

## ИНТЕРНЕТ ВЕЩЕЙ Рубашенков А.М.<sup>1</sup>, Бобров А.В.<sup>2</sup>

<sup>1</sup>Рубашенков Антон Михайлович – студент;

<sup>2</sup>Бобров Андрей Виорелович – студент,  
кафедра защиты информации,

Институт комплексной безопасности и специального приборостроения,  
Московский технологический университет,  
г. Москва

**Аннотация:** интернет вещей — это термин, обозначающий миллиарды электронных устройств, которые теперь могут подключаться к сетям передачи данных и к Интернету.

Пятьдесят миллиардов объектов обеспечивают триллионы гигабайт данных. Существует ли способ их объединения в целях оптимизации процессов принятия решений и взаимодействия и, как следствие, усовершенствования нашего образа жизни и нашей деятельности? Ответ на этот вопрос кроется в сетях, которые мы используем ежедневно.

**Ключевые слова:** интернет вещей, сети, вещь, туманные вычисления, информационная безопасность.

### Объединенная сеть и вещи

Согласно оценкам Cisco, 99 % вещей в физическом мире в настоящее время не подключены к сетям. Поэтому по мере подключения все большего и большего числа не подключенных на сегодня устройств будет происходить бурный рост Интернета вещей.

На сегодняшний день много вещей подключены с помощью слабо связанных между собой независимых сетей, предназначенных для конкретных целей. Например, в современных автомобилях задействовано множество собственных сетей, предназначенных для контроля работы двигателя, функций безопасности и систем коммуникации. Само по себе объединение этих систем в единую сеть могло бы облегчить конструкцию более чем на 23 кг кабеля в современном полноразмерном седане. В качестве другого примера можно привести коммерческие и жилые здания, в которых функционируют отдельные системы и сети для управления отоплением, вентиляцией, кондиционированием воздуха (ОВК, англ. HVAC), освещением; для телефонной связи и для охранных систем.

Эти разнородные сети объединяются, чтобы совместно использовать одну и ту же инфраструктуру. Эта инфраструктура включает комплексные функции обеспечения информационной безопасности, аналитики и управления. Подключение компонентов в конвергентную сеть, использующую технологии Интернета вещей, увеличивает потенциал сетей по улучшению повседневной жизни человека.

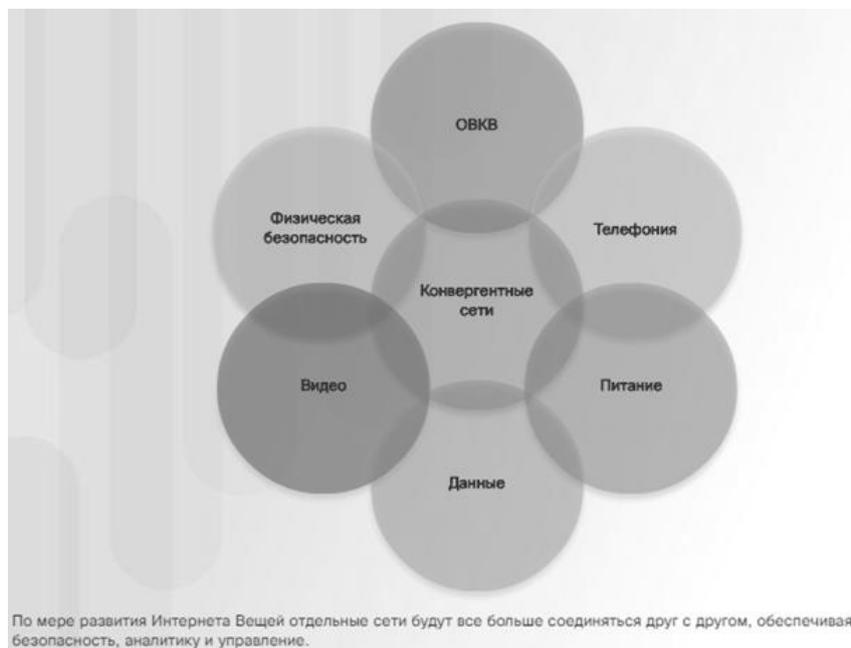


Рис. 1. Объединение разнородных сетей

### Проблемы и сложности при подключении вещей

Интернет вещей подключает интеллектуальные объекты к Интернету. Он соединяет как традиционные компьютерные устройства, так и необычные устройства. В Интернете вещей обмен

данными происходит в формате межмашинного обмена информацией, то есть возможно взаимодействие между машинами без участия человека. Например, межмашинный обмен информацией происходит в автомобилях, когда датчики температуры и давления масла передают информацию бортовому компьютеру.

Цифровое преобразование — это обеспечение связи как предметов, так и людей между собой, а также интерпретация данных осмысленным и защищенным образом.

#### **Компонент сетевого подключения**

Существует много различных типов сетей: домашние сети, общедоступные сети Wi-Fi, бизнес-сети малых предприятий, корпоративные сети, сети поставщика услуг, сети в центрах обработки данных, облачные сети и сети Интернета вещей (IoT). Независимо от типа в каждой сети, требуется оборудование, обеспечивающее сетевые подключения. В то же время виды используемого сетевого оборудования зависят от типа сети. Например, домашняя сеть обычно содержит широкополосный маршрутизатор беспроводной связи, в то время как в сетях предприятий содержатся коммутаторы, точки доступа, один или несколько межсетевых экранов, маршрутизаторы и т. д.

Компонент сетевого подключения в Интернете вещей Cisco определяет устройства, которые могут использоваться для обеспечения сетевых подключений Интернета вещей во многих различных отраслях и вариантах прикладного применения.

При использовании цифрового потолка Cisco сеть может осуществлять управление освещением и температурой области согласно предпочтениям находящихся в помещениях людей.

#### **Компонент туманных вычислений**

Модели сетей описывают схему передачи данных в сети. Модели сетей включают следующие:

Модель «клиент-сервер». Это самая распространенная из применяемых в сетях моделей. Клиентские устройства запрашивают предоставление услуг на серверах.



*Рис. 2. Модель «клиент-сервер»*

Модель облачных вычислений. Это более новая модель, в которой серверы и сервисы глобально рассеяны по распределенным центрам обработки данных. Облачные вычисления более подробно рассматриваются ниже в этой главе.

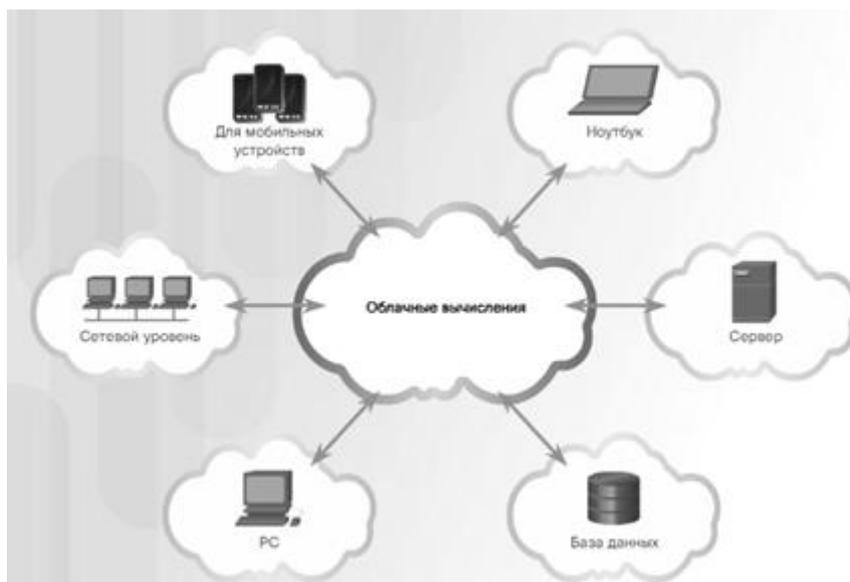


Рис. 3. Модель облачных вычислений

Туманные вычисления. Эта модель сети для Интернета вещей (IoT) определяет инфраструктуру распределенных вычислений, расположенную ближе к периметру сети. Она позволяет устройствам на периметре локально выполнять приложения и принимать немедленные решения. При этом уменьшается нагрузка по передаче данных в сети, поскольку необработанные данные не требуется передавать по сетевым соединениям; она улучшает отказоустойчивость за счет работы устройств Интернета Вещей во время потери сетевых подключений, а также повышает уровень безопасности, благодаря хранению чувствительных данных в пределах границы, где они необходимы. [3]

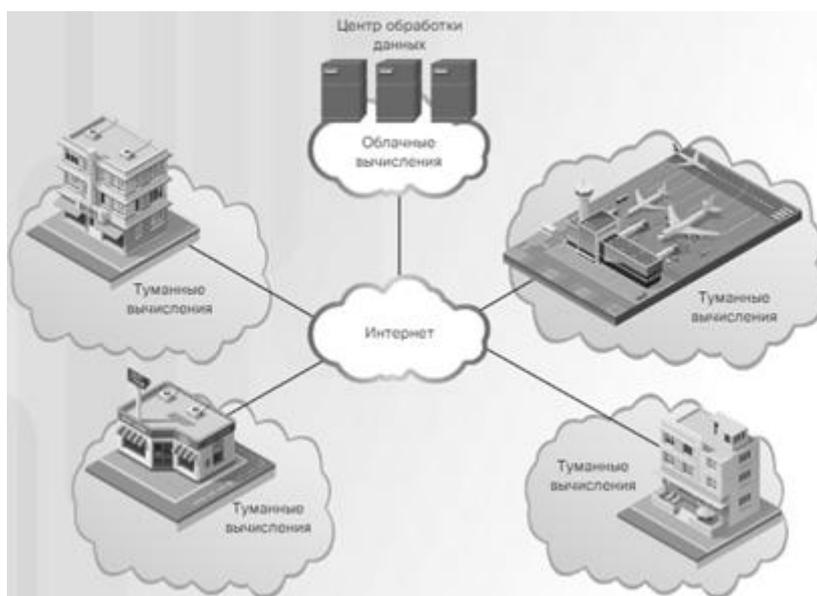


Рис. 4. Модель туманных вычислений

Эти модели не являются взаимоисключающими. Сетевые администраторы могут применять для удовлетворения потребностей пользователей сети все три названные модели в любых сочетаниях. Компонент туманных вычислений фактически распространяет облачную схему подключений ближе к периметру сети. Он обеспечивает для конечных устройств, таких как интеллектуальные счетчики, промышленные сенсоры, роботизированные станки и др., подключение к локальной интегрированной системе вычислений, сетевой связи и хранения данных.

Приложения, которые задействуют туманные вычисления, могут отслеживать и анализировать поступающие в реальном времени потоки данных от подключенных к сети вещей, а затем предпринимать действия, будь то запирание дверей, менять настройки оборудования, включать тормоза в железнодорожном составе и т. д. Например, светофор может локально взаимодействовать с рядом сенсоров, обнаруживающих присутствие пешеходов и велосипедистов, а также измеряющих расстояние

до приближающихся автомобилей и их скорость. Светофор также может взаимодействовать с соседними светофорами для координированной работы («зеленая волна»). Исходя из этой информации, светофор с интеллектуальной системой отправляет приближающимся машинам предупреждающие сигналы и изменяет собственный цикл работы, чтобы предотвратить аварии. Данные, собранные интеллектуальной системой управления светофорами, обрабатываются локально для выполнения анализа в реальном времени. Координация с соседними системами интеллектуальных светофоров в тумане позволяет изменять цикличность каждого из сигналов любым образом. Например, она может изменять продолжительность циклов светофора в зависимости от дорожных условий или закономерностей в характере дорожного движения. Данные из кластеров систем интеллектуальных светофоров отправляются в облако для анализа долгосрочных закономерностей дорожного движения.

Согласно прогнозам Cisco, 40 % формируемых в Интернете вещей данных к 2018 году будет обрабатываться в тумане.

#### **Компонент информационной безопасности**

Все сети нужно защищать. В то же время в Интернете вещей (IoT) появляются новые векторы атак, обычно отсутствующие в типичных корпоративных сетях. Компонент информационной безопасности в Интернете вещей Cisco представляет масштабируемые решения по кибербезопасности, позволяя организации быстро и эффективно выявлять и ограничивать атаки, противодействовать им, минимизируя ущерб.

Эти решения по кибербезопасности включают следующие:

Специфическая безопасность операционных технологий (OT) — под OT подразумеваются аппаратное и программное обеспечение, которые обеспечивают работу электростанций и управляют заводскими технологическими линиями. Сегмент информационной безопасности OT включает устройство промышленной безопасности ISA 3000 (рис. 1) и туманные службы данных.

Сетевая безопасность Интернета вещей — включает устройства обеспечения безопасности сети и периметра, такие как коммутаторы, маршрутизаторы, устройства межсетевых экранов ASA, а также сервисы предотвращения вторжений нового поколения (NGIPS) Cisco FirePOWER.

Физическая безопасность Интернета вещей (IoT) — IP-камеры для видеонаблюдения Cisco с широким набором функций обеспечивают видеонаблюдение в разнообразных средах. Они доступны в вариантах со стандартной и высокой четкостью изображения, в прямоугольных и купольных корпусах, с проводным и беспроводным подключением, в неподвижных версиях и версиях с поворотом, наклоном и увеличением (PTZ). Камеры поддерживают протоколы сжатия MPEG-4 и H.264, обеспечивающие эффективное использование полосы пропускания сети при высоком качестве изображения. [1]

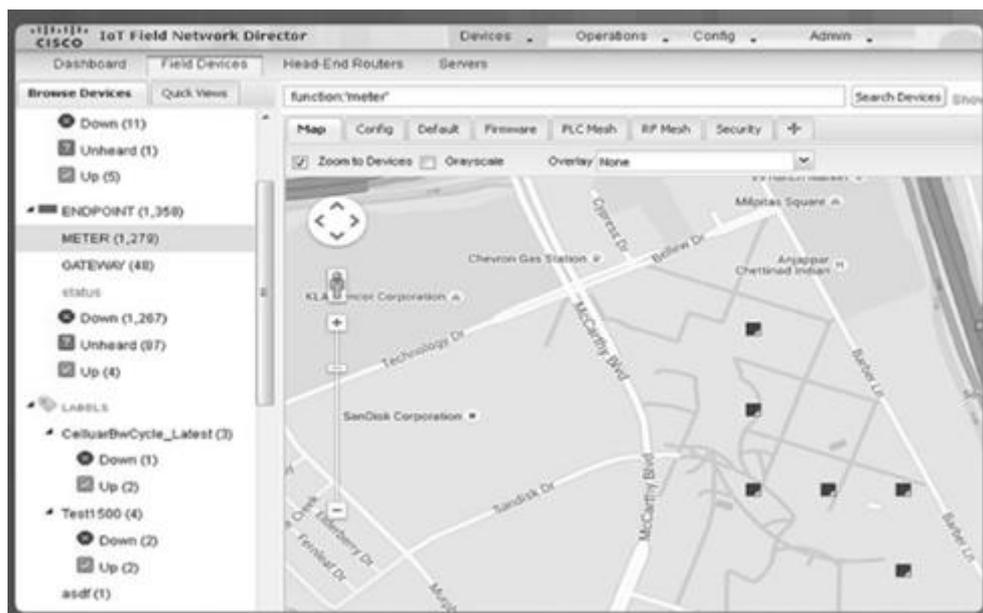
#### **Компонент аналитики данных**

Интернет вещей может соединять миллиарды устройств, способных генерировать целые эксабайты данных ежедневно. Чтобы получать реальную пользу, эти данные необходимо быстро обрабатывать и превращать в оперативную аналитику.

Инфраструктура аналитики Интернета вещей (IoT) Cisco состоит из компонентов распределенной сетевой инфраструктуры и специально предназначенных для Интернета вещей прикладных программных интерфейсов (API-интерфейсов).

#### **Компонент «Управление и автоматизация»**

Интернет вещей существенно увеличивает размер и разнообразие сети, в которую входят миллиарды интеллектуальных объектов: измеряющих, контролируемых, управляющих и реагирующих. Хотя объединение в сетях этих ранее неподключенных устройств может обеспечить непревзойденные уровни бизнес-аналитики и операционной аналитики, крайне важно учитывать, что операционные среды состоят из многочисленных разрозненных функциональных областей. У каждой из этих областей также имеются собственные требования, в том числе необходимость отслеживания определенных показателей. Системы операционных технологий могут существенно различаться как между отраслями, так и в рамках отдельной отрасли.



*Рис. 1. Базовый компонент «Управление и автоматизации»*

### **Компонент платформы поддержки приложений**

Компонент платформы поддержки приложений реализует инфраструктуру для размещения приложений и обеспечения мобильности приложений между средами облачных и туманных вычислений. Туманная среда обеспечивает работу многочисленных экземпляров приложения на различных оконечных устройствах и сенсорах. Эти экземпляры могут связываться между собой для обеспечения резервирования и общего доступа к данным, реализуя, например, такие бизнес-модели, как оплата по мере потребления для объектов, машин и продуктов. [2]

### **Заключение**

Интернет вещей означает миллиарды физических объектов, которые становятся доступными через Интернет по мере того, как мы подключаем к нему то, что раньше было неподключенным. Одна из проблем Интернета вещей — это безопасная интеграция в существующие сети новых объектов от различных поставщиков.

### **Список литературы**

1. Материал из Википедии — свободной энциклопедии. [Электронный ресурс]. Режим доступа: [https://ru.wikipedia.org/wiki/Интернет\\_вещей](https://ru.wikipedia.org/wiki/Интернет_вещей) (дата обращения 19.05.2018).
2. Материал с информационного форума habr. [Электронный ресурс]. Режим доступа: <https://habr.com/post/149593/> (дата обращения 25.05.2018).
3. Материал с информационного форума habr. [Электронный ресурс]. Режим доступа: <https://habr.com/post/259243/> (дата обращения 27.05.2018).