Веб Вещей и Интернет Вещей в цифровой экономике

В.П. Куприяновский, М.А. Шнепс-Шнеппе, Д.Е.Намиот, С.П.Селезнев, С.А.Синягов, Ю.В.Куприяновская

***Аннотация* – В статье рассмотрено место в цифровой экономике для таких направлений, как Интернет Вещей, Сети Вещей и Веб Вещей. Базой для этой статьи послужили исследования института стандартов NIST и консорциума W3C. В работе рассматриваются вопросы кибер-безопасности Интернета Вещей, международной стандартизации и программирования Интернета вещей. В разделе, посвященном стандартизации, рассматривается введенный NIST термин "сеть вещей". Также подробно разобраны примитивы для сетей вещей, к которым относятся датчики, агрегаторы, каналы связи, внешние устройства и решающие триггеры. В разделе, посвященном программированию, рассматриваются предложения W3C по использованию веб-технологий – веб-вещей. Этот подход призван устранить фрагментацию в стандартах разработки Интернета Вещей. Статья завершается обсуждением ключевой роли инфо-коммуникаций в цифровой экономике.**

***Ключевые слова* — Internet of Things, Web of Things**

I. Введение

Мы уважаем читателя и пытаемся писать статьи о том, как мы видим процессы в мире вообще и в России в частности. Но на этом пути приходится вводить совсем новые термины и ссылаться на те технические и научные аспекты, которые и составляют сущность цифровых трансформаций. Часто этот подход оказывается непонятым или, хуже того, порождает неумелые попытки высмеять, обозвать теоретиками и рассуждать о том, что авторы такого рода пассажей по своему образованию и навыкам не имеют никакого понятия.

Так было с терминами «интернет вещей» [1], «кибер-безопасность», «кибер-физические системы», о чем мы писали, ссылаясь, как нам казалось, на авторитетнейшие в мире источники, такие как институт NIST [15,16,17,18,19,20,21]. Мы пытались показать те мифы, которые связаны с этой новой областью, опубликовали статью «Демистификация цифровой экономики» [22] сразу после того, как на сайте Кремля появились сообщения о G20 и подписании от имени России соответствующих документов о цифровой трансформации. Но оказывается и этот сайт не очень вдумчиво читают (там публикация была в сентябре 2016 года) и для очень многих стало неожиданностью публикация Указа Президента России от 1 декабря 2016 [27].

Сообщества профессионалов в мире весьма отрицательно относились к термину интернет вещей. Но огромный маркетинговый шум о перспективах этого направления цифровой экономики приводил многих в мире в состояние оцепенения. При более серьезных рассмотрениях начались попытки модернизации терминологии на «промышленный интернет», на «интернет всюду» или «интернет доверенных вещей», которые шли от конкретных компаний или платформ, которые, тем не менее, не были до конца приняты многими в сообществе профессионалов.

Мы стремились конкретно указывать на области применения, такие как городские решения (умный город), производственные [22,23,24] или логистические [26] применения. Но это не избавляло от употребления не до конца понятного и не однозначного термина «Интернет вещей», полезного в рамках конкретных решений и платформ, но приводящего к коллизиям и практическим потерям в сложных системах, например, при кибератаках. Появился еще один термин Very Large Internet of Things (сверхбольшой Интернет вещей), который характеризует то, что технология начала выходить на интеграцию нескольких разнородных систем. Сегодня, когда решения государства [27] резко подняли цену любых ошибок в выборе путей развития России, в том числе, в употреблении терминов, мы вновь решили вернуться к общим вопросам.

Далее в статье обсуждаются вопросы кибер-безопасности (раздел 2), международной стандартизации (раздел 3) и программирования Интернета вещей (раздел 4). Статья завершается обсуждением ключевой роли инфо-коммуникаций в цифровой экономике.

II. О кибер-безопасности

Человечество уже более века использует автоматические датчики и средства управления, называя их сенсорами (от слова чувствовать и измерять) и

Статья получена 22 марта 2017

В.П. Куприяновский – Национальный центр компетенций в области цифровой экономики (email: vpkupriyanovsky@gmail.com)

М.А. Шнепс-Шнеппе – AbavaNet (email:sneps@mail.ru).

Д.Е.Намиот – МГУ имени М.В. Ломоносова (email:dnamiot@gmail.com).

С.П.Селезнев - Фактор ТС (e-mail: spseleznev@yandex.ru).

С.А.Синягов – Национальный центр компетенций в области цифровой экономики (email: ssinyagov@gmail.com)

Ю.В.Куприяновская. – Университет Оксфорда (email: Yulia.Kupriyanovskaya@sbs.ox.ac.uk).

подсоединяет их к компьютерам на протяжении десятилетий, но сейчас мы находимся в самом разгаре огромных технологических изменений, что дает небывалые возможности, но порождает и огромные риски, связанные с этими изменениями. Теперь есть возможность использовать крайне недорогие датчики и средства управления с удивительным и экспоненциально растущим разнообразием, доступностью и глубиной возможностей. Следуя их безусловной полезности и экономической реализуемости, уже развернуты технологии на базе IoT в зеленых зданиях, мониторинге окружающей среды, мониторинге здоровья и безопасности объектов. Мы покупаем автомобили с уже встроенными датчиками и элементами управления или, если угодно, то с Интернетом вещей (хотя автомобили, по большей части, не подключены к интернету).

Под угрозой находятся все объекты, которые входят в понятие «Интернет вещей» (IoT): объекты Министерства обороны и критически важных инфраструктур, оборудование, служащие и имущество - любое из которых может быть использовано для причинения вреда. Мы скоро можем оказаться в положении, когда решительный противник отключит нашу энергетику и воду, отключит наши системы безопасности, нарушит нашу способность оказывать медицинскую помощь, станет слушать наши беседы и следить за нашими движениями [2]. Собственно, [2] - это новейшая официальная публикация по этому вопросу Министерства обороны США (от февраля 2017 года). Не менее тревожны очень близкие по срокам официальные публикации Министерств торговли и внутренней безопасности США [28,29]. Так или иначе, все эти солидные ведомства пристально изучают применения IoT в различных системах, включая кибер-физические системы, общую операционную картину и кибер-безопасность (рис. 1).

В [2] сообщено, что: «по оценкам Gartner, в 2016 году будет развернуто более 6 миллиардов устройств IoT, и к 2020 году их число возрастет почти до 21 миллиарда. Если не предпринимать никаких действий, чтобы обойти эту проблему, он будет экспоненциально расти дальше, а рост IoT может захлестнуть эти структуры как приливная волна».

В документе [2] содержатся справочные и политические рекомендации по устранению уязвимостей (и использование возможностей), «связанные с всё более распространяющимися и полуавтономными устройствами, поддерживающими Интернет, что составляет так называемый Интернет вещей (IoT). Благодаря высокой полезности, низкой стоимости и простоте развертывания, IoT быстро распространяется как на автономные устройства, так и на встроенные датчики и элементы управления почти для всех типов электронных устройств - от бытовой техники до самолетов.

В то же время в [2] указывается на уязвимости и безопасность сетей и информации, в том числе и в Министерстве обороны. Век IoT уже наступил, и миллионы таких устройств уже установлены на наших объектах, транспортных средствах и медицинских устройствах. В новейших зеленых зданиях министерства обороны США есть десятки тысяч датчиков. Рост интернет-подключенных медицинских устройств так же увеличивается подобно взрыву.

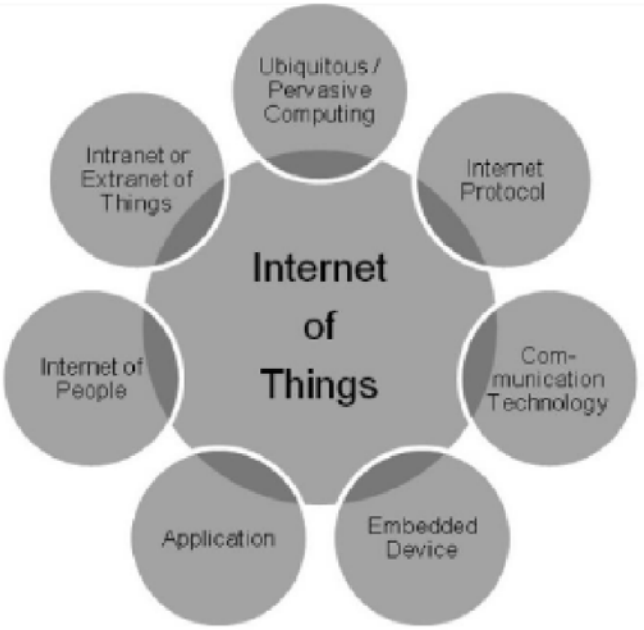

Рис. 1. Области использования IoT [2]

Устройства IoT могут быть включены в наши системы оружия и разведки (как преднамеренно, так и непреднамеренно). Из-за большого числа сенсоров IoT и из-за ограниченной вычислительной мощности брандмауэров и антивирусной защиты проблема их уязвимостей в плане безопасности количественно и качественно отличается от уязвимостей, ранее связанных с мобильными устройствами и промышленными системами управления. Учитывая безопасность и чувствительность миссий миротворческих сил, нам необходимо действовать сейчас, чтобы определить интересы министерства обороны и определить дополнительные шаги, которые необходимо предпринять. Полученные знания следует распространять в коммерческом мире»

III. О МЕЖДУНАРОДНОЙ СТАНДАРТИЗАЦИИ ИНТЕРНЕТА ВЕЩЕЙ (IOT)

В области стандартизации Интернета вещей наиболее фундаментальные работы проводятся в институте NIST. Летом 2016 вышел нашумевший документ [3]. В этом документе используются два акронима - IoT и NoT (Сеть Вещей, Network of Things), использование которых, как считают авторы, широко и взаимозаменяемо. Связь между NoT и IoT тонкая. IoT представляет собой экземпляр NoT, более конкретно, IoT имеет свои «вещи», привязанные к Интернету. Другой тип NoT может быть локальной сетью (ЛВС), при этом ни одна из его «вещей» не подключена к Интернету. Сети социальных сетей, сенсорные сети и Промышленный Интернет - это все варианты NoT [3]. Эта дифференциация в терминологии облегчает разделение вариантов использования на различные

вертикальные и качественные области (например, транспорт, медицинское, финансовое, сельскохозяйственное, критическое для безопасности, критическое для безопасности, критическое для производительности, создавая высокую степень уверенности, чтобы назвать несколько). Это полезно, так как нет сингулярного IoT, и бессмысленно говорить о сравнении одного IoT с другим.

В [3] вводится много новых понятий, базовым из которых является понятие примитива. Примитивы являются строительными блоками, которые дают возможность ответить на вышеупомянутые вопросы и утверждения, позволяя проводить сравнения между NoT. Термин примитив используется в [3] для представления меньших элементов, из которых могут быть построены более крупные блоки или системы. Например, при программном кодировании примитивы обычно включают арифметические и логические операции (плюс, минус, и, или и т.д.).

В [3] не дано определение того, что является или не является «вещью». Считается, что каждый примитив вводит поведение, представляющее эту «вещь», рабочий поток и поток данных. «Вещи» могут встречаться в физическом пространстве или виртуальном пространстве. В физическом пространстве рассматриваются люди, транспортные средства, компьютеры, коммутаторы, маршрутизаторы, интеллектуальные устройства, дорожные сети, офисные здания и т.д. В виртуальном пространстве рассматриваются программное обеспечение, потоки информации социальных медиа, файлы, потоки данных, виртуальные машины, виртуальные сети и т. д.

Примитивы предлагают унифицирующий словарь [3], который позволяет компоновать и обмениваться информацией между различными сетями. Они предлагают ясность относительно тонкостей, включая функциональную совместимость, компоновку и непрерывно связывающие активные процессы, которые приходят и уходят «на лету». Поскольку не существует простого, действенного и общепринятого определения IoT, предлагаемая модель и словарь раскрывают лежащие в основе IoT вещи и явления, т. е. [3] раскрывает ингредиенты, которые могут выразить поведение IoT, без определения IoT. Это дает представление о проблемах, связанных с доверием к таким системам и их безопасностью.

Мы считаем, что [3] является значительной работой в стандартизации уже состоявшегося в мире явления «интернет вещей», поэтому остановимся на базовом понятии примитива более подробно (NIST провел публичное мировое обсуждение темы примитивов IoT с февраля по март 2016 года [9]).

Примитивы NoT - это:

1) датчик (Sensor),
2) агрегатор (Aggregator),
3) канал связи (Communication channel),
4) внешнее устройство (external utility, eUtility) и
5) решающий триггер (Decision trigger).

Первые три примитива показаны на рис. 2.

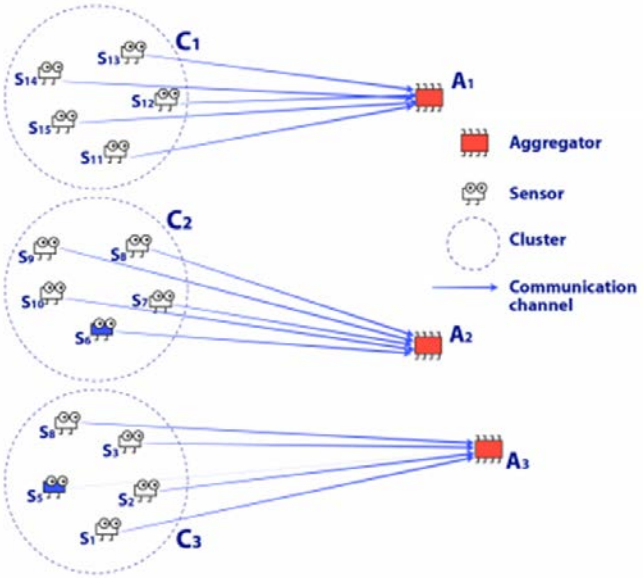

Рис. 2. Первые три примитива: датчик, агрегатор и канал связи

A. Примитив №1: Датчик

Датчик - это электронное устройство, которое измеряет физические свойства объекта, такие как температура, ускорение, вес, звук, контакт, местоположение, наличие, идентичность и т.д. Все датчики используют механические, электрические, химические, оптические или другие эффекты на интерфейсе контролируемого процесса или открытой среде. Вот основные свойства, предположения, рекомендации и общие сведения о датчике:

1. Датчики являются физическими; некоторые из них могут иметь доступ в Интернет.

2. Выходной сигнал датчика - данные; s1 → d1 означает, что датчик 1 создал часть данных, пронумерованных как датчик 1; аналогично, s2 → d2 означает, что датчик 2 создал часть данных с номером 2. Это - цифровые данные. Аналоговые датчики, такие как микрофоны и вольтметры, являются контр-примерами.

3. Датчик может также передавать информацию идентификации устройства, такую как радиочастотная идентификация (RFID).

4. Датчики могут иметь идентичность или иметь идентичность «вещи», к которой они прикреплены.

5. Датчики могут иметь незначительное или полное отсутствие функциональности программного обеспечения и вычислительной мощности; более продвинутые датчики могут иметь программную функциональность и вычислительную мощность.

6. Датчики могут быть разнородными, от разных производителей, и собирать данные с разным уровнем целостности данных.

7. Датчики могут быть связаны с фиксированным географическим местоположением или могут быть мобильными.

8. Датчики могут обеспечивать наблюдение. Камеры и микрофоны - это датчики.

9. Датчики могут иметь владельца (владельцев), который будет контролировать данные, собираемые их датчиками, и определять, кому разрешен доступ к нему и когда.

10. Датчики будут иметь родословную - географические места происхождения и производителей. Родословная может быть неизвестной и подозреваемой.

11. Датчики могут быть дешевыми, одноразовыми, подвержены износу с течением времени.

12. Могут быть различия в безопасности и надежности датчиков, например, между потребительским, военным, промышленным и т.д.

13. Датчики могут: не давать данные, возвращать полностью испорченные, частично испорченные или правильные и приемлемые данные. Датчики могут работать полное время или периодически. Они могут терять чувствительность или калибровку.

14. Ожидается, что датчики возвратят данные в определенных диапазонах, например, [1, ..., 100]. Если диапазоны нарушаются, и игнорирование данных за пределами границ является недопустимым, могут потребоваться правила о передаче управления человеку или машине.

15. Датчики могут быть одноразовыми или исправными с точки зрения калибровки, чувствительности или других форм обновления. Сложные и дорогие датчики могут быть отремонтированы вместо замены.

16. Датчики могут питаться различными способами, включая переменный ток, солнечную энергию, ветер, батарею или пассивно через радиоволны.

17. Датчики могут быть приобретены в готовом виде или построены по спецификации.

18. Датчики получают данные, которые могут управляться событиями, управляться вручную, управляться командами или запускаться в заранее заданное время.

19. Датчики могут иметь определенный уровень целостности данных.

20. Датчики могут иметь свои данные в зашифрованном виде, чтобы реализовать в них некоторые соображения безопасности.

21. Датчики должны иметь возможность быть аутентифицированными как настоящие.

22. Данные датчика могут быть отправлены и переданы нескольким NoT. Датчик может иметь несколько получателей своих данных. Данные датчика могут быть сданы в аренду одному или нескольким NoT.

23. Частота, с которой датчики выпускают данные, влияет на валидность и релевантность данных. Датчики могут возвращать действительные, но устаревшие данные. Данные датчика могут находиться в состоянии покоя в течение длительных периодов времени.

24. Точность информации датчика может определяться точностью датчика. Необходимо учитывать погрешность данных датчика.

25. Датчики могут передавать данные о «здоровье» системы, например, при прогнозировании и управлении здоровьем человека.

26. В этом документе и в этой модели мы не классифицируем людей как датчики; человек классифицируется как внешнее устройство (eUtility) или решающий триггер (Decision trigger). Когда они классифицируются как eUtility, люди все еще могут действовать в роли датчиков, вручную передавая данные в рабочий поток NoT и в поток данных.

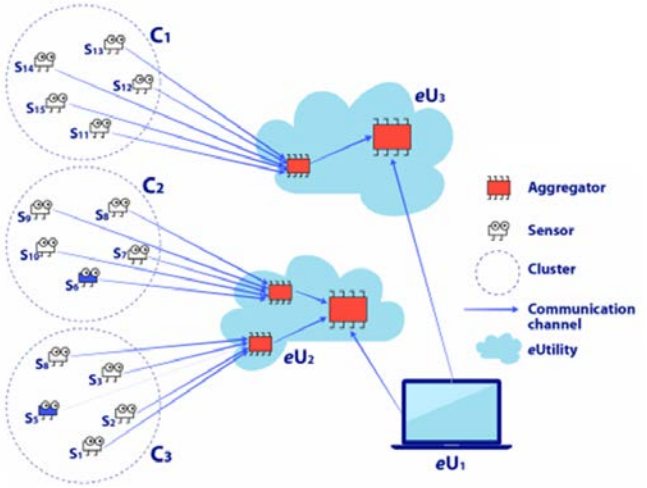

Рис. 3. Место внешнего устройства (eUtility)

27. Люди могут влиять на работу датчика в результате несоблюдения правил, неправильной установки датчика и т. д. (или их положительных аналогов). Люди потенциально способствуют сбоям датчиков.

28. Безопасность касается датчиков, если они или их данные подделываются, украдены, удалены или переданы небезопасно, так чтобы к ним могли получить доступ неавторизованные стороны. Построение безопасности в конкретных датчиках может быть или не быть необходимым на основе общей конструкции системы.

29. Надежность касается датчиков.

B. Примитив №2: Агрегатор.

Это программная реализация, основанная на математических функциях, которая преобразует группы исходных данных в промежуточные, агрегированные данные. Необработанные данные могут поступать из любого источника. Агрегаторы помогают управлять большими данными.

Кластер представляет собой абстрактную группу датчиков, которые могут появляться и исчезать мгновенно.

Понятие «Вес» - это степень, в которой данные конкретных датчиков влияют на вычисление агрегатора.

C. Примитив №3: Канал связи.

Это среда, с помощью которой передаются данные (например, физические через универсальную

последовательную шину (USB), беспроводные, проводные, устные и т.д.).

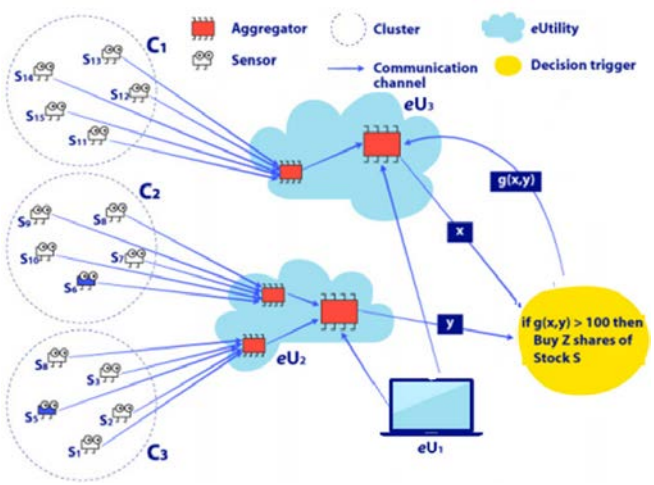

Рис. 4. Общая схема Интернета вещей (включая решающий триггер с обратной связью)

NIST – самое большое в мире исследовательское учреждение по вопросам стандартизации во всех сферах народного хозяйства. Оно находится в составе Министерства торговли США (размещается в пригороде Вашингтона). Только по отдельной позиции Интернета вещей потребовалось провести огромный объем работ. Понадобилась даже публикация с названием «Демистификация интернета вещей» [4], чтобы остудить горячие маркетинговые головы. Перечислим лишь некоторые из фундаментальных работ NIST:

[6]— январь 2017 года, об управлении рисками инженерных работ;

[7]- декабрь 2016 года, руководство по кибер-безопасности;

[8] - начало 2017 года, технические требования и допуски для весов и измерительных приборов;

[9] – февраль 2016, уточнения документа [3] о примитивах и других элементах IoT;

[10] – ноябрь 2016 года, обзор состояния и новые направления обнаружения атак на физическом уровне в управляющих системах;

[11] – декабрь 2016, аддитивные производства - сетевой характер;

[12] – апрель 2016, измерение удобства использования и безопасности разрешенных паролей на мобильных платформах;

[13] - октябрь 2016 года, руководство по совместному использованию информации о кибер-угрозах;

[14] - апрель 2016 года, семинар по открытой облачной архитектуре для интеллектуального производства.

IV. О программировании Интернета вещей: Веб вещей

Веб вещей (Web of Things, WoT) относится к области программировании IoT и наиболее серьезно этим занимается консорциум W3C [30]. Предоставим слово википедии: «Web of Things - термин, используемый для описания подходов, архитектурных стилей программного обеспечения и шаблонов программирования, которые позволяют объектам реального мира быть частью World Wide Web. Подобно тому, что Web (Application Layer) относится к Интернету (Network Layer), Web of Things предоставляет Application Layer, который упрощает создание приложений Internet of Things. Вместо того, чтобы повторно изобретать совершенно новые стандарты, Web of Things направлен на повторное использование уже существующих средств и известных Web стандартов (e.g., REST, HTTP, JSON), семантического Web (e.g., JSON-LD, Microdata), Web реального времени (e.g., Websockets) и средства социального Web (рис. 5)».

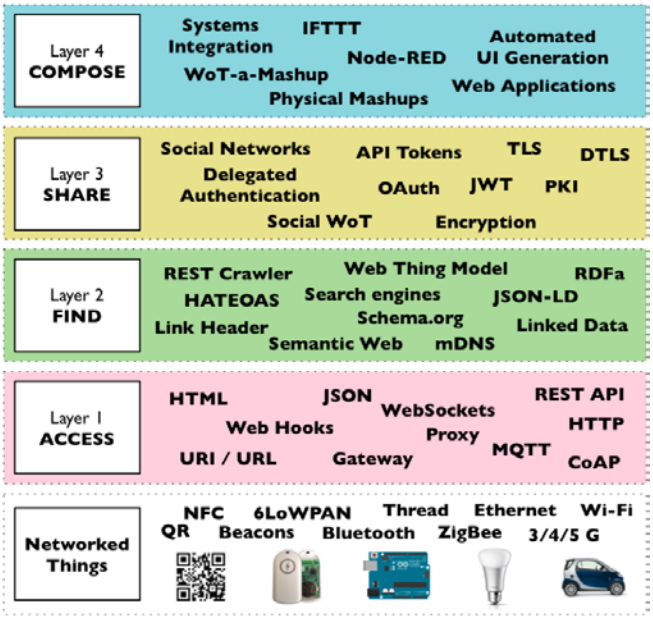

Рис. 5. Архитектура уровней Web of Things [32]

В феврале 2017 W3C объявил [31], что начинает работу над веб-стандартами, чтобы уменьшить фрагментацию IoT. Недавно W3C организовал Рабочую группу Web of Things для разработки исходных стандартов Web of Things, чтобы противостоять фрагментации IoT, сократить расходы на разработку, снизить риски для инвесторов и клиентов и стимулировать экспоненциальный рост рынка устройств и услуг IoT.

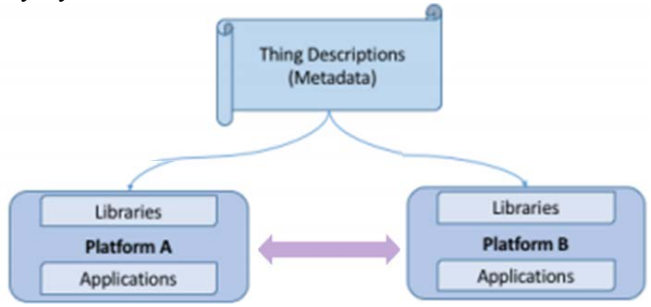

Рис. 6. Взаимодействие разнородных платформ

Болезни и недостатки IoT стали очевидными в эпоху его «взросления»: он страдает от недостатка функциональной совместимости между разнородными платформами (рис. 6). Это можно сравнить с ситуацией

в Интернете, когда существуют конкурирующие несовместимые сетевые технологии. Интернет позволяет легко создавать сетевые приложения независимо от этих технологий. W3C стремится сделать то же самое для Интернета Вещей. Для достижения этой цели необходимы независимые от платформы API-интерфейсы для разработчиков приложений, а также средства для различных платформ, чтобы обеспечить их взаимодействие. Подход, который использует W3C, основан на богатых метаданных, которые описывают модели данных и взаимодействия, доступные для приложений, а также требования к коммуникациям и безопасности для эффективной коммуникации с платформами. Еще одним аспектом является необходимость обеспечения того, чтобы платформы обменивались одним и тем же значением при обмене данными. Поэтому W3C стремится обеспечить возможность выражения семантики вещей и связанных с ними ограничений домена, опираясь на обширную работу W3C по семантическому интернету, RDF и связанным данным.

Подход W3C включает в себя возможности использования таких языков сценариев, как JavaScript, кодирование данных, таких как JSON и EXI, форматы данных и метаданных, включая связанные данные, и протоколы, такие как HTTP и WebSockets, и это лишь несколько примеров. JavaScript может использоваться для прямого доступа к датчикам и исполнительным устройствам IoT из браузера, на платформах обслуживания в облаке или в границах сети, а также для драйверов устройств в шлюзах, которые используют протоколы IoT для доступа к встроенным / ограниченным устройствам, и веб-протоколы для отображения их для обслуживания на платформах.

Идентификация важна для устройств, пользователей, приложений и служб, как часть комплексной защиты и доверительного управления. В отличие от обычных веб-приложений, мы не можем предполагать, что пользователь присутствует и может аутентифицировать себя. Доверительное управление повлечёт за собой, например, средства проверки метаданных, их происхождение, местоположение данного датчика и т.д. Это аналогично тому, как вы узнаете потребности своих клиентов в банковском мире.

Приложениям и сервисам часто требуются данные на более высоком уровне, чем исходные данные, предоставляемые датчиками. Кроме того, данные необходимо интерпретировать в контексте других источников информации. То же самое относится к системам управления, действия которых должны быть переведены в контексте объектов более низкого уровня. Web of Things должна быть в состоянии моделировать реальный мир на разных уровнях абстракции и открывать открытые рынки со свободной конкуренцией услуг на этих уровнях. Вещи в Web of Things можно рассматривать как виртуальные представления физических или абстрактных сущностей.

W3C резонно отмечает, что всю работу он не может сделать в одиночку и предлагает сотрудничество с другими отраслевыми альянсами и организациями по разработке стандартов IoT. Эта помощь необходима, чтобы реализовать огромный потенциал веб-рынка, обеспечивая масштабируемость услуг на основе межплатформенных веб-технологий. Собственно, в профессиональных публикациях никогда и не прекращалось употребление термина ВЕБ вещей [5], но главное в описываемых событиях в том, что мировое сообщество ученых и технологов начинает находить правильный путь к построению системы стандартов и технических правил в этом направлении. Фактически именно через тексты стандартов W3C, написанные на искусственном языке, более понятном компьютерам, чем людям и развиваются сегодняшние приложения интернета, которыми все мы пользуемся.

V. О КЛЮЧЕВОЙ РОЛИ ИНФОКОММУНИКАЦИЙ В ЦИФРОВОЙ ЭКОНОМИКЕ

Ключевым понятием цифровой экономики является обеспечение критической инфраструктуры государства и обеспечение сервисов безопасности общества (рис. 7).

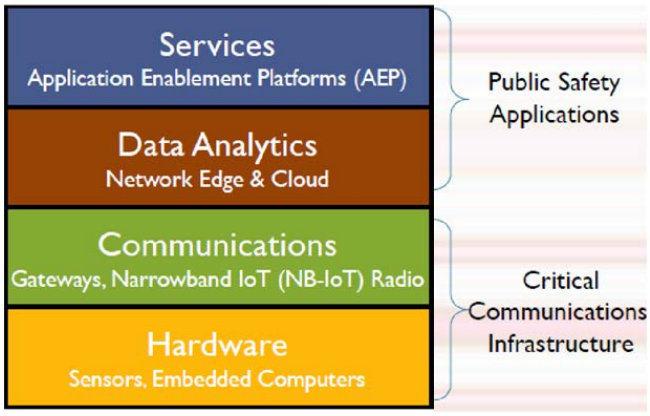

Рис. 7. Роль критической инфокоммуникационной инфраструктуры в обеспечении сервисов IoT

Более подробно архитектура безопасности государства представлена на рис. 8. Показаны прикладные области (приложения), которые упорядочены по государственной важности. Во всех этих областях имеются сенсоры, которые через средства связи общаются с приложениями, как показано на рис. 7. Центральное место занимает служба First Responders, что по российскому законодательству называется аппаратно-программный комплекс «Безопасный город», и включает пожарную охрану, отравляющие материалы (Hazmat), экстренную медицинскую службу (EMS), правонарушения (полицию) и службу 911 (в России – 112). Далее от центра находятся менее важные экстренные службы.

Перспективные преимущества IoT для общественной безопасности, удобства персонала, эффективности и окружающей среды ясны. Обновленный IoT может сделать наши дороги более безопасными, позволяя связанным транспортным средствам взаимодействовать друг с другом для предотвращения несчастных случаев.

Рис. 8. Архитектура безопасности государства

Он поможет сделать доступ к качественному медицинскому обслуживанию более доступным с помощью устройств дистанционного мониторинга и практики телемедицины для тех, кто не может легко путешествовать, сократить количество отходов и повысить эффективность, как в заводских цехах, так и в городах. Он даже имеет потенциал для создания новых отраслей промышленности и потребительских товаров, которые еще предстоит создать. Однако для полного осуществления потенциала необходимо создать инфраструктуру и политику, включая стратегии реагирования на вызовы, возникающие в таких областях, как кибер-безопасность и неприкосновенность частной жизни. Путь к этому лежит через систему стандартов и правил, принятых профессиональным сообществом ученых и специалистов.

Нам представляется, что вопросы, поднятые в этой статье про изменения в подходах к IoT, а также потенциальный масштаб влияния этих изменений на всю экономику России, должен иметь хорошие последствия для решения этих задач и для защиты развития надежной среды IoT, которая приносит пользу потребителям, экономике и обществу в целом.

БИБЛИОГРАФИЯ

[1] Minerva R., Biru A., Rotondi D. Towards a definition of the Internet of Things (IoT) //IEEE Internet Initiative. – 2015. – №. 1.
[2] DoD Policy Recommendations for The Internet of Things (IoT). Chief Information Officer. U.S. Department of Defense. December 2016
[3] Jeffrey Voas. Networks of 'Things'. NIST Special Publication 800-183. July 2016
[4] Elizabeth B. Lennon. Demystifying the internet of things. NIST Information Technology Laboratory. ITL Bulletin for September 2016
[5] Khan M., Silva B. N., Han K. A Web of Things-Based Emerging Sensor Network Architecture for Smart Control Systems //Sensors. – 2017. – Т. 17. – №. 2. – С. 332.
[6] NISTIR 8062. Sean Brooks, Michael Garcia, Naomi Lefkovitz, Suzanne Lightman, Ellen Nadeau. "An Introduction to Privacy Engineering and Risk Management in Federal Systems". Information Technology Laboratory .National Institute of Standards and Technology. Internal Report 8062, January 2017
[7] NIST Special Publication 800-184. Guide for Cybersecurity Event Recovery. December 2016
[8] NIST. Specifications, Tolerances, and Other Technical Requirements for Weighing and Measuring Devices. 2017
[9] NIST IR 8063 DRAFT. Primitives and Elements of Internet of Things (IoT) Trustworthiness. February 16, 2016
[10] NIST GCR 16-010. Survey and New Directions for Physics-Based Attack Detection in Control Systems, November 2016
[11] NIST Advanced Manufacturing Series 600-2. Network Charter Manufacturing USA Program, December 2016
[12] NISTIR 8040. Measuring the Usability and Security of Permuted Passwords on Mobile Platforms. NIST, April 2016
[13] NIST Special Publication 800-150. Guide to Cyber Threat Information Sharing, October 2016
[14] NISTIR 8124. OAGi/NIST Workshop on Open Cloud Architecture for Smart Manufacturing, April 2016
[15] Добрынин А. П. и др. Цифровая экономика-различные пути к эффективному применению технологий (BIM, PLM, CAD, IOT, Smart City, BIG DATA и другие) //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 1.-С.4-11.
[16] Куприяновский В. П., Намиот Д. Е., Синягов С. А. Кибер-физические системы как основа цифровой экономики //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 2.-С.18-25.
[17] Куприяновский В. П. и др. Цифровая экономика и Интернет Вещей–преодоление силоса данных //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 8.-С.36-42.
[18] Шнепс-Шнеппе М. А. и др. О кибербезопасности критической инфраструктуры государства //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 7.-С.22-31.
[19] Шнепс-Шнеппе М. А. и др. О телекоммуникационной инфраструктуре комплекса «Безопасный город» //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 6.-С.17-31.
[20] Куприяновский В. П., Намиот Д. Е., Куприяновский П. В. Стандартизация Умных городов, Интернета Вещей и Больших Данных. Соображения по практическому использованию в России //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 2.-С.34-40.
[21] Шнепс-Шнеппе М. А. и др. К системному проектированию Системы 112 и комплекса «Безопасный город» //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 9.-С.44-63.
[22] Куприяновский В. П., Намиот Д. Е., Синягов С. А. Демистификация цифровой экономики //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 11.-С.59-63.
[23] Куприяновский В. П. и др. Интернет Вещей на промышленных предприятиях //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 12.-С.69-78.
[24] Куприяновский В. П. и др. Трансформация промышленности в цифровой экономике - проектирование и производство //International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 1.-С.50-70.
[25] Куприяновский В. П. и др. Трансформация промышленности в цифровой экономике – экосистема и жизненный цикл //International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 1.-С.34-49.
[26] Куприяновский В. П. и др. Интеллектуальная мобильность в цифровой экономике //International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 2.-С.46-63.
[27] Указ Президента Российской Федерации «О Стратегии научно-технологического развития Российской Федерации» от 1 декабря 2016 года № 642
[28] Fostering the advancement of the internet of things. The department of commerce. Internet policy task force & digital economy leadership team. January 2017.
[29] Strategic Principle for securing the internet of things (IoT). U.S. Departament of Homeland Security. Version 1.0, November 15, 2016
[30] Восков Л. С. и др. Web вещей–новый этап развития интернета вещей //Качество. Инновации. Образование. – 2013. – №. 2. – С. 44-49.
[31] Web of Things https://www.w3.org/WoT/ Retrieved: Apr, 2017
[32] Guinard, D., Vlad, T.: Building the web of things. Manning (2015)

Web of Things and Internet of Things in the Digital Economy

Vasily Kupriyanovsky, Manfred Sneps-Sneppe, Dmitry Namiot, Sergey Seleznev, Sergey Sinyagov, Julia Kupriyanovsky

Abstract – The article examines the place in the digital economy for such areas as Internet of Things, Network of Things and Web of Things. The basis for this article has been formed from research of the institute of standards NIST and the consortium W3C. The paper addresses the issues of cyber security of the Internet Things, international standardization, and programming of the Internet of Things. In the section on standardization, we consider the term "network of things" introduced by NIST. Also, primitives for networks of things, such as sensors, aggregators, communication channels, external devices, and decision triggers are analyzed in details. In the section on programming, the paper discusses W3C suggestions on the use of web technologies – Web of Things. This approach is designed to eliminate fragmentation in the standards of developing Internet of Things applications. The article concludes with a discussion of the key role of information and communication technologies in the digital economy.

Keywords – Internet of Things, Web of Things