ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Лекция 4. Туманные вычисления и Интернет вещей

Курс лекций

Концепция туманных вычислений

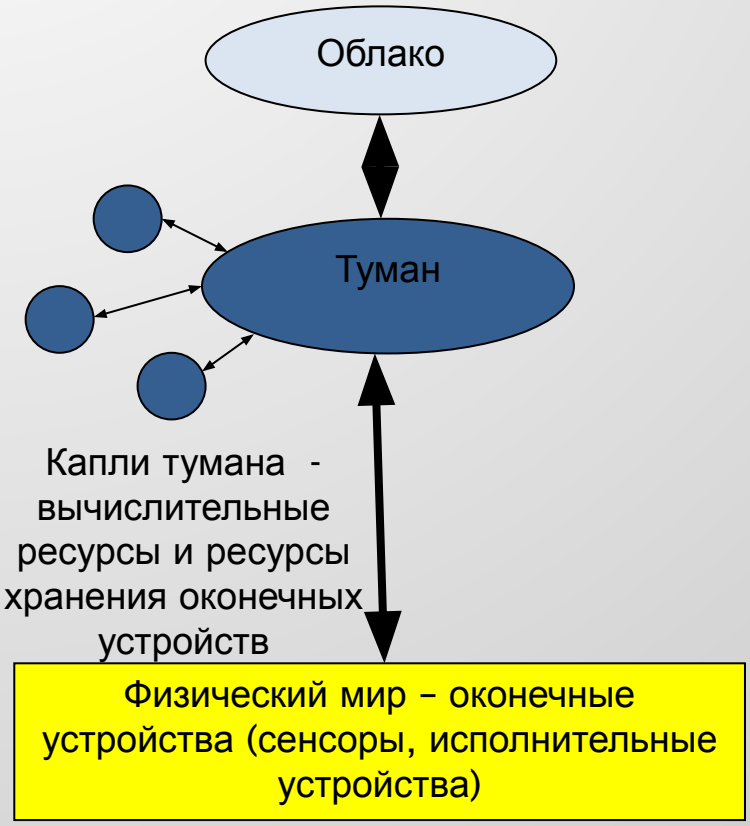
Термин Fog Computing («туманные вычисления») был введен в оборот вице-президентом компании Cisco Флавио Бономи в 2011 году. Он предложил концепцию туманных вычислений по аналогии с облачными вычислениями, как расширение «облака» до границ сети (конечных устройств). Таким образом, отличительная черта Fog Computing - приближенность к конечным пользователям и поддержка их мобильности.

Развитие новых интернет-технологий, в частности, интернета вещей потребовало поддержки мобильности устройств конечных устройств для различных местоположений с геолокацией и с небольшой задержкой на обработку данных. Поэтому была предложена новая платформа для удовлетворения таких требований, которая и получила название «туманные вычисления». Её основной особенностью является обработка данных в непосредственной близости от источников их получения, без необходимости их передачи в крупные центры обработки данных (ЦОД) только для того, чтобы их там обработать и передать назад результаты.

Что такое туманные вычисления?

Таким образом, туман – это облако, опустившееся на землю. Это понятие, обозначает связанные между собой распределенные вычисления, частично выполняемые на оконечных устройствах (сенсорах и исполнительных устройствах), имеющих ограниченные ресурсы и непосредственную связь, как с физическим миром («землей»), так и с облаком. Возникновение технологии обусловлено современной тенденцией интеграции сетевых технологий во все большее число оконечных устройств, обладающих собственными вычислительными ресурсами и системами хранения данных (СХД). Эти устройства можно считать «каплями» тумана, опустившегося на «землю», т.е. приблизившегося к физическому миру облака.

Как функционирует технология туманных вычислений?



Технология туманных вычислений подразумевает предоставление доступа к оконечным устройствам и выполнение на них части вычислений, а также хранения на них части используемой информации, отправляя в облако информацию, подвергшуюся первичной обработке, существенно меньшего объема. Дальнейшая обработка информации, требующая существенно больших вычислительных мощностей, производится в облаке.

Туман и облако образуют распределенный ЦОД.

Реализация туманных вычислений

Необходимость фильтрации и предварительной обработки данных перед отправкой в облако потребовали, прежде всего приложения:

- требующие низкой и предсказуемой задержки передачи информации по сети, например, игровые приложения или видеоконференции.
- предназначенные для транспорта, такие как: беспилотные автомобили, скоростные поезда, интеллектуальные транспортные системы (ИТС) и др.
- требующие локальной обработки данных в реальном времени, такие как: интеллектуальные системы электроснабжения, ИТС, геофизическая разведка недр, управление трубопроводами, сенсорные сети мониторинга окружающей среды и пр.

«Туман» не является альтернативой «облаков». Напротив, он плодотворно взаимодействует с облаками, особенно в администрировании и аналитике данных, и такое взаимодействие порождает новый класс приложений.

Архитектура туманных вычислений представляет собой некую «прослойку» на границе между облаком и сенсорными, а также мобильными устройствами пользователей.

Отличие туманных вычислений от облачных

- обеспечение качества услуг (QoS, Quality of Service), что требует динамической адаптации приложений к состоянию сети.
- отслеживание местоположения для того, чтобы поддерживать стабильность работы приложения в условиях мобильности терминала.
- отслеживание контекстной информации, т.е. способность обнаруживать наличие доступных ресурсов поблизости, чтобы задействовать их в работе приложения, с возможностью горизонтального взаимодействия.

В «туманной» архитектуре сетевые узлы, расположенные ближе к облачным ЦОД, обладают большей вычислительной мощностью и бóльшим объемом данных в системах хранения. Сетевые узлы, расположенные ближе к сенсорам и мобильным устройствам, обладают большей интерактивностью и быстрым откликом.

Важной особенностью туманных технологий является то, что в качестве сетевого узла могут выступать устройства пользователя, такие как персональные компьютеры, телеприставки и мобильные устройства.

Особенности технологии туманных вычислений

- крайнее положение, осведомленность о своей позиции;
- малые задержки в сети;
- географическая распределенность;
- большое количество сенсоров и/или исполнительных устройств;
- большое количество узлов;
- поддержка мобильности, поддержка реального времени;
- возможность (и желательность) беспроводного взаимодействия;
- гетерогенность;
- возможность взаимодействия и объединения с другими типами сетей;
- поддержка вычислений на узлах и взаимодействие с облаком.

Сценарии использования

- **Автономные системы управления транспортом (ADS, Autonomous Driving System) -** используют различные многорежимные сенсоры, технологии компьютерного зрения и анализа изображений, спутниковое и сетевое позиционирование на картах; требуют высокого быстродействия и, соответственно, размещения «туманного» устройства непосредственно в транспортном средстве.
- **В медицине** системы применяются в тех случаях, когда необходимо произвести оперативный анализ полученных данных с носимых пациентом датчиков и предпринять немедленные действия в соответствии с планом лечения (сенсор на теле пациента определяет критическое значение содержания сахара в крови, и через «туманную» сеть выдает сигнал на выполнение инъекции при помощи микро-шприца).

В России технология используется в решениях «интеллектуальный карьер» компании «ВИСТ Майнинг Технолоджи» (добывающей компании).

Преимущества «туманных» вычислений и рынки

Преимущества «туманных» вычислений - снижение объема данных, передаваемых в облако, что уменьшает требования к пропускной способности сети, увеличивает скорость обработки данных и снижает задержки в принятии решений. Они решают проблемы:

- высокой задержки в сети;
- трудностей, связанных с подвижностью оконечных точек;
- потерей связи;
- высокой стоимости полосы пропускания;
- непредвиденных сетевых заторов;
- большой географической распределенности систем и клиентов.

Потенциальные рынки:

- энергетика;
- коммунальные услуги;
- здравоохранение;
- транспорт.

Перспективы туманных вычислений и «туман» в России

В ноябре 2015 года Cisco, Microsoft, Dell, ARM, Intel и Princeton University основали **OpenFog Consortsium** для создания открытой архитектуры, которая обеспечит масштабируемость и совместимость различных устройств.

Консорциум **OpenFog** выделил три особенности разработки структуры туманных вычислений:

- горизонтальная масштабируемость;
- возможность работы через облако;
- возможность представлять собой общесистемную технологию, простирающуюся от границ сети (оконечных устройств) до облака и различных сетевых протоколов.

В России в июне 2016 года по инициативе «Ростелекома» Администрация президента РФ поручила Минкомсвязи, Минпромторгу, «Ростелекому» и Агентству стратегических инициатив проработать внедрение "туманных вычислений" в экономику России, а также заняться подготовкой программно-аппаратных комплексов, необходимых для работы соответствующей инфраструктуры. Представить результаты выполнения поручения необходимо было уже в октябре того же года.

Интернет вещей. История

В 1926 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.

В 1990 выпускник MIT, один из отцов протокола TCP/IP, Джон Ромки создал первую в мире интернет-вещь. Он подключил к сети свой тостер.

Термин «Интернет вещей» (Internet of Things - **IoT**) предложен Кевином Эштоном в 1999 году. В этом же году был создан Центр автоматической идентификации (Auto-ID Center), занимающийся радиочастотной идентификацией и сенсорными технологиями, благодаря которому эта концепция получила широкое распространение.

В 2008-2009 произошел переход от «Интернета людей» к «Интернету вещей», т.е. количество подключенных к сети предметов превысило количество людей.

Что такое Интернет вещей?

Интернет вещей подразумевает, что человек определяет цель, а не задаёт программу по достижению этой цели. В идеале: система сама анализирует данные и предугадывает желания человека.

Главные особенности IoT:

- постоянное сопровождение повседневных действий человека;
- ориентация на результат;
- человек указывает на то, что должно получиться, а не как это сделать.

«Туманные» технологии тесно связаны с IoT, поскольку позволяют в этих ситуациях снизить интернет-трафик, производя первичную обработку данных в датчиках сенсорах и исполнительных устройствах.

Существуют разные определения IoT:

- это сеть сетей с уникально идентифицируемыми конечными точками, которые общаются между собой в двух направлениях по протоколам IP и обычно без человеческого вмешательства;
- это сеть физических объектов, которые имеют встроенные технологии, позволяющие осуществлять взаимодействие с внешней средой, передавать сведения о своем состоянии и принимать данные извне.

Примеры интернета вещей

- развитие концепции «умного дома», который способен при приближении владельца открывать двери, подогревать ужин, включать кондиционер, телевизор со сделанной предварительно записью, самостоятельно пополнять запасы холодильника и т.д.;
- с помощью подключенных датчиков станет возможным измерить загруженность транспортных каналов и оптимизировать их;
- классические магазины уже могут составить конкуренцию онлайн-ритейлерам, предложив уникальный, персонализированный и привлекательный сервис своим клиентам;
- посмотреть на данные аэрофотосъемки лесного массива, оценить запасы, проконсультироваться с экспертом, продать лес и заказать услуги по высаживанию или рубке растений.

Какие из информационных технологий необходимы для развития Интернета вещей?

Таких технологий три. Это средства:

- идентификации при подключении к Интернету вещей с помощью идентификаторов, например, штрих-кодов или QR-кодов (quick respond code – кодов быстрого распознавания);
- измерения, что требует высокой автономности датчиков, т.е. понижения их энергопотребления и повышения емкости аккумуляторов; желательно иметь полностью автономные датчики;
- передачи данных, для чего необходим единый стандарт (в настоящее время наиболее широко используется стандарт IEEE 802.15.4);

Необходимо также решить проблемы разработки:

- единого языка, на котором смогут общаться между собой подключенные датчики, сенсоры и приборы;
- единых стандартов в области всего Интернета вещей, а не только в области передачи данных;
- защиты информации («умные тапочки» не должны быть болтливыми).

Принципы обеспечения безопасности пользователя

Безопасность связи: для обеспечения безопасности необходимо использовать защищенный канал связи. Благодаря криптографии в настоящее время эффективное шифрование и проверка подлинности различных устройств IoT происходит даже в устройствах малой мощности.

Защита устройств: криптографический код должен включать его безопасность и целостность. Подписанный криптографически код гарантирует, что он не был изменен после подписания и безопасен для запуска; также все критически важные датчики должны иметь возможность запускать только надежный, проверенный, криптографически подписанный код.

Контроль устройств: со временем происходит обнаружение новых уязвимостей, и их необходимо устранять, хотя не всегда есть возможность физического доступа к устройству; но всегда необходимы своевременные обновления для обеспечения безопасности.

Контроль взаимодействий в сети: важно иметь системы анализа безопасности, которые могут своевременно заметить подозрительные и, возможно, критичные для устройства аномалии, а также зафиксировать их и передать информацию.

Информационная безопасность и IoT

Специалисты HP выделяют следующие проблемы информационной безопасности (ИБ) при использовании IoT:

- пользователи в начале эксплуатации не заменяют фабричный пароль, установленный по умолчанию, на свой личный;
- не все приборы имеют встроенные средства ИБ, поэтому следует установить внешнюю защиту, предназначенную для домашнего использования, с тем чтобы интернет-устройства не стали открытыми шлюзами в домашнюю сеть или прямыми инструментами причинения ущерба;
- в большинстве устройств не шифруется беспроводной трафик;
- 90% устройств собирают ту или иную персональную информацию о владельце без его ведома.

Специалисты HP насчитали около 25 различных уязвимостей в каждом из исследованных устройств (телевизоров, дверных замков, бытовых весов, домашних охранных систем, электророзетки т.д.) и их мобильных и облачных компонентах.

Вывод экспертов: безопасной системы IoT на сегодняшний день не существует. Особую опасность вещи Интернета таят при целевых атаках.

Слабые места IoT

- питание датчиков;
- стандартизация архитектуры и протоколов, сертификация устройств;
- информационная безопасность;
- стандартные учётные записи от производителя, слабая аутентификация;
- отсутствие поддержки со стороны производителей для устранения уязвимостей;
- трудность или невозможность обновления ПО и ОС;
- использование текстовых протоколов и ненужных открытых портов;
- слабость отдельных гаджетов, через которые хакеру легко попасть во всю сеть;
- использование незащищённых мобильных технологий;
- использование незащищённой облачной инфраструктуры;
- использование небезопасного ПО.

Способы и возможности доступа к потребителю IoT:

- изменение заказа (заказ 53 литра молока) или заказ кофе без кофеина;
- создание ложной тревоги (вызов пожарных);
- возможность запереть в доме с требованием выкупа;
- возможность отключения сигнализации перед взломом;
- возможность получения персональных данных, в том числе, при их публикации в социальных сетях;
- блокировка доступа к машине, используя доступ к ней через интернет;
- доступ к банковским счетам;
- уязвимости в бытовом устройстве (например, в пылесосе) могут привести к проблемам, например, к пожару в доме.

Безопасность IoT

- умные замки легко можно взломать, в результате чего они не могут гарантировать выполнение своей основной функции, для которой, собственно говоря, они и существуют; существующие системы достаточно просты для кибер-хакеров и не являются препятствием для того, чтобы проникнуть в дом;
- возможность получать информацию (и использовать ее в дальнейшей работе) от других смарт-устройств, что позволяет системе реагировать соответствующим образом в случае опасности, и, в свою очередь, позволяет домашней системе, которая обнаружила пожар, разблокировать все двери в доме, чтобы помочь выбраться из него как можно быстрее;
- IoT-устройства предоставляют хакерам доступ к потенциально взрывоопасным устройствам, например, к смартфонам, пылесосам и т.д.;
- DDoS-атаки (отказ в обслуживании) - хакеры могут попытаться отключить как можно больше машин чтобы они работали неправильно;
- смарт-устройства становятся все умнее, т.е. хакер может получить доступ к банковским данным пользователя или вмешаться в его покупки.

Промышленный Интернет вещей (IIoT)

Промышленный Интернет Вещей (Industrial Internet of Things, IIoT) – или интернет вещей для корпоративного/отраслевого применения - система объединенных компьютерных сетей и подключенных производственных объектов со встроенными датчиками и ПО для сбора и обмена данными, с возможностью удаленного контроля и управления в автоматизированном режиме, без участия человека.

Ключевой драйвер реализации концепции IIoT - возможность повышения эффективности производственных и технологических процессов, на фоне сокращения капитальных затрат. Технологии позволяют предприятиям сокращать простои (до 10%), снижать затраты на техническое обслуживание, а также усовершенствовать процедуры прогнозирования и предотвращения отказов оборудования (на 10%). Все это способствует повышению производительности труда и росту ВВП. «Ростелеком»» подсчитал, что к 2020-2021гг. эффект от внедрения интернета вещей в реальном секторе экономики может составить до 0,8-1,4 трлн. руб., благодаря повышению производительности труда на 10-25% и уменьшению расходов на 10-20%. Основными отраслями, где будет формироваться выручка, станут транспорт, промышленность, ЖКХ, здравоохранение, а также сегмент умных зданий и умных городов.

Перспективные способы применения IIoT на промышленных предприятиях

Сквозная автоматизация**:** позволяет оперативно реализовывать сложные сквозные, полностью автоматизированные бизнес-процессы, которые охватывают различные АСУ предприятия.

Удаленный мониторинг и предикативная диагностика: применение датчиков контроля работы оборудования с выходом в сеть позволяет производителю вести удаленный мониторинг и своевременно проводить регламентные работы, предсказывать аварии или заранее готовить необходимые детали на замену и т. п. Знание о фактической и планируемой загрузке производственного оборудования, позволяет организовать автоматическую сеть заказов между различными производствами от поставщиков материалов до потребителей конечной продукции.

Новые сервисные бизнес-модели: Продажа услуги «по требованию» – ключевая характеристика облачной модели. IIoT позволяет запустить переход от модели продажи устройств, измеряемых количеством поставленного оборудования, к модели продажи функционала оборудования «по требованию», когда оборудование не передается в собственность заказчика, а оплачивается им по факту использования его функций. По такому принципу работают, например, крупнейший поставщик промышленных компрессоров Kaeser.

IIoT в России

На российском рынке выделяются следующие направления для применения IIoT:

1. Управление производством – для удаленного анализа состояния производственного оборудования, осуществления контроля и управления производственными операциями, проведения диагностики для предотвращения неполадок.

2. Мониторинг транспорта – для создания систем, осуществляющих мониторинг местоположения, маршрутов, условий перевозки грузов в режиме реального времени с помощью беспроводных, спутниковых или других каналов связи.

3. Интеллектуальные энергосистемы – для повышения эффективности, безопасности и надежности энергоснабжения, построенные на принципах активного децентрализованного взаимодействия между различными элементами сети в режиме реального времени.

Наибольшее распространение до недавнего времени в России получило внедрении мониторинга транспорта, однако сегодня формируется устойчивый интерес и к системам предупредительной диагностики технического состояния оборудования.

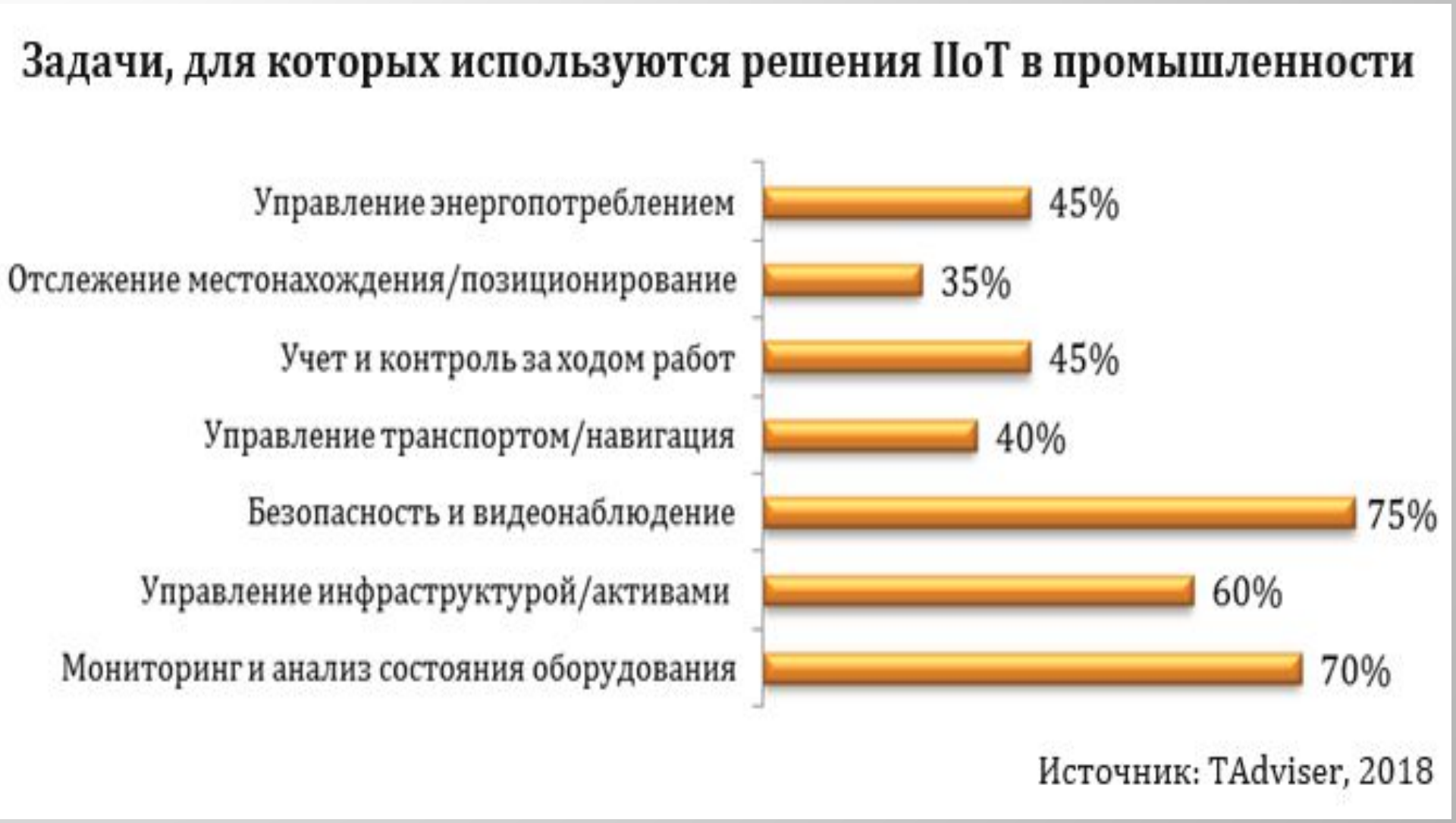
IIoT в России

Самыми популярными на российских промышленных предприятиях становятся устройств IIoT, которые занимаются автоматизированным сбором данных. В «Концерне Росэнергоатом» на блоках 1 и 2 Смоленской АЭС за последние два года модернизирована функция эксплуатации оборудования.

Завод радиоэлектронной продукции «Технинжиниринг» внедрил беспроводной контроль (разработчик – компания «СТРИЖ»), установив более 550 датчиков и устройств (электросчетчиков, датчиков протечки, температуры, теплосчетчиков и пр.). За 4 месяца эксплуатации экономия на отоплении (за счет сокращения потерь тепла и более точного учета коммунальных ресурсов) составила 48%.

General Electric подписала с «Роснефтью» соглашение о создании совместного предприятия, ориентированного на внедрение промышленного интернета. Ожидается, что внедрение цифровых решений позволит оптимизировать системы сбора, обработки и анализа промышленных данных «от скважины до пистолета на АЗС». Можно будет точнее прогнозировать техническое состояние оборудования предприятий, предотвращать нештатные ситуации и снижать риски незапланированного простоя производственных объектов.

Использование IIoT



Что можно ожидать в будущем?

Есть мнение, что Интернет вещей будет решать 3 самостоятельные задачи:

- идентификацию каждого объекта из окружения пользователя;
- предоставление сервиса по обеспечению потребностей пользователя по примеру системы «умный дом»;
- сбор и обработку информации, организацию процессов и управление обществом на основе полученных сведений (пример - автоматическое регулирование дорожного движения на основе анализа трафика – одна из реализаций концепции «умного города»).

В дальнейшем можно ожидать переход от города в масштаб планеты, организация глобальной «сети сетей» и создание «Интернета всего» или «Всеобъемлющего интернета», который позволит подключить к всемирной сети буквально все, что только возможно.

Фантастика? Возможно, но еще несколько десятилетий назад интернета не было. Даже междугородная телефонная связь работала плохо, а обычная почта шла неделями.