличивается до 6,25 МБ/сек, а расстояние — до 200 м (в идеальных условиях, с отсутствием явных препятствий) и, что важно, при большей энергоэффективности по сравнению с предыдущими версиями стандарта. Стандарт Bluetooth 5.0 разработан для IoT устройств и представлен в 2016 году.

ZigBee (IEEE 802.15.4)

ZigBee относится к семейству протоколов WPAN. (WPAN – Wireless personal area network, применяется для связи различных устройств, включая компьютерную, бытовую и оргтехнику, средства связи). Данный протокол можно отнести к переходному между малым и средним радиусом действия. Расстояние уверенного

приёма-передачи устройств, осуществляющих подключение по данному протоколу, не более 75 м (до 1,5 км с использованием дополнительного оборудования в виде усилителя ZigBee Pro). Скорость передачи данных — до 250 КБ/сек.

Ключевой особенностью данной технологии является способность при низком энергопотреблении поддерживать не только простые топологии сети («точка-точка», «дерево» и «звезда»), но и самоорганизующуюся и самовосстанавливающуюся ячеистую (Mesh) топологию с ретрансляцией и маршрутизацией данных. Также она 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 развёртывания, обслуживания и модернизации.

ZigBee, в основном, применяется в решениях промышленного интернета вещей.

Мобильная связь (LTE, 5G)

Мобильная связь стала основным фактором, повлиявшим на рост рынка IoT-устройств. При повсеместном вводе сетей 5G в эксплуатацию рост рынка IoT станет лавинообразным. Базовые станции 5G смогут одновременно обслуживать миллионы устройств, обеспечивая надёжные соединения с ними на скоростях до нескольких ГБ/сек при большей энергоэффективности, чем в сетях 4G. Конечно же, сначала 5G будет доступен только в крупных городах, а максимальное расстояние до базовых станций составит сотни метров.

Особенность сетей 5G заключается в том, что в рамках физической сети можно создавать программно-определяемые сети (SDN) и создавать Mesh-сети с задаваемыми параметрами маршрутизации и ретрансляции данных.Важным фактором роста IoT в сетях 5G будет отказ от физической SIM-карты и переход к виртуальной SIM-карте, что одновременно и уменьшит, и удешевит конечные потребительские устройства.

Энергоэффективная сеть дальнего радиуса действия (Low-power Wide-area Network, LPWAN)

LPWAN — беспроводная технология передачи небольших по объёму данных на дальние расстояния, разработанная для распределённых сетей телеметрии, M2M решений и оборудования IoT. Технологии LPWAN позволяют передавать данные на расстояния до 15 км при достаточно низком энергопотреблении. Особенность LPWAN заключается в высокой проникающей способности радиосигнала в условиях городской застройки.

В семействе LPWAN выделяют технологии NB-IoT и LoRa.

NB-IoT разработана на базе существующих стандартов мобильной связи. Сети NB-IoT работают в лицензируемом спектре частот. Стандартизация технологии завершилась в июне 2016 года. Курирует разработку этой сети объединение 3GPP. В NB-IoT обеспечивается поддержка более 100 тысяч соединений на соту; аккумулятор устройства, подключенного к NB-IoT, может

работать до 10 лет без подзарядки. Технология проприетарная и требует лицензирования.

Технологию **LoRa** продвигает LoRa Alliance, в который входят IBM, CISCO и ещё более 500 компаний. Наиболее известный протокол LoRa, **LoRaWAN** – это аппаратный протокол управления связью между LPWAN-шлюзами и конечными узлами устройств. Сеть LoRaWAN (Long Range Wide-Area Networks – глобальная сеть большого радиуса действия) развёртывается в частотном спектре, не требующем лицензирования. Устройства в сети LoRaWAN асинхронно передают данные для отправки на шлюз. Затем несколько шлюзов, получившие эту информацию, отправляют пакеты данных на централизованный сервер сети, а с него пакеты уходят на серверы приложений.

Мобильные операторы связи предоставляют услуги связи LoRaWAN более чем в 250 городах мира. Такую популярность этого стандарта специалисты объясняют низким уровнем энергопотребления (устройства могут работать до 10 лет без подзарядки), большой территорией покрытия и невысокой стоимостью адаптеров.

Также на отечественном рынке доступна технология СТРИЖ.

СТРИЖ — российская телекоммуникационная компания, разработчик автоматизированных решений на базе собственной LPWAN-технологии. Компания занимается построением национальной LPWAN-сети для подключения различных энергоэффективных устройств, приборов и датчиков, разрабатывает и внедряет системы по удаленному сбору данных телеметрии для M2M и Интернета вещей.

Нательная компьютерная сеть (Body Area Network, BAN, IEEE 801.15.6)

Тело человека проводит радиоволны и электричество, что позволяет создавать нательную сеть. BAN-устройства могут быть имплантированы в тело, прикреплены к поверхности тела в фиксированном положении или совмещены с мобильными переносными устройствами.

Устройства, использующие BAN, прежде всего ориентированы на сферу медицины. Такие IoT-устройства собирают информацию о состоянии здоровья человека и передают её потребителю с помощью мобильных устройств.

Особенности маршрутизации в сетях IoT

Важным вопросом является маршрутизация в IoT-сетях. Многие IoT-устройства оснащены лишь коммуникационными модулями ближней связи и нуждаются в ретрансляционном устройстве для передачи данных по назначению.

По оценкам аналитиков, к 2020 году количество IoT-устройств может составить до 50 млрд. Единиц — а, как известно, пространство IPv4 адресов заканчивается. В связи с этим всё острее встает необходимость перехода на протокол IPv6.

Существует разработка «усечённого» протокола IPv6 для сокращения размера IP-адреса в малых сетях IoT 6LoWPAN, при этом пограничные маршрутизаторы могут преобразовывать эти «хеши» в обычные адреса IPv6.

Сети ячеистой топологии (Mesh)

Ячеистая топология сети построена по принципу ячеек, в которых узлы сети соединяются друг с другом и способны выполнять роль маршрутизаторов для остальных подключенных узлов. Такая топология сети является достаточно сложной в настройке, однако, при такой топологии реализуется высокая отказоустойчивость. Как правило, узлы соединяются по принципу «каждый — с каждым (доступным)». Таким образом, большое количество связей обеспечивает широкий выбор маршрута трафика внутри сети — следовательно, обрыв одного соединения не нарушит функционирования сети в целом. Mesh-сети обеспечивают возможность ретранслировать трафик от источника постоянного соединения с глобальной сетью к отдалённым, мобильным устройствам (IoT).

Mesh-сети бывают проводными, однако наибольшее распространение получили их беспроводные реализации, которые называются беспроводными ячейковыми сетями. Выделяют следующие особенности таких сетей:

• **Самоорганизация сети**. Является ключевой особенностью беспроводной Mesh-сети. Это означает, что при подключении каждый узел автоматически получает информацию обо всех других узлах и определяет свою роль.

• **Самовосстановление сети**. При выходе из строя одного из узлов сеть способна перенаправить данные, т.е. переопределить маршруты автоматически.

• **Быстрое и недорогое развёртывание**. Развёртывание ячеистой сети не требует дорогостоящей инфраструктуры. В силу способностей к самоорганизации и самовосстановлению, такая сеть во многих случаях является экономически выгодной в эксплуатации.

Многие протоколы по умолчанию поддерживают ячеистую организации сети. Например, Bluetooth поддерживает протокол Bluetooth Mesh, протокол ZigBee поддерживает ячеистую структуру… Достаточно просто собрать Mesh-сеть и из маршрутизаторов Wi-Fi. Принцип работы сетей 5G также включает возможность организации Mesh-сети.

Благодаря большому адресному пространству IPv6 позволяет поднимать Web-сервисы на любом устройстве IoT. Для этого создан протокол Constrained Application Protocol (CoAP, RFC 7252), который предназначен для использования в устройствах с сильно ограниченными ресурсами. Он обеспечивает возможность передачи данных через Интернет (Web Transfer Protocol) с полной поддержкой архитектуры REST.

IPv6 не только предоставляет мощные функции для поддержки мобильности конечных узлов, но и обеспечивает мобильность узлов маршрутизации сети, что, в свою очередь, позволяет создавать не только классические сети, но и такие, как сети ячеистой топологии (mesh) или гибридные (Рис. 6.2.2).

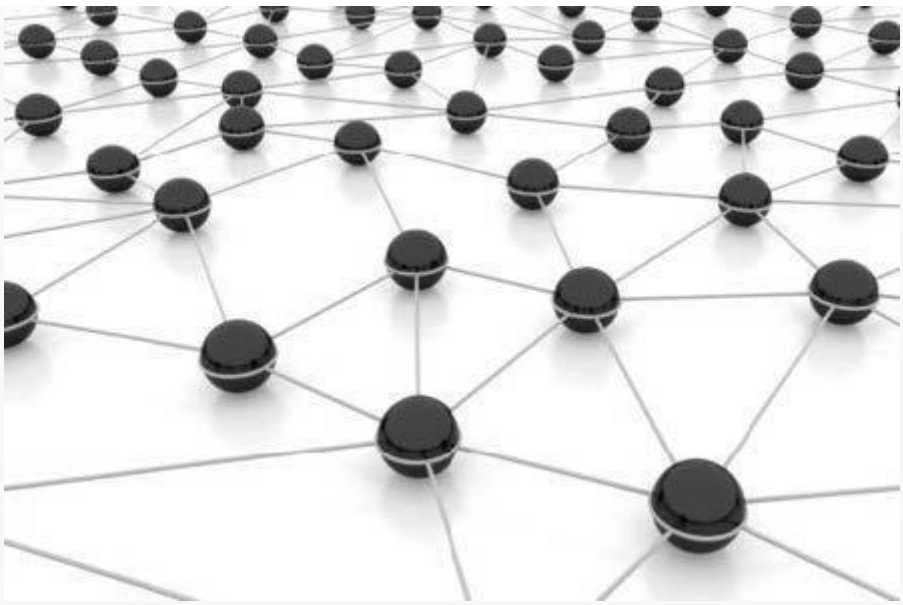

Рис. 6.2.2. Топология Mesh сети.

Энергоэффективность сетей

В большинстве случаев IoT-устройства проектируют с учетом двух ключевых тезисов:

- максимальная компактность конструктива и исполнения с целью упрощения дальнейшего монтажа устройства;
- обеспечение максимально продолжительного времени автономной работы, в идеале без потребности во внешнем источнике питания.

В идеале устройство не должно требовать дополнительного внешнего питания для своего функционирования, либо должно быть встроенным в инфраструктуру другого объекта, который и обеспечивает IoT-блок энергией (например, IoT-кофеварка, где датчик запуска легко может питаться от сети, к которой подключена сама кофеварка). Но в ряде случаев обойтись только внутренним питанием для устройства все еще не представляется возможным — и всё чаще возникает задача автономного питания. На Рис. 6.2.3 схематично представлена зависимость между расстоянием и энергоэффективностью для рассмотренных выше сетевых технологий.

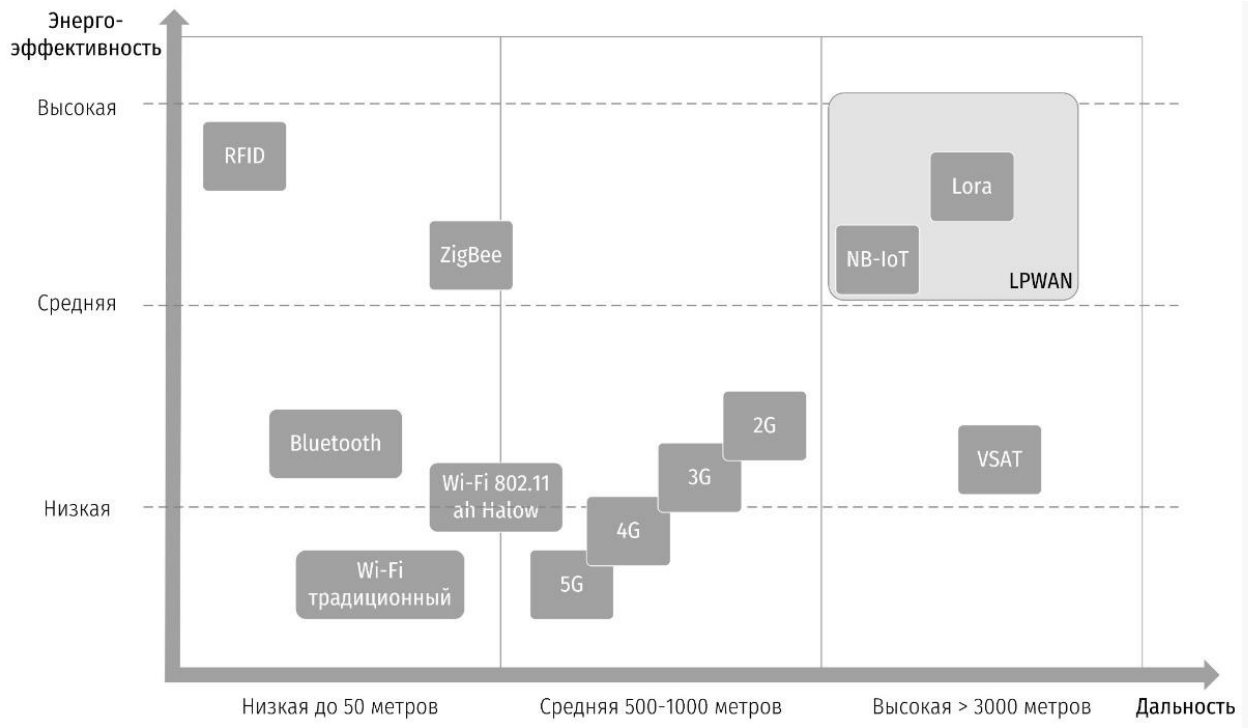

Рис. 6.2.3. Схема энергоэффективности для различных сетевых технологий.

Области применения IoT

Умный дом

Домашняя автоматизация (home automation), или умный дом (smart home) — это система домашних устройств, объединенных в сеть по различным каналам связи и способных решать повседневные задачи без участия человека.

Задачи, решаемые контроллерами автоматизации умного дома, разделяются на контроль (мониторинг) и управление — как и в обычной промышленной автоматизации.

Система умного дома включает три типа устройств:

- шлюзовые контроллеры (хабы) — управляющие устройства, соединяющие все элементы системы друг с другом и обеспечивающие централизованный доступ к системе (по единому протоколу, API, приложению и др.);
- датчики (сенсоры) — устройства, получающие информацию о внешних условиях;
- актуаторы —устройства, непосредственно исполняющие команды.

Датчики и актуаторы – IoT-устройства, в составе которых есть модуль сетевого взаимодействия и передачи данных в сети умного дома– разделяются:

- контроллеры управления водоснабжения, газоснабжения, электроснабжения, Smart Grid и др.;
- контроллеры домашнего климатического оборудования (кондиционеры, увлажнители, отопительная техника др.);

- контроллеры управления уровнем освещения;
- контроллеры управления бытовыми устройствами (чайник, духовка и др.);
- контроллеры управления медиаустройствами (аудио, видео, связь);
- контроллеры клинингового оборудования (робот-пылесос, робот-мойщик окон);
- контроллеры голосового управления;
- контроллеры управления жестами;
- контроллеры систем безопасности (системы контроля и управления доступом — СКУД, мониторинг движения, голоса, пирометрии и т.д.);
- датчики протечек воды.

Существует три механизма управления умным домом:

- автономное управление;
- управление пользователем;
- управление внешним оператором.

Умный дом с автономным управлением выполняет базовые простейшие сценарии управления, например:

- зашёл в комнату — включился свет;
- все покинули дом — все системы перевелись в энергосберегающий режим.

Пользовательское управление заключается в прямых осознанных действиях пользователя, например:

- хлопнул в ладоши два раза — выключился свет;
- сказал «чайник, кипяти!» или нажал кнопку в мобильном приложении — включился чайник, если в нём есть вода;
- перевёл дом в режим сна — все системы перевелись в энергосберегающий режим.

Умный дом, управляемый внешним оператором — это отдельный бизнес будущего, элементы которого можно наблюдать уже сегодня (например, мониторинг безопасности домов и квартир).

Внешнее оперативное управления можно разделить на два типа: автоматизированное и ручное. Потребителю будут доступны пакеты услуг (пакеты сценариев) управления его умным домом. С каждым новым устройством сложность управления умным домом будет расти, и на помощь придут соответствующие приложения, которые будут загружаться в умный дом (контроллеры, хабы, серверы управления) или будут доступны в режиме SaaS (Software as a Service). Возможно, что в «умном доме будущего» не будет даже сервера и хаба, все контроллеры будут управляться в режиме IaaS (Infrastructure as a Service; SHaaS — Smart Home as a Service). Такие сервисы будут обеспечивать выполнение сложных задач, таких как:

- анализ содержимого холодильника и заказ продуктов — сервис будет анализировать запах и внешний вид в холодильнике, принимать решение: какой продукт испортился, информировать об этом пользователя и предлагать перечень продуктов к закупке. Возможен и сценарий без информирования пользователя:

служба доставки привезёт новые продукты, положит их в холодильник и утилизирует испорченные или просроченные;

- анализ чистоты помещений — управление клининговой техникой, возможно, доставляемой при необходимости по подписке; вызов клининговой службы и контроль её работы;
- управление медиаконтентом в умном доме и другие активности.

Очевидно, что для управления IoT умного дома потребуется платформа, сопрягаемая с огромным количеством сервисов, обеспечивающая функционально-групповое управления (ФГУ) устройствами — как в автономном интеллектуальном режиме, так и в режиме оперативного управления.

Smart Grid

Современный умный дом — это не только потребление электроэнергии из сети, но и её генерация. В умном доме могут быть установлены солнечные батареи, реже — частные ветрогенераторы, ещё реже — генераторы, работающие на биогазе, или источники геотермальной энергии.

Такие умные дома подключены к умной сети распределения электричества (Smart Grid), и они могут не только обеспечить собственные нужды умного домохозяйства, но и отдавать часть сгенерированной электроэнергии в сеть. Концепция Smart Grid предусматривает компенсацию за принятое в сеть электричество домохозяйству согласно тарифам.

Также концепция Smart Grid включает механизмы автономного накопления электроэнергии и её использования в случае нехватки мощности автономных источников домохозяйства. В случае отключения централизованного энергоснабжения (аварии в энергосистеме), Smart Grid может перераспределить электроэнергию автономных домохозяйств на важнейшие источники потребления в округе, например, в больницу.

Естественно, что узлы Smart Grid являются узлами IIoT и могут централизованно управляться местным оператором.

Умное здание

Умное здание отличается от умного дома тем, что в здании могут не только жить, но и работать. Управление умным зданием требует большей ответственности, следовательно, многие системы должны быть резервированы — в том числе и IoT-устройства, управляющие умным зданием. Управление умным зданием может быть сопряжено с бизнес-показателями, достижение которых запланировано занимающими его бизнес-единицами. Умное здание может содействовать в выполнении поставленных бизнес-показателей, корректируя поведение каждого отдельного постоянного или временного пользователя умного здания:

- СКУД умного здания может ограничивать нахождение пользователя на рабочем месте, напоминать о необходимости размяться, пообедать, закончить курить, покинуть рабочее место;

- видеонаблюдение СКУД может контролировать не только перемещение сотрудника, но и его эмоциональное состояние;
- климатические контроллеры умного здания могут создавать требуемые условия для повышения эффективности труда;
- личная окружающая среда сотрудника и энергетическая эффективность;
- умное здание может быть сопряжено с личными IoT-устройствами пользователей, контролировать их медицинские показатели и др.

Для крупного бизнеса энергоэффективность становится все более значимым фактором, напрямую связанным с ростом числа сотрудников, а следовательно, и офисного пространства. Внедрение датчиков и систем управления освещением, системами кондиционирования и офисной техникой потенциально могут привести к экономии электроэнергии в 20-30%. Интересные примеры подходов к оптимизации энергоэффективности демонстрировали сотрудники Массачусетского технологического университета, разработавшие систему учета количества людей на территории, чтобы повысить энергоэффективность системы отопления в полупустом здании. Система должна регулировать уровень систем отопления в зависимости от числа людей в офисе и их расположения. Также разрабатывается система, позволяющая создавать для каждого сотрудника свой микроклимат.

При наличии автоматизированного управления климатическими системами (термостаты, кондиционеры, системы очистки/увлажнения воздуха, ионизаторы и прочие системы) с помощью датчиков можно исключить ошибки и снизить негатив, связанный с изменением параметров климата в здании вручную. Более того, в некоторых случаях возможно обеспечение «индивидуального микроклимата» для каждого из сотрудников. С точки зрения обеспечения безопасности и контроля доступа в здание, применение устройств промышленного интернета вещей позволяет обеспечить мониторинг перемещений сотрудников, а также обеспечивать максимально оперативную реакцию на нештатные ситуации (пожар, потоп, другие техногенные происшествия) и потенциальные угрозы (вторжение посторонних лиц в здание, нарушение сотрудником периметра безопасности, неадекватное поведение окружающих и прочие).

Разработка и внедрение сценариев управления умным зданием в скором времени может стать высокодоходным бизнесом, ведь в корпоративном мире очень мало тех, кто легко и безосновательно поддается на очарование появляющихся на рынке новых технологий — во главе угла по-прежнему должен оставаться бизнес, а значит, и требования к внедрению подобной автоматизации должны отталкиваться от выгоды предприятия, включая появление возможности централизованного управления (как административного, так и технического), что в целом упрощает жизнь специалистам административно-хозяйственных подразделений, а также снижает расходы на содержание и обслуживание инженерной инфраструктуры.

Офисная автоматизация во многом подразумевает внедрение специфичных для бизнеса сервисов. Их состав и варианты интеграции в единое корпоративное информационное пространство могут варьироваться в зависимости от сферы деятельности компании, регламентов информационной безопасности и внутреннего устава компании (отсутствие фиксированных рабочих мест сотрудников, удаленная работа с доступом к внутренней офисной инфраструктуре, жесткая ролевая модель доступа к определенному типу ресурсов и пр.).

Рис. 6.2.4. Часы-тонометр Omron Zero 2.0.

Умный город

Умный город — это концепция сопряжения различных автоматизированных систем управления объектами городской инфраструктуры в единую управляемую систему управления городом. Большая роль в концепции отведена IoT-устройствам. По оценкам ООН, к 2050 году две трети населения Земли будут проживать в городах.

Термин «Умный город» начал проскальзывать в СМИ с середины 1990-х годов, и с каждым годом, видя всё большее проникновение информационных технологий во все сферы деятельности, широкая общественность и эксперты начали осознавать роль, отведённую ИТ-отрасли в проектировании и эксплуатации городских объектов, среди которых можно упомянуть транспорт, логистику, общественную безопасность, защиту окружающей среды и многие другие. Со временем за счет появления все новых технологических инноваций ориентир понятия «умный город» стал затрагивать и область управления/самоуправления городской инфраструктуры — речь о предоставлении удобных и понятных механизмов, позволяющих гражданам принимать участие в решении ряда административных вопросов, а также выносить на обсуждение собственные предложения и идеи. На сегодняшний день ИТ-составляющая начинает закладываться уже при проектировании зданий и кварталов, а также при городском планировании в целом. Можно привести в пример ряд городов Южной Кореи и Китая, где эта практика применяется уже достаточно широко. Цели создания умного города заключаются в:

- повышении эффективности управления города в целом;
- повышении эффективности использования бюджетных средств города;
- управление ресурсами инфраструктуры города;
- повышении интегральной безопасности города;
- планировании управления городом в целом.

Концепция умного города подразумевает «переиспользование» как инфраструктуры, так и данных.

В современном городе масса различных объектов инфраструктуры:

• гражданские строения и здания — жилые и офисные, гостиницы, торговые центры, школы, больницы, поликлиники;

• промышленные инфраструктурные объекты — генерация и распределение электричества; водоочистка, водораспределение, водоотведение; теплоснабжение; газоснабжение; ЦОД (информационное снабжение);

• транспортная инфраструктура — метро, инфраструктура трамвайного и троллейбусного движения, дороги, мосты, эстакады, тоннели, светофоры, речные шлюзы, порты, аэропорты; геоинформационные системы; общественный и частный транспорт; обслуживающий и ремонтный транспорт;

• службы реагирования (МЧС, скорая помощь, пожарная охрана и др.) — ситуационные центры, системы поддержки принятия решений, система 112;

• инфраструктура безопасности — видеонаблюдение, видеоаналитика, фотофиксация;

• человек — биометрия; дополненная и виртуальная реальность.

Каждый объект инфраструктуры города (подсистема) уже так или иначе автоматизирован, и встаёт несколько важных вопросов:

• Как определить пригодность существующих подсистем к сопряжению и модернизации?

• Как автоматизировать устаревающие системы?

• С чем сопрягать все подсистемы?

• Где хранить собираемые данные?

• Как и где обрабатывать собираемые данные?

• Что «вытаскивать» из обрабатываемых данных?

• Каким образом использовать результат обработки в сопрягаемых системах и обеспечивать обратную связь?

• Как обеспечить информационную безопасность сопрягаемых систем и сопряжения в целом?

• Как обеспечить прозрачность и управляемость системы в целом?

Рис. 6.2.5. Glucowear — неинвазивный глюкометр.

Рис. 6.2.6. Робот-хирург Da Vinci.

Умный транспорт

В умных городах общественный транспорт будет (а в некоторых уже) оснащён контроллерами IoT. Кроме мониторинга позиционирования, такие контроллеры выполняют много различных функций — некоторые изложены ниже.

В общественном транспорте:

- приём платежей и контроль проезда;
- контроль безопасности пассажиров и водителя;
- контроль расхода топлива;
- управление интервалами движения.

В личном и персональном общественном транспорте (например, в каршеринге):

- разблокировка и активация двигателя с помощью личных IoT-устройств;
- контроль и получение информации о состоянии транспортного средства;
- управление маршрутами и мониторинг пробок;
- контроль и экстренное реагирование при авариях (например, ЭРА ГЛОНАСС);
- прослушивание салона и анализ речи в целях обеспечения безопасности и персонификации рекламы.

Умный транспорт, оснащённый IoT, позволяет оптимизировать маршруты и управлять загруженностью дорог. Умный транспорт сам становится IoT-устройством и позволяет контролировать своё состояние, вовремя предупреждает о необходимости технического обслуживания. Умный транспорт сопрягается с сервисами оператора технического центра, дорожными службами, службами экстренного реагирования, используя специальные платформы сопряжения.

Использование IoT в логистических и транспортных услугах и сервисах может существенно повысить их эффективность и функциональность. Например, IoT, а точнее, уже IIoT, может быть использован при управлении складским хозяйством и таможенными/складскими терминалами, где технология может использоваться для автоматического заказа расходных материалов/объектов хранения до того, как их запасы полностью иссякнут. Это позволит сократить количество ненужных единиц хранения на складах, обеспечивая наиболее оптимальное и эффективное использование складских помещений, постоянное наличие востребованных товаров на складах. Благодаря этому снижается время ожидания поставок конечным заказчикам, снижается нагрузка на сотрудников — и появляется возможность переориентировать их на выполнение других задач.

Также данные технологии могут применяться для отслеживания и обеспечения сохранности транспортируемых грузов, а также осуществлять мониторинг корректности функционирования климатического оборудования для обеспечения оптимальной среды транспортировки/хранения замороженных и/или скоропортящихся грузов. Внедрение данных технологий позволяет повысить эффективность транспортировки, выявить наличие проблем и нарушений в процессе транспортировки и хранения, а также сократить процент порчи грузов.

Обеспечение безопасности и отслеживания контейнерных перевозок — в данном случае транспортные контейнеры могут быть снабжены устройствами типа «электронная пломба», датчиками открытия контейнера, отказа климатического оборудования и спутниковыми системами геолокации объекта транспортировки. В отдельных случаях возможно использование технологии триангуляции по сотовым вышкам мобильных операторов с целью определения местоположения.

В число задач IIoT может входить обеспечение контроля транспортных средств и маршрутов следования водителей при транспортировке грузов. Технология позволяет обеспечить контроль расхода горюче-смазочных материалов, а также режима работы водителей (количество и место остановок для отдыха и сна, время, проведенное за рулем, соблюдение правил дорожного движения и скоростного режима, корректность выбранного маршрута следования и прочие факторы).

Интеллектуальная транспортная инфраструктура

В состав умного города входит интеллектуальная транспортная инфраструктура (ИТС), которая, в свою очередь, сопрягается с подсистемами умного транспорта.

Основной целью ИТС является сбор данных о дорожной ситуации, ее анализ и прогнозирование ситуации в будущем. Например, в Москве по разным подсчетам более двух тысяч светофоров, трех с половиной тысяч установок мониторинга дорожного движения и двух тысяч камер видеонаблюдения. С целью обработки и

анализа данных, поступающих с данных устройств в реальном времени, был создан ситуационный центр обеспечения дорожного движения (ЦОДД). На основе данных ЦОДД в дальнейшем упрощается планирование и регулирование дорожного движения, планирование маршрутов следования общественного транспорта. По данным портала mos.ru на текущий момент, благодаря использованию интеллектуальных транспортных систем, сообщается о повышении средней скорости движения транспорта в городе на 13% при сохранении роста числа машин. Для водителей уже не в новинку наблюдать электронные табло на главных трассах города, сообщающие водителям «оперативные данные» о погоде, расчетном времени в пути до ключевых объектов инфраструктуры города (к примеру, ТТК, СВХ, МКАД и пр.), а также о степени загруженности дороги на текущем участке, что сильно способствует снижению уровня аварийности на дорогах. Для тех, кто пользуется общественным транспортом, такие табло представлены на автобусных остановках, сообщая пассажирам об ориентировочном времени прибытия автобуса, работающих на данной остановке маршрутах и пр.

Частью ИТС также являются умные дороги, в состав которых включены решения для сбора и обработки данных о транспортных средствах и дорожной инфраструктуре с целью принятия решений, включая:

- детекторы транспортного потока;
- адаптивные (умные) светофоры;
- системы автоматизированного управления освещением;
- средства автоматической фиксации нарушений правил дорожного движения;
- электронные средства безостановочной оплаты проезда;
- паркоматы;
- подключенные информационные табло.

Системы безопасности и видеоаналитика

Видеоаналитика и системы обеспечения безопасности и правопорядка наряду со здравоохранением являются одним из ключевых приоритетов умного города. В данном контексте речь идет как о личной безопасности граждан, так и жилых объектов и бизнеса. Системы ориентированы в первую очередь на предотвращение потенциальных угроз и планирование защитных мер. К примеру, Москва обладает покрытием из 160 тысяч камер, расположенных как в жилом секторе (дворы жилых домов, подъезды), так и в местах массового скопления людей и критически важных инфраструктурных объектах города. Но сама по себе обширная сеть камер видеонаблюдения не способна обеспечить требуемый уровень безопасности. Ключевую роль в процессе играет видеоаналитика.

Видеоаналитика — аппаратно-программное обеспечение или технология, использующая методы компьютерного зрения для автоматизированного сбора данных на основании анализа потокового видео (видеоанализа). Видеоаналитика опирается на алгоритмы обработки изображения и распознавания образов, позволяющие анализировать видео без прямого участия человека. Она используется в составе интеллектуальных систем видеонаблюдения (CCTV, охранного телевидения), управления бизнесом и видеопоиска.

Использование видеоаналитики позволяет автоматизировать следующие ключевые задачи обеспечения безопасности:

- Обнаружение объектов в поле зрения камеры производится при помощи видеодетектора движения. В зависимости от реализации системы, может присутствовать возможность выделения, ведения с учетом траектории перемещения и независимого анализа нескольких объектов одновременно. Обнаружение может производиться при помощи шаблонов; примерами таких шаблонов может служить обнаружение лиц людей или номерных знаков автомобилей.
- Слежение за объектами. Алгоритмы слежения позволяют получить как траекторию движения объекта в поле зрения одной камеры, так и обобщённую траекторию по данным сразу нескольких камер.
- Идентификация объектов. Позволяет идентифицировать людей по биометрическим признакам лица или транспортное средство – по номерным знакам.
- Обнаружение нештатных ситуаций. Видеоаналитика позволяет не только выделять объекты из потокового видео, но и распознавать тревожные ситуации на основе анализа поведения конкретного объекта. Также ситуационная видеоаналитика может автоматически обнаруживать пересечение сигнальной линии, падение людей, запрещенную парковку, возникновение пожара, потасовки, большое скопление людей.
- Прогнозирование поведения объекта наблюдения или возникновение ситуации.

Медицина

Перспективное направление развитие технологий IoT — применение IoT в медицине. Здесь необходимо различать два класса устройств:

1. Бытовые устройства, в основном обеспечивают диагностику и мониторинг.

2. Профессиональное медицинское оборудование, которое, в свою очередь, можно разделить на два подкласса:

- пассивное — для диагностики и мониторинга;
- активное, которое с помощью исполнительных механизмов производит манипуляции с телом человека (важно отметить: в акцептном и безакцептном порядке).

Благодаря IoT-устройствам, обеспечивающим возможность удаленного слежения за состоянием и жизненными показателями пациента, возрастает шанс на оперативное и своевременное предоставление скорой медицинской помощи. Благодаря носимым пациентом устройствам, способных передавать уведомление медицинским службам, снижается процент смертности из-за неоказания своевременной медицинской помощи, а также обеспечивается возможность самодиагностики текущего состояния пациента. По мнению экспертов, со временем с данными системами будет также сопряжен искусственный интеллект — он сможет выступать в роли диагноста, что сократит время на постановку диагноза, а значит, позволит медицинскому персоналу максимально оперативно приступить к лечению и проводить его более эффективно.

В качестве бытовых медицинских IoT можно привести пример носимых трекеров, в состав которых могут входить различные датчики физической активности, термометры, пульсометры, тонометры, глюкометры и др., например:

мотоциклетный шлем, измеряющий активность головного мозга и качество реакции, устройство слежения за зрачками водителя и оценки его реакции при вождении. Бытовые медицинские IoT-устройства чаще всего вмонтированы в носимые трекеры, используют смартфоны для ретрансляции информации в соответствующие сервисы или ограничиваются её передачей на смартфон.

Профессиональное медицинское IoT-оборудование для диагностики и мониторинга принципиально мало чем отличается от носимых бытовых устройств, но оно однозначно отличается качеством сенсоров и стоимостью приборов. К такому классу оборудования можно отнести, например, IoT-холтеры — приборы, непрерывно снимающие ЭКГ, давление и другие параметры, капсулы для гастроскопии. Такие IoT-устройства имеют собственный канал связи с целевой IoT-платформой сбора и обработки информации.

Профессиональное медицинское IoT-оборудование может применяться и для манипуляций с телом человека. Например, носимые IoT-устройства могут по расписанию или по состоянию вводить лекарства в организм, например, инсулин диабетикам или адреналин военным при получении ранения. Такие IoT-устройства могут быть встроены, скажем, в униформу военного, пожарного, в бронежилет полицейского.

К классу IoT можно отнести не только мобильные медицинские устройства. Существует масса примеров стационарного оборудования, которое можно отнести к данной категории. Профессиональное медицинское оборудование, применяемое для диагностики и манипуляций, в XXI веке сопряжено с сетью и позволяет решать массу полезных задач:

- возможность мониторинга состояния пациента профильным специалистом из любой точки мира;
- возможность проведения манипуляций в удалённом режиме профильным специалистом — одним или несколькими;
- мониторинг и диагностики самого оборудования для своевременного технического обслуживания и ремонта.

Самым современным медицинским устройством на сегодняшний день является медицинский робот-хирург Da Vinci, который позволяет профильному хирургу проводить операции пациенту, находящемуся на другом конце света, а в будущем, вероятно, «дотянется» и до космических станций.

Ближайшее будущее медицинских IoT заключается в роботизации клиник, повышении автономности пациентов, которым необходим мониторинг и своевременные манипуляции. Позже появятся наноботы и их группы для манипуляций с организмом человека, которые будут подчинены «роевому» принципу управления.

Важнейший драйвер роста IoT-устройств в медицине — это совершенствование методов диагностики, выявление заболеваний на ранней стадии и общее повышения знаний о теле человека. Этому будут способствовать методы сбора и обработки больших данных, машинное обучение и искусственный интеллект.

Следует отметить, что тема кибербезопасности медицинских IoT-устройств и платформ является важнейшим вопросом и камнем преткновения.

По прогнозам исследователей (компания Allied Market Research), рынок медицинских IoT-гаджетов и IoT-приложений до 2021 года вырастет до $140 млрд.

Военное применение

Применение IoT в армии исторически является классической задачей Автоматизированных Систем Управления Войсками (АСУВ), таких как, например, Единая Система Управления Тактическим Звеном (ЕСУ ТЗ).

Задача ЕСУ ТЗ определяется по классической схеме: необходимо связать воедино большой набор децентрализованных автономных систем, обеспечить слаженность работы системы в целом, её безопасность и целостность, увязать воедино всех разработчиков различного вида оборудования и контроллеров, определить протоколы связи и обеспечить их сопряжение с единой децентрализованной системой, обеспечить прозрачный контроль выполнения команд и задач в рамках функционирования системы в боевом режиме. Современные АСУВ типа «Акация» и «Заря-22» («Заря-21») — чем не IoT? Удивительно, но в индустрии до сих пор не принят термин Military IoT (MIoT).

В целом, все АСУВ движутся в сторону повышения автономности РСУ (DCS), повсеместно внедряются технологии автономных интеллектуальных исполнительных устройств и датчиков (IoT, IIoT), искусственного интеллекта и машинного обучения, технологии дополненной и виртуальной реальности (AR, VR), технологии анализа неструктурированных данных (Big Data), технологии надёжных распределённых архивов (Block Chain). Некоторые функции АСУВ выносятся в облачные сервисы, в том числе локальные частные облака, распределённые мобильные ЦОД, в которых они размещаются.

Современный российский комплект снаряжения «Ратник 3.0» представляет собой целую сеть MIoT устройств: контроллер экзоскелета, шлем дополненной реальности, средства связи с высокой криптостойкостью, средства позиционирования, набор медицинских IoT для контроля состояния военнослужащего — и это не считая интеллектуального оружия.

Концепция армии США Future Combat Systems (FCS) также полностью включает весь приведённый стек технологий. Американская компания Nutanix, создающая технологии гражданской виртуализации для ЦОД, создала для вооружённых сил США мобильный ЦОД для построения локальных частных облаков прямо на поле боя, тактический дата-центр, фактически десантируемый облачный ЦОД в рамках проекта Deployable Joint Command and Control System.

В военной технике отрабатываются передовые средства связи: например, уже сейчас проектируются и испытываются средства беспроводной связи 6-го поколения. Именно военные определяют будущее гражданских технологий, лишь на военные бюджеты можно отработать и отладить технологии до их коммерческого применения.

В армии уже давно эксплуатируются сложнейшие MIoT — не только с удалённым управлением средствами разминирования, наземным транспортом

доставки боеприпасов, различными роботизированными комплексами, но и полностью автономные летающие дроны со сверх- и гиперзвуковыми скоростями, с оффлайн-средствами идентификации и распознавания цели, а также алгоритмами на базе ИИ для принятия решения о её поражении.

Именно в армии впервые появились полноценные работающие Mesh-сети, позволяющие строить системы управления «роем» (вооружения), именно эти технологии в дальнейшем определят стандарты управления «роем» автомобилей и других подвижных устройств на дорогах общего пользования, а также иных автономных роботизированных комплексов в любой среде эксплуатации.

Армия — сильнейший драйвер развития технологий IoT. И не забывайте, многие IoT могут по запросу мгновенно превратиться в MIoT.

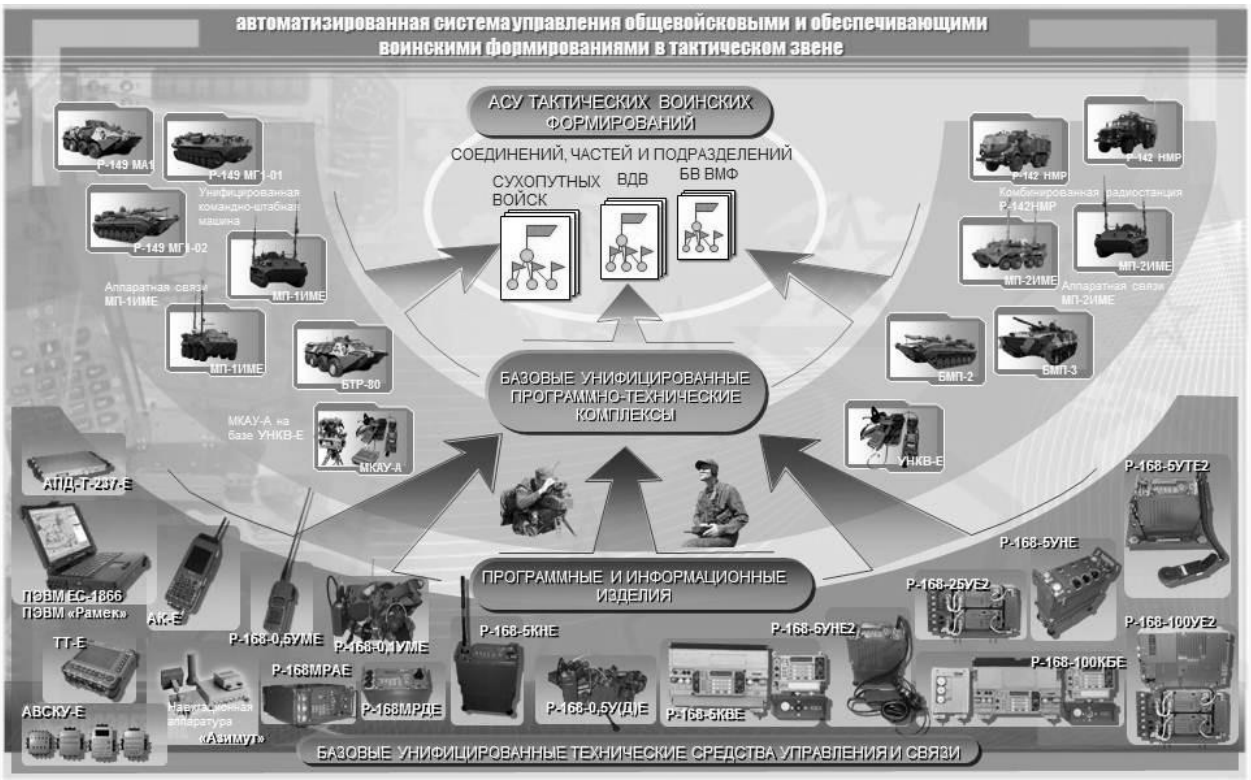

Рис. 6.2.7. Российская АСУВ.

Телеком

Операторы связи становятся операторами трафика с IoT-устройств. Существуют операторы, давно принявшие обслуживание трафика с подключенных устройств IoT, как часть портфеля услуг (раньше некоторые операторы указывали эту услугу как M2M). Возможно, в скором времени на рынке IoT телеком-услуг появятся отраслевые виртуальные операторы (Mobile Virtual Network Operator, MVNO).

Многие телеком-операторы располагают серьёзными мощными ЦОД, на базе которых развёртываются отраслевые сервисные платформы (в том числе и IoT-платформы) для предоставления сервисного обслуживания потребителям соответствующих услуг. Также телеком-операторы выстраивают бизнес на основе

агрегации сервисных услуг платформ, предоставляемых внешними ЦОД и провайдерами услуг.

Телеком-услуги разделяются на два типа: передача данных по каналам связи и предоставление по этим каналам связи доступа к сервисным услугам. В последнее время операторы начинают предоставлять пакетные услуги (для конечных потребителей, бизнеса, государственных учреждений), в состав которых входят необходимые сервисы и службы, включая модели обслуживания IoT-устройств.

В России лидером данного направлении является компания «Ростелеком» в связке с «большой тройкой» операторов мобильной связи (МТС, Мегафон, Билайн). В США, Европе таким лидером является Amazon в связке с локальными операторами мобильной связи.

Рис. 6.2.8. Десантируемый облачный ЦОД Nutanix.

Платформы IoT

Платформа — это набор технологий, которые определяют реализацию задач части или всего жизненного цикла изделия (продукции, решения). Платформа может решать как задачи проектирования (разработки, design time), так и задачи выполнения (эксплуатации, runtime).

Чем сложнее система (большее число узлов, компонентов, соединений — и большее их разнообразие), тем тяжелее проектировать и эксплуатировать такую систему; необходимо следить за актуальной версией прошивки (ОС, ПО) на каждом конечном устройстве системы в целом. Современные технологии позволяют эффективно решать данные вопросы.

Значимые платформы IoT

Крупные интернет-гиганты создают программные технологические IoT-платформы, среди которых нужно отметить следующие:

- AWS IoT;

- Microsoft Azure IoT;
- Google Cloud Platform;
- SAP Leonardo IoT Platform;
- Oracle Integrated Cloud;
- IBM Watson IoT Platform.

Производители аппаратных компонентов и устройств не отстают и создают свои IoT-платформы, например, интересно выделить следующие:

- Cisco IoT Cloud Connect;
- HPE Universal of Things (IoT) Platform;
- Siemens Mindsphere;
- Bosch IoT Suite;
- General Electric’s Predix.

Следует отметить также следующие разработки с открытым исходным кодом:

- Kaa IoT platform;
- IoTivity;
- ThingsBoard IoT Platform.

Кибербезопасность IoT

Одной из важнейших задач в области IoT является обеспечение информационной безопасности. Появляются абсолютно новые модели угроз, и обеспечивать кибербезопасность необходимо на каждом из этапов жизненного цикла IoT-решения.

В современном мире, где уже появилось множество примеров применения IoT, требуется обеспечивать защиту:

- сетей связи;
- конечных устройств (стационарных и мобильных);
- узлов сопряжения, граничных и периферийных узлов;
- серверных узлов.

С точки зрения ПО, необходимо обеспечивать защиту широкого класса:

- ОС и прошивок IoT, конечных устройств, серверов и др.;
- платформ виртуализации и облачных платформ;
- виртуальных сетей, виртуальных ЦОД и платформ их организации;
- платформ хранения данных;
- платформ сопряжения, обработки и предоставления интерфейсов доступа к данным.

Подробнее о способах и инструментах обеспечения информационной безопасности смотрите в разделе Учебника «Информационная безопасность».

Интернет всего (IoE)

Цифровизация шагает по планете и охватывает всё новые и новые отрасли и сферы. Устройства наравне с людьми становятся потребителями связи, данных, вычислительных ресурсов. Обычный «Интернет людей» сопрягается с «Интернетом вещей» и становится единой сетью сопряжения, которую стали называть «Интернетом всего» (Internet of Everything, IoE).

В какой-то момент платформы и сервисы перестанут отличать потребителей-людей от машин. Глобальный океан данных позволит любому участнику сети воспользоваться теми или иными данными для решения поставленных задач. Такая доступность данных и вычислительных ресурсов приведёт к существенному ускорению глобализации.

Тотальная автоматизация и доступность вещей в сети является существенным драйвером глобализации человечества. Тотально контролируемые вещи должны сообщать и о неисправностях в самих вещах, и о «неисправностях» в теле человека и его действиях. В числе прочего они могут обеспечивать повышение эффективности их применения — и бережливого отношения к ним.