

*Кара-Сал А.А., Левченко М.О. Стандартизация в области интернета вещей // Академия педагогических идей «Новация». Серия: Научный поиск. – 2017. – № 04 (декабрь). – АРТ 16-эл. – 0,3 п.л. - URL: <http://akademnova.ru/series-scientific-search>*

**РУБРИКА: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ**

**УДК 004.75**

**Кара-Сал Ай-Кат Айдысовна,**

**Левченко Мария Олеговна**

студенты 3-го курс, Факультет математической  
экономики, статистики и информатики

*Научный руководитель:* Попов А.А., доцент

РЭУ им. Г.В. Плеханова

г. Москва, Российская Федерация

[wow.letsfight@ya.ru](mailto:wow.letsfight@ya.ru), [karasal.97@mail.ru](mailto:karasal.97@mail.ru)

**СТАНДАРТИЗАЦИЯ В ОБЛАСТИ  
ИНТЕРНЕТА ВЕЩЕЙ**

*Аннотация:* В данной работе рассматривается актуальная проблема по стандартизации Интернет вещей. Были проанализированы предложенные рекомендации по стандартизации и обнаружены их узкие места.

*Ключевые слова:* Интернет вещей, стандартизация, информационная безопасность, информационные технологии.

**Kara-Sal Ai-Kat Aidysovna,**

**Levchenko Maria Olegovna**

3 course, Faculty of Mathematical Economics, Statistics and  
Informatics

Supervisor: Popov A.A., Associate Professor

Plehanov Russian University of Economics

Moscow, Russian Federation

[wow.letsfight@ya.ru](mailto:wow.letsfight@ya.ru), [karasal.97@mail.ru](mailto:karasal.97@mail.ru)

## **STANDARTISATION IN THE AREA OF IOT**

*Abstract:* In this work, the current problem on standardization of the Internet of things is considered. The offered recommendations about standardization have been analyzed and their bottlenecks are found.

*Keywords:* Internet of things, standardization, information security, information technologies.

Стандарты занимают огромное место в сфере информационных технологий и являются практически основным фактором глобализации и мирового развития. Вопрос стандартизации интернета вещей в настоящее время остро обсуждается практически во всех международных организациях, связанных с данной областью. Обращение к рекомендациям по стандартизации в области интернета вещей является

исходным моментом в выявлении основных проблем создания единых стандартов для IoT устройств.

Явление IoT занимает одно из главенствующих мест, определяющих дальнейшее развитие инфокоммуникационной среды. По мнению Gartner, IoT выйдет в «mass-market» не раньше, чем через пять лет. Полагают, что к 2020 году к интернету вещей будет подключено от 50 до 100 миллиардов устройств, которые будут контактировать между собой с помощью большого разнообразия способов. В связи с этим началась разработка стандартов в данной сфере. К сожалению, фирмы-производители устройств Интернета вещей и производители соответствующего программного обеспечения зачастую не беспокоятся о возможности совместной работы устройств от разных производителей.

На данном этапе развития ИТ стандартизируются различные технологии, и отсутствие единой всеобъемлющей стандартизации IoT является одной из главных проблем, не позволяющих IoT выйти в массы. В общем и целом, для такого молодого направления, как Интернет вещей, на данном этапе имеются общие концептуальные и архитектурные решения.

Архитектура IoT включает четыре функциональных уровня:

1. Уровень сенсоров и сенсорных сетей.

Этот уровень архитектуры включает «умные» объекты, интегрированные с сенсорами. Сенсоры реализуют соединение физического и виртуального миров, обеспечивая сбор и обработку информации в реальном масштабе времени. Они имеют небольшую память, давая возможность записывать некоторое количество результатов измерений. Сенсор может измерять физические параметры контролируемого объекта/явления и преобразовать их в сигнал, который может быть принят соответствующим устройством.

Зачастую сенсор требует соединения со шлюзом, которые могут быть реализованы с использованием локальной вычислительной сети, таких как Ethernet и Wi-Fi или персональной сети, таких как ZigBee, Bluetooth и ультраширокополосной беспроводной связи на малых расстояниях. Для сенсоров, которые не требуют подключения к агрегатору, их связь с серверами/приложениями может предоставляться с использованием глобальных беспроводных сетей, таких как GSM, GPRS и LTE. Сенсоры, которые характеризуются низким энергопотреблением и низкой скоростью передачи данных, образуют широко известные беспроводные сенсорные сети и набирают все большую популярность, поскольку они могут содержать гораздо больше сенсоров с поддержкой работы от батарей и охватывают большие площади.

## 2. Уровень шлюзов и сетей.

Большой объем данных, создаваемых на первом уровне IoT многочисленными миниатюрными сенсорами, требует надежной и высокопроизводительной проводной или беспроводной сетевой инфраструктуры в качестве транспортной среды. Сети должны обеспечивать требуемые значения качества передачи информации, и прежде всего по задержке, пропускной способности и безопасности. Данный уровень состоит из конвергентной сетевой инфраструктуры, которая создается путем интеграции разнородных сетей в единую сетевую платформу.

## 3. Сервисный уровень.

Сервисный уровень содержит набор информационных услуг, призванных автоматизировать технологические и бизнес операции в IoT.

## 4. Уровень приложений.

На последнем уровне архитектуры IoT существуют всевозможные приложения для различных промышленных сфер.

В ближайшем будущем основным аспектом, на который стоит обратить внимание, будет гармонизации и слияние различных стандартов для формирования единой и непротиворечивой нормативной базы с целью практической реализации Интернета вещей.

В настоящее время данной проблемой занимаются ассоциации и международные организации:

- ETSI (Европейский институт стандартов телекоммуникаций)
- IEEE (Институт инженеров по электротехнике и электронике)
  - OASIS (Организация по внедрению стандартов структурированной информации)
  - OGC (Открытый геопространственный консорциум)
  - IoT-A

«Комплексный проект Европейского маяка, посвященный архитектуре Интернет-вещей, предлагает создание архитектурной эталонной модели вместе с определением исходного набора ключевых строительных блоков».

- Международное общество автоматизации ISA
- IEC (Международная электротехническая комиссия) и ISO (Международная организация по стандартизации), через JTC (Совместный технический комитет) .
- ITU (Международный союз электросвязи МСЭ-Т)

В рамках серии МСЭ-Т Y.2xxx, посвященной сетям следующего поколения NGN, уже утверждены первые рекомендации, посвященные специально Интернету

вещей: У.2060 «Обзор Интернета вещей», У.2063 «Основа WEB вещей» и У.2069 «Термины и определения Интернета вещей» и др.

В рекомендации МСЭ-Т У.2060 прописаны возможности обеспечения безопасности, которые в последующем могут быть стандартизированы: общие возможности обеспечения безопасности и специализированные возможности обеспечения безопасности.

Общие возможности обеспечения безопасности не зависят от приложений и включают:

- на уровне приложения: авторизацию, аутентификацию, защиту конфиденциальности и целостности данных приложения, защиту неприкосновенности частной жизни, аудит безопасности и антивирусную программу;
- на уровне сети: авторизацию, аутентификацию, конфиденциальность данных об использовании и данных сигнализации, а также защиту целостности данных сигнализации;
- на уровне устройства: аутентификацию, авторизацию, проверку целостности устройства, управление доступом, защиту конфиденциальности и целостности данных.

Специализированные возможности обеспечения безопасности тесно связаны с требованиями

приложений, например, требованиями безопасности мобильных платежей.

В настоящий момент в соответствии с архитектурой IoT существуют стандарты только для первого уровня-уровня сенсоров и сенсорных сетей.

Среди этих стандартов выделяются:

- Стандарт IEEE Std 802.15.4.

Предназначен для реализации беспроводных персональных сетей большой емкости с низким энергопотреблением и низкой скоростью передачи данных. Он реализует только два нижних уровня стека протоколов – физический уровень (PHY) и уровень доступа к среде (MAC). Стандарт является базовой основой для более высокоуровневых протоколов, таких как ZigBee, WirelessHART и MiWi и может быть использован совместно со стандартом 6LoWPAN и стандартными протоколами Интернета для построения беспроводных сенсорных сетей.

- Стандарт ZigBee

Стандарт ZigBee включает описание сетевых процессов управления, совместимости и профилей устройств, а также информационной безопасности. На сетевом уровне в ZigBee определены механизмы маршрутизации и формирования логической топологии сети.

Основная особенность технологии ZigBee заключается в том, что она при малом энергопотреблении поддерживает не только простые топологии сети, но и самоорганизующуюся и самовосстанавливающуюся ячеистую топологию с ретрансляцией и маршрутизацией сообщений, 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 развертывания, обслуживания и модернизации

- Стандарт 6LoWPAN

Стандарт, обеспечивающий взаимодействие малых беспроводных сетей с сетями IP по протоколу IPv6 с малым энергопотреблением. Технология используется в основном для организации сетей датчиков и автоматизации жилого и офисного помещения с возможностью управления через интернет, однако может использоваться и автономно для реализации простых беспроводных сетей датчиков.

- Стандарты WirelessHART и ISA100.11a

WirelessHART – протокол передачи данных по беспроводной линии связи, разработанный фондом HART Communication Foundation для передачи данных в виде HART- сообщений в беспроводной среде.

ISA100.11a – стандарт организации промышленных сенсорных сетей, сетей датчиков и приводов. Стандарт разработан Международным обществом по автоматике ISA (International Society of Automation) и одобрен МЭК в качестве общедоступной спецификации.

Таким образом, для остальных уровней архитектуры IoT, а также для сферы безопасности и конфиденциальности, в настоящее время стандарты не разработаны. Отсутствие единого стандарта, охватывающего все уровни архитектуры IoT, тормозит развитие данной сферы и подвергает опасности уже включенные в сеть «вещи». Однако, данная проблема уже рассматривается многими ассоциациями, которые на данный момент уже выпустили определенные рекомендации по стандартизации, а также проекты стандартов.

На основании всего вышесказанного можно выделить основные угрозы и сдерживающие факторы развития интернета вещей:

- Отсутствие согласованных стандартов: государство и международные организации должны провести системную работу по адаптации технологических стандартов и протоколов к новым технологическим условиям;
- Недостаточно проработанное правовое поле;

- Неполноценное обеспечение кибербезопасности: недостаточная защита данных в глобальных сетях и вторжение IoT в частную жизнь;

- Отсутствие понимания необходимости рассмотрения безопасности «вещей» с точки зрения жизненного цикла.

Поэтому возможными направлениями развития Интернета вещей являются:

- Создание единых стандартов. Проектом стандарта Интернета вещей в России является Narrow Band Fidelity (NB-FI), разработанный Ассоциацией интернета вещей (АИВ). NB-FI является стандартом сотовой связи для устройств телеметрии с низкими объёмами обмена данными. Устройства по этому стандарту будут работать на частоте 868 МГц — это свободный диапазон как в России, так и в Европе. Не требуются разрешения или лицензии для передачи данных на этой частоте. Передатчики NB-FI могут обмениваться данными на расстоянии до 10 км и работают от одной батарейки до 10 лет.

Интернет вещей предполагает подключение радио сенсоров на разнообразные устройства: автомобили, бытовую технику, счётчики ЖКХ (вода, электричество, тепло), охранные системы, бытовую технику, домашние устройства в «умном доме», игровые устройства, носимые гаджеты и т. д. Все эти устройства теоретически

могут общаться между собой и согласовывать свои действия.

- Повышение качества существующих продуктов и сервисов за счет обеспечения бесперебойности их работы, превентивного устранения возможных неполадок, оптимизации использования сырья и сокращения влияния человеческого фактора.

Таким образом, была освещена проблема отсутствия стандартов для устройств Интернета вещей, необходимости разработки единого стандарта, охватывающего все аспекты и уровни архитектуры и рассмотрены возможные пути её решения, которые на наш взгляд являются наиболее перспективными и достаточно легко осуществимыми.

#### **Список использованной литературы:**

1. Рекомендация МСЭ-Т Y.2060 (06/2012).
2. Попов А.А., Дутов К.С. Возможность использования Интернета вещей в едином информационном пространстве для жилищно- коммунального хозяйства региона // Научные труды Вольного экономического общества России. 2014. Т.186. С.391-396
3. Росляков А.В. Интернет вещей: учебное пособие [Текст] / А.В. Росляков, С.В. Ваняшин, А.Ю. Гребешков. – Самара: ПГУТИ, 2015. – 200 с.
4. В России появится национальный стандарт интернета вещей
5. <https://www.vedomosti.ru/technology/articles/2017/07/11/719563-standart-interneta-veschei> (дата обращения: 18.11.2017).

6. Are We Creating An Insecure IoT Security Challenges and Concerns <https://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things> (дата обращения: 22.11.2017).

*Дата поступления в редакцию: 12.12.2017 г.*

*Опубликовано: 18.12.2017 г.*

*© Академия педагогических идей «Новация». Серия: «Научный поиск»,  
электронный журнал, 2017*

*© Кара-Сал А.А., Левченко М.О., 2017*