Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Y.2066

(06/2014)

СЕРИЯ Y: ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ

Сети последующих поколений –
Структура и функциональные модели архитектуры

Общие требования к интернету вещей

Рекомендация МСЭ-Т Y.2066

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Y

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ МЕЖСЕТЕВОГО ПРОТОКОЛА, СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ, ИНТЕРНЕТ ВЕЩЕЙ И "УМНЫЕ" ГОРОДА

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА	
Общие положения	Y.100–Y.199
Услуги, приложения и промежуточные программные средства	Y.200–Y.299
Сетевые аспекты	Y.300–Y.399
Интерфейсы и протоколы	Y.400–Y.499
Нумерация, адресация и присваивание имен	Y.500–Y.599
Эксплуатация, управление и техническое обслуживание	Y.600–Y.699
Безопасность	Y.700–Y.799
Рабочие характеристики	Y.800–Y.899
АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ	
Общие положения	Y.1000–Y.1099
Услуги и приложения	Y.1100–Y.1199
Архитектура, доступ, возможности сетей и административное управление ресурсами	Y.1200–Y.1299
Транспортирование	Y.1300–Y.1399
Взаимодействие	Y.1400–Y.1499
Качество обслуживания и сетевые показатели качества	Y.1500–Y.1599
Сигнализация	Y.1600–Y.1699
Эксплуатация, управление и техническое обслуживание	Y.1700–Y.1799
Начисление платы	Y.1800–Y.1899
IPTV по NGN	Y.1900–Y.1999
СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ	
Структура и функциональные модели архитектуры	**Y.2000–Y.2099**
Качество обслуживания и рабочие характеристики	Y.2100–Y.2199
Аспекты обслуживания: возможности услуг и архитектура услуг	Y.2200–Y.2249
Аспекты обслуживания: взаимодействие услуг и СПП	Y.2250–Y.2299
Нумерация, присваивание имен и адресация	Y.2300–Y.2399
Управление сетью	Y.2400–Y.2499
Архитектура и протоколы сетевого управления	Y.2500–Y.2599
Пакетные сети	Y.2600–Y.2699
Безопасность	Y.2700–Y.2799
Обобщенная мобильность	Y.2800–Y.2899
Открытая среда операторского класса	Y.2900–Y.2999
БУДУЩИЕ СЕТИ	Y.3000–Y.3499
ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ	Y.3500–Y.3999
ИНТЕРНЕТ ВЕЩЕЙ И "УМНЫЕ" ГОРОДА И СООБЩЕСТВА	
Общие положения	Y.4000–Y.4049
Определения и терминология	Y.4050–Y.4099
Требования и сценарии использования	Y.4100–Y.4249
Инфраструктура, возможность установления соединений и сети	Y.4250–Y.4399
Структуры, архитектуры и протоколы	Y.4400–Y.4549
Услуги, приложения, вычисления и обработка данных	Y.4550–Y.4699
Управление, контроль и рабочие характеристики	Y.4700–Y.4799
Идентификация и безопасность	Y.4800–Y.4899
Анализ и оценка	Y.4900–Y.4999

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т Y.2066

Общие требования к интернету вещей

Резюме

Рекомендация МСЭ-Т Y.2066 содержит общие требования к интернету вещей (IoT). В основу этих требований положены общие сценарии использования IoT и типы участников IoT, выведенные из определения IoT, которое дано в Рекомендации МСЭ-Т Y.2060. Общие требования к IoT не зависят от области применения, под которой подразумевается область знаний или деятельности в одной конкретной экономической, коммерческой, социальной или административной сфере, например область применения на транспорте или в здравоохранении.

В настоящей Рекомендации на основе обзора IoT (Рекомендация МСЭ-Т Y.2060) устанавливаются общие требования к IoT исходя из общих сценариев использования и типов участников IoT с учетом вопросов, требующих особого внимания при формулировке требований. Кроме того, приводятся некоторые характерные сценарии использования IoT, не привязанные к областям применения. Общие требования к IoT, определяемые в настоящей Рекомендации, разделяются на следующие категории: нефункциональные требования, требования к поддержке приложений, требования к услугам, требования к связи, требования к устройствам, требования к управлению данными, а также требования к обеспечению безопасности и защите конфиденциальности.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т Y.2066	22.06.2014 года	13-я	11.1002/1000/12169

Ключевые слова

Общие требования, функциональные требования, интернет вещей (IoT), нефункциональные требования, сценарии использования

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: http://handle.itu.int/, после которого следует уникальный идентификатор Рекомендации. Например, http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

Содержание

Рекомендация МСЭ-Т Y.2066

Общие требования к интернету вещей

1 Сфера применения

Настоящая Рекомендация содержит общие требования к интернету вещей (IoT). В основу этих требований положены общие сценарии использования IoT и типы участников IoT, выведенные из определения IoT, содержащегося в [ITU-T Y.2060]. Общие требования к IoT не зависят от области применения, под которой подразумевается область знаний или деятельности в одной конкретной экономической, коммерческой, социальной или административной сфере, например область применения на транспорте или в здравоохранении.

В настоящей Рекомендации на основе обзора IoT [ITU-T Y.2060] устанавливаются общие требования к IoT исходя из общих сценариев использования и типов участников IoT с учетом вопросов, требующих особого внимания при формулировке требований. Общие требования к IoT, определяемые в настоящей Рекомендации, разделяются на следующие категории: нефункциональные требования, требования к поддержке приложений, требования к услугам, требования к связи, требования к устройствам, требования к управлению данными, а также требования к обеспечению безопасности и защите конфиденциальности.

Сфера применения настоящей Рекомендации включает следующие вопросы:

- общие сценарии использования IoT;
- участники IoT;
- вопросы, требующие особого внимания при формулировке требований;
- общие требования к IoT.

Нумерованный перечень общих требований к IoT приведен в Приложении A.

Некоторые характерные сценарии использования IoT, не привязанные к областям применения, приведены в Дополнении I.

ПРИМЕЧАНИЕ. – Регуляторные, юридические и деловые аспекты наряду с требованиями, касающимися протоколов и интерфейсов (например, в части контроля и управления IoT), выходят за рамки настоящей Рекомендации.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылки на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ в данной Рекомендации не придает ему как отдельному документу статус Рекомендации.

[ITU-T Y.2060] Рекомендация МСЭ-Т Y.2060 (2012 год), *Обзор интернета вещей*

[ITU-T Y.2091] Рекомендация МСЭ-Т Y.2091 (2011 год), *Термины и определения для сетей последующих поколений*

3 Определения

3.1 Термины, определяемые в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах.

3.1.1 приложение (application) [ITU-T Y.2091] – структурированный набор возможностей, которые обеспечивают дополнительную функциональность, поддерживаемую одной или несколькими услугами, которые могут предоставляться через интерфейс API.

3.1.2 потребитель (customer) [ITU-T Y.2091] – потребитель приобретает продукты и услуги у предприятия либо получает бесплатные предложения или услуги. Потребитель может быть физическим лицом или предприятием.

ПРИМЕЧАНИЕ. – На одного потребителя может приходиться несколько пользователей.

3.1.3 устройство (device) [ITU-T Y.2060] – применительно к интернету вещей означает элемент оборудования, который обладает обязательными возможностями осуществления связи и дополнительными возможностями считывания данных, срабатывания устройств, а также сбора, хранения и обработки данных.

3.1.4 интернет вещей (Internet of things (IoT)) [ITU-T Y.2060] – глобальная инфраструктура для информационного общества, которая обеспечивает возможность предоставления более сложных услуг путем соединения друг с другом (физических и виртуальных) вещей на основе существующих и развивающихся функционально совместимых информационно-коммуникационных технологий.

ПРИМЕЧАНИЕ 1. – Благодаря задействованию возможностей идентификации, сбора, обработки и передачи данных в интернете вещей обеспечивается наиболее эффективное использование вещей в целях предоставления услуг для всех типов приложений при одновременном выполнении требований безопасности и неприкосновенности частной жизни.

ПРИМЕЧАНИЕ 2. – В широком смысле интернет вещей можно воспринимать как концепцию, имеющую технологические и социальные последствия.

3.1.5 услуга (service) [ITU-T Y.2091] – набор функций и средств, предлагаемых поставщиком пользователю.

3.1.6 вещь (thing) [ITU-T Y.2060] – применительно к интернету вещей означает предмет физического мира (физические вещи) или информационного мира (виртуальные вещи), который может быть идентифицирован и интегрирован в сети связи.

3.2 Термины, определяемые в настоящей Рекомендации

В настоящей Рекомендации определяется следующий термин.

3.2.1 Область применения (application domain) – область знаний или деятельности в одной конкретной экономической, коммерческой, социальной или административной сфере.

ПРИМЕЧАНИЕ. – Примерами областей применения могут служить транспорт, здравоохранение и государственное управление.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

2G	Second Generation		Второе поколение
3G	Third Generation		Третье поколение
API	Application Programming Interface		Интерфейс прикладного программирования
CAN	Controller Area Network		Локальная сеть контроллеров
DSL	Digital Subscriber Line	ЦАЛ	Цифровая абонентская линия
IoT	Internet of Things		Интернет вещей
ITS	Intelligent Transportation Systems	ИТС	Интеллектуальные транспортные системы

LTE	Long Term Evolution	Долгосрочное развитие
M2M	Machine-to-Machine	Межмашинное взаимодействие
MOC	Machine Oriented Communication	Машинно-ориентированное взаимодействие
SDP	Service Delivery Platform	Платформа доставки услуг
SLA	Service Level Agreement	Соглашение об уровне обслуживания
UML	Unified Modelling Language	Унифицированный язык моделирования
Wi-Fi	Wireless Fidelity	Стандарт Wi-Fi (высокая точность воспроизведения беспроводной передачи)

5 Соглашения по терминологии

В настоящей Рекомендации

ключевые слова **"требуется, чтобы"** означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии этому документу;

ключевое слово **"рекомендуется"** означает требование, которое рекомендуется соблюдать, но это не является абсолютно необходимым, таким образом, для заявления о соответствии это требование не является обязательным;

ключевые слова **"может дополнительно"** и **"может"** означают необязательное требование, которое допустимо, но не имеет рекомендательного значения. Эти термины не означают, что вариант реализации поставщика должен обеспечивать выполнение данной функции, которая может быть дополнительно активирована оператором сети или поставщиком услуг. Это означает лишь, что поставщик может дополнительно предоставить данную функцию и по-прежнему заявлять о соответствии спецификации.

6 Общие сценарии использования IoT и участники IoT

В настоящем разделе описаны общие сценарии использования IoT и участники IoT, а также взаимосвязи сценариев и участников. Под участником IoT в настоящей Рекомендации понимается любой объект, внешний по отношению к IoT и взаимодействующий с IoT.

6.1 Общие сценарии использования

Общие сценарии использования составлены исходя из определения IoT, данного в [ITU-T Y.2060].

Согласно этому определению IoT "обеспечивает возможность предоставления более сложных услуг путем соединения друг с другом (физических и виртуальных) вещей на основе существующих и развивающихся функционально совместимых информационно-коммуникационных технологий". Отсюда следует, что цель соединения вещей друг с другом в IoT – считывание данных или обеспечение срабатывания тех или иных устройств, а также предоставление более сложных услуг. Из этого положения можно вывести два общих сценария использования: "Считывание данных или обеспечение срабатывания устройств в IoT" и "Предоставление услуг в IoT".

Примечание к определению из [ITU-T Y.2060] гласит: "Благодаря задействованию возможностей идентификации, сбора, обработки и передачи данных в IoT обеспечивается наиболее эффективное использование вещей в целях предоставления услуг для всех типов приложений при одновременном выполнении требований безопасности и неприкосновенности частной жизни". При этом предполагается, что возможности сбора и обработки данных могут быть объединены в общую категорию возможностей управления данными, а кроме того должна гарантироваться защита конфиденциальности. Таким образом можно вывести два общих сценария использования – "Управление данными в IoT "и "Защита конфиденциальности в IoT".

На рисунке 6-1 приведена модель общих сценариев использования IoT, описываемая на унифицированном языке моделирования UML (подробную информацию см. в [b-UML]). Эта модель состоит из четырех общих сценариев использования – "Считывание данных или обеспечение срабатывания устройств в IoT", "Управление данными в IoT", "Предоставление услуг в IoT" и "Защита конфиденциальности в IoT".

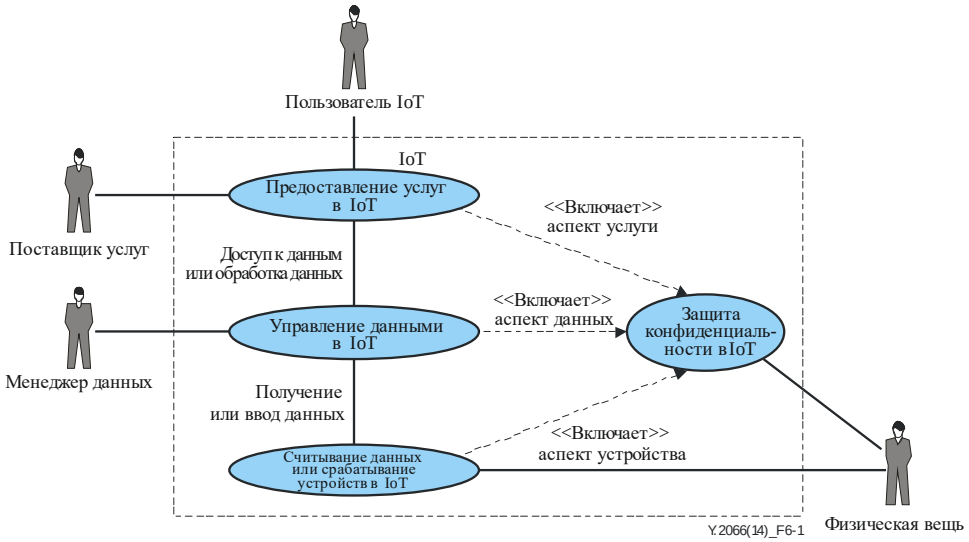

Рисунок 6-1 – Модель общих сценариев использования IoT

ПРИМЕЧАНИЕ 1. – В [b-UML] сценарий использования определяется как элементарная единица осмысленной работы в системе. Он может представлять обзор поведения, наблюдаемого объектами, которые находятся за пределами системы. Сценарии использования можно применять для сбора предъявляемых к системе требований. Модель сценариев использования (комбинация элементарных единиц работы) может иллюстрировать взаимодействие между системой и внешними объектами. Эти внешние объекты называются в UML участниками. С этой точки зрения IoT становится системой, моделируемой с помощью UML, в то время как участник IoT – это внешний объект, взаимодействующий с IoT.

ПРИМЕЧАНИЕ 2. – Некоторые сценарии использования, не связанные с приложениями IoT (характерные сценарии использования, описываемые в Дополнении I), можно разложить на общие сценарии использования, которые описаны в разделах 6.1.1–6.1.4, в целях упрощения формулировки функциональных требований, относящихся к участникам IoT. Например, описываемый в п. I.1 сценарий использования "Видеонаблюдение" можно разложить на три сценария использования: сбор видеоданных (считывание данных или срабатывание устройств в IoT), передача и хранение видеоданных (управление данными IoT), воспроизведение и анализ видеоданных (предоставление услуг в IoT). На основании этих сценариев использования можно сформулировать функциональные требования от лица различных участников видеонаблюдения, такие как временна́я синхронизация для поддержки передачи видеоданных в реальном времени и виртуальное хранилище для поддержки хранения большого объема видеоданных, поступающих с видеокамер в непрерывном режиме.

6.1.1 Сценарий использования "Считывание данных или срабатывание устройств в IoT"

Сценарий использования "Считывание данных или срабатывание устройств в IoT" имеет общий характер и может встречаться во множестве областей применения. Он предполагает установление соединений с физическими вещами, считывание данных об их состоянии или обеспечение срабатывания соответствующих устройств.

6.1.2 Сценарий использования "Управление данными в IoT"

Сценарий использования "Управление данными в IoT" имеет общий характер и может встречаться во множестве областей применения. Он предполагает сбор, передачу, хранение и обработку данных о физических вещах.

6.1.3 Сценарий использования "Предоставление услуг в IoT"

Сценарий использования "Предоставление услуг в IoT" имеет общий характер и может встречаться во множестве областей применения. Он предполагает предоставление услуг поставщиком услуг и их потребление пользователем IoT.

6.1.4 Сценарий использования "Защита конфиденциальности в IoT"

Сценарий использования "Защита конфиденциальности в IoT" имеет общий характер и может встречаться во множестве областей применения. Он предполагает защиту и скрытие конфиденциальной информации о физических вещах.

6.1.5 Взаимосвязи общих сценариев использования

Взаимосвязи общих сценариев использования показаны на рисунке 6-1. Сценарий использования "Управление данными в IoT" связан с со сценариями "Считывание данных или срабатывание устройств в IoT" и "Предоставление услуг в IoT". Сценарий использования "Защита конфиденциальности в IoT" связан со всеми остальными сценариями использования.

6.2 Типы участников IoT

Сценарии использования применяются для сбора информации о требованиях к системе (см. [b-UML]). Каждый сценарий использования включает в себя функциональные требования его участников.

В соответствии с моделью общих сценариев использования, представленной на рисунке 6-1, существует четыре типа участников IoT: физическая вещь, менеджер данных, поставщик услуг и пользователь IoT. Эти четыре типа участников, описываемые в настоящем разделе, представляют собой объекты, которые определяются вне рамок IoT и задаются применительно к их требованиям. Они отличаются от описываемых в Дополнении I к [ITU-T Y.2060] деловых ролей, которые задаются с позиций хозяйственной деятельности.

ПРИМЕЧАНИЕ 1. – Тип участника "физическая вещь", описываемый в настоящей Рекомендации, соответствует определению физической вещи, данному в [ITU-T Y.2060]. Согласно модели общих сценариев использования IoT, в настоящей Рекомендации не рассматривается тип участников, соответствующий определению виртуальной вещи в [ITU-T Y.2060], так как виртуальная вещь представляет собой объект в составе самого IoT.

ПРИМЕЧАНИЕ 2. – Типы участников IoT, описываемые в настоящей Рекомендации, и роли, описываемые в Дополнении I к [ITU-T Y.2060], могут быть сопоставлены друг с другом следующим образом:

- тип участника "пользователь IoT" соответствует роли абонента приложений;
- тип участника "поставщик услуг" соответствует ролям поставщика приложений, поставщика платформы и поставщика сети;
- тип участника "менеджер данных" соответствует роли поставщика приложений, если предоставляемые приложения содержат функциональные возможности управления данными, и может также соответствовать роли поставщика устройств, если предоставляемые устройства содержат функциональные возможности управления данными.

6.2.1 Тип участника "физическая вещь"

Физическая вещь – это такой тип участника IoT, у которого есть уникальный идентификатор в физическом мире. Взаимодействие физической вещи с IoT заключается в считывании данных или обеспечении срабатывания устройств.

ПРИМЕЧАНИЕ. – Тип участника "физическая вещь" может быть разделен на два подтипа: искусственная вещь и естественная вещь. Искусственная вещь – это изготовленная человеком физическая вещь, которую можно идентифицировать по серийному номеру изделия. Естественная вещь – это физическая вещь, которая создается природой и может быть идентифицирована, например, по времени и месту ее возникновения, а также по категории. Считывание информации применительно к естественным вещам может представлять собой трудную задачу при разработке систем IoT.

Следует обратить внимание, что в последующих разделах настоящей Рекомендации термин "вещь" употребляется как синоним термина "физическая вещь".

6.2.2 Тип участника "менеджер данных"

Менеджер данных – это тип участника IoT, отвечающий за сбор, передачу, хранение и обработку данных IoT для удовлетворения требований к предоставлению услуг IoT.

ПРИМЕЧАНИЕ. – Тип участника "менеджер данных" может быть разделен на два подтипа – человеческий и машинный. Человек – менеджер данных управляет данными IoT вручную, а машинный менеджер – автоматически. Эти два подтипа участника "Менеджер данных" связаны с различными сценариями использования, относящимися к управлению данными в IoT.

6.2.3 Тип участника "поставщик услуг"

Поставщик услуг – это тип участника IoT, предоставляющий всевозможные услуги, связанные с вещами, например мониторинг, отслеживание местоположения и обнаружение услуг.

ПРИМЕЧАНИЕ. – Тип участника "поставщик услуг" может быть разделен на два подтипа – общий, который предоставляет услуги, не зависящие от конкретных областей применения, и прикладной, который предоставляет приложения для конкретных областей применения.

6.2.4 Тип участника "пользователь IoT"

Пользователь IoT – это тип участника IoT, потребляющий всевозможные услуги, связанные с вещами, например услуги мониторинга, отслеживания местоположения и обнаружения услуг.

7 Вопросы, требующие особого внимания при формулировке требований

Существует ряд вопросов, которые требуют особого внимания при формулировке требований к IoT. Эти важные вопросы определены исходя из характеристик IoT и требований высокого уровня, описываемых в [ITU-T Y.2060], а также из результатов государственных и научных исследований по тематике IoT (например, [b-IoT-A D6.2]) и рассматриваются в следующих разделах.

7.1 Аспекты реализации и эксплуатации

Аспекты реализации и эксплуатации IoT важны для рассмотрения, например, в аспекте обеспечения функциональной совместимости между разнородными реализациями IoT, достаточной масштабируемости для поддержки большого количества подключенных устройств и высокой эксплуатационной готовности для поддержки работы IoT в автоматическом режиме.

7.2 Возможность повсеместного установления соединений

Требуется рассмотреть вопрос об обеспечении возможности повсеместного установления соединений между вещами и IoT. Эта возможность не должна зависеть от конкретных областей применения, а также необходимо обеспечить поддержку интеграции разнородных технологий связи.

7.3 Сквозное интеллектуальное обеспечение

Требуется рассмотреть вопрос о сквозном интеллектуальном обеспечении, в частности в отношении интеллектуальной связи и интеллектуальных услуг – например, для предоставления услуг без вмешательства человека. К этому вопросу относится возможность обеспечения связи на основе определения местоположения, а также контекстно зависимой связи (что можно рассматривать как интеллектуальную связь), контентно и контекстно зависимых услуг (которые можно рассматривать как интеллектуальные услуги), а также услуг автоматического конфигурирования, самовосстановления, автоматической оптимизации и автоматической защиты (которые можно отнести к разряду прочих интеллектуальных услуг, собирательно называемых автономными услугами [ITU-T Y.2060]).

7.4 Временна́я синхронизация

Чтобы обеспечить согласование во времени действий, которые выполняют соединенные друг с другом вещи при использовании ими возможностей связи и услуг, требуется рассмотреть вопрос о временной синхронизации.

7.5 Физическое взаимодействие с организмом человека

Для предоставления возможностей связи, предполагающих физическое взаимодействие с организмом человека в соответствии с требованиями законов и других нормативных актов, требуется тщательно продумать требования к такому взаимодействию. В частности требуется определить особые требования в качеству обслуживания (QoS), дать количественную характеристику надежности и обеспечить защиту конфиденциальности.

7.6 Большой объем данных, поступающих от вещей

К IoT будет подключаться большое количество устройств, поэтому объем данных, поступающих от них в IoT, также будет велик. В последнее время приобрел популярность термин "большие данные", которым обозначают большие объемы разнородных данных, поступающих с высокой скоростью от вещей в сеть IoT. Для классификации, передачи, хранения, обработки, проверки корректности и запроса больших данных в пределах временных ограничений, задаваемых пользователями или приложениями IoT, следует рассмотреть вопрос о масштабируемости таких ресурсов, как полоса пропускания каналов связи, емкость хранилищ данных и вычислительная мощность.

7.7 Защита конфиденциальности в отношении вещей

Поступающие от вещей данные могут содержать конфиденциальную информацию о владельцах или пользователях вещей. Эти данные могут использоваться для определения местонахождения владельцев или пользователей и для слежки за ними, что нарушает конфиденциальность. Поэтому следует рассмотреть вопрос о защите конфиденциальности при сборе, передаче, хранении, проверке корректности и обработке данных о вещах. Не следует однако использовать защиту конфиденциальности с целью воспрепятствовать проверке корректности указанных данных о вещах.

8 Общие требования к IoT

Общие требования к IoT, изложенные в настоящей Рекомендации, имеют технический характер и не зависят от конкретной области применения. Требования, касающиеся протоколов и интерфейсов (например, в части контроля и управления IoT), выходят за рамки настоящей Рекомендации.

8.1 Категории общих требований к IoT

В настоящей Рекомендации общие требования к IoT разделены на нефункциональные и функциональные.

Под нефункциональными требованиями к IoT понимаются требования, относящиеся к реализации и эксплуатации сети IoT как таковой.

Под функциональными требованиями понимаются требования, относящиеся к участникам IoT, то есть внешним по отношению к IoT объектам, взаимодействующим с IoT. Функциональные требования к IoT, изложенные в настоящей Рекомендации, разделяются на следующие категории:

– требования по поддержке приложений;
– требования к услугам;
– требования к связи;
– требования к устройствам;
– требования к управлению данными;
– требования к обеспечению безопасности и защите конфиденциальности.

Все требования, описываемые в следующих разделах, перечисляются и нумеруются в Приложении A. В этих разделах порядковые номера требований согласно Приложению A приводится в квадратных скобках в конце каждого абзаца, где описывается соответствующее требование.

8.2 Нефункциональные требования

Требования из этой категории не относятся к участникам IoT, так как не исходят из общих сценариев использования IoT, описываемых в разделе 6.

8.2.1 Функциональная совместимость

Требуется обеспечить функциональную совместимость между разнородными реализациями IoT [N1].

ПРИМЕЧАНИЕ. – Для поддержки функциональной совместимости в IoT необходимо стандартизировать эталонную модель архитектуры IoT.

8.2.2 Масштабируемость

Требуется обеспечить в IoT масштабируемость для работы с большим количеством устройств, приложений и множеством пользователей [N2].

ПРИМЕЧАНИЕ 1. – Требование масштабируемости для работы с большим количеством устройств подразумевает требование обеспечить возможность работы с большими объемами данных (большими данными) в IoT.

ПРИМЕЧАНИЕ 2. – Требование масштабируемости для работы с большим числом приложений и пользователей подразумевает требование предоставить большие объемы вычислительных ресурсов и хранилища большой емкости. Выполнить его можно путем интеграции облачных технологий в IoT.

ПРИМЕЧАНИЕ 3. – Следует рассмотреть вопрос о справедливой организации работы с большим количеством устройств, приложений и пользователей.

8.2.3 Надежность

Требуется обеспечить надежность предоставляемых возможностей IoT – в частности возможностей связи, услуг и управления данными [N3].

ПРИМЕЧАНИЕ. – В целях обеспечения надежности следует рассмотреть вопрос об отказоустойчивости.

8.2.4 Высокая эксплуатационная готовность

Требуется обеспечить высокую эксплуатационную готовность при оказании услуг, управлении данными, связи, считывании данных и обеспечении срабатывания устройств в составе IoT [N4].

8.2.5 Возможность адаптации

Требуется предусмотреть в IoT возможность адаптации к новым технологиям, которые могут появиться в будущем [N5].

ПРИМЕЧАНИЕ. – Технические стандарты, применяемые в сфере IoT, должны накладывать минимальные ограничения в отношении возможности адаптации к новым технологиям.

8.2.6 Управляемость

Для поддержки нормальной работы требуется обеспечить в IoT управляемость Обычно работа IoT происходит в автоматическом режиме, без вмешательства человека, но процесс работы должен быть управляемым [N6].

ПРИМЕЧАНИЕ 1. – Следует рассмотреть вопрос об управлении устройствами IoT, например управлении их состоянием, энергопотреблением, возможностью подключения к ним и т. д. При этом следует учитывать ресурсные ограничения устройств – в частности связанные с емкостью их источников автономного питания, объемом памяти и шириной полосы пропускания.

ПРИМЕЧАНИЕ 2. – Следует рассмотреть вопрос об автоматической обработке сбоев в IoT, которая может предусматривать, например, активное уведомление о сбоях, диагностику, восстановление после неисправностей и т. д.

ПРИМЕЧАНИЕ 3. – Следует рассмотреть вопрос об автоматическом управлении конфигурацией в IoT, например об автоматической настройке параметров устройств.

8.3 Требования по поддержке приложений

Под требованиями по поддержке приложений подразумеваются функциональные требования, обусловленные разработкой приложений IoT в различных областях применения. Эти требования относятся только к типу участника "поставщик услуг".

8.3.1 Программируемые интерфейсы

Требуется предусмотреть стандартные программируемые интерфейсы для предоставления открытого доступа к возможностям поддержки приложений [A1].

ПРИМЕЧАНИЕ. – Программируемые интерфейсы обеспечивают программируемую поддержку приложений IoT.

8.3.2 Управление группами

Требуется обеспечить в IoT поддержку управления группами, в частности отображение, создание, изменение и удаление групп IoT, а также отображение, добавление, изменение и удаление членов групп IoT [A2].

ПРИМЕЧАНИЕ. – Группа IoT может состоять из пользователей и/или устройств IoT.

8.3.3 Временна́я синхронизация

Требуется обеспечить надежную временну́ю синхронизацию для простановки глобальных временных меток в IoT [A3].

ПРИМЕЧАНИЕ. – Простановка временных меток обеспечивает возможность предоставления безопасных доверенных услуг, критичных ко времени.

8.3.4 Взаимодействие

Требуется предусмотреть взаимодействие в автономном режиме между услугами или устройствами, осуществляющими доступ с одной и той же целью к приложениям IoT [A4].

ПРИМЕЧАНИЕ. – Предполагается, что устройства, осуществляющие доступ к приложениям IoT, будут самостоятельно инициировать взаимодействие друг с другом – это обеспечивает масштабируемость такого взаимодействия с распределением функций управления между устройствами.

8.3.5 Управление пользователями

Требуется предусмотреть управление пользователями IoT, в том числе их создание, аутентификацию, авторизацию и учет [A5].

8.3.6 Учет потребления ресурсов

Требуется предусмотреть учет потребления ресурсов IoT отдельно для каждого приложения [A6].

8.4 Требования к услугам

Эти требования относятся к участникам типа "поставщик услуг", "пользователь IoT" и "вещь".

ПРИМЕЧАНИЕ. – Согласно общему определению услуги как набора функций и средств, предлагаемых поставщиком пользователю [ITU-T Y.2091], требования к услугам распространяются как на пользователей, так и на поставщиков услуг IoT. Это не исключает того, что услуга может предлагаться непосредственно участнику типа "вещь".

8.4.1 Ранжирование услуг по приоритетам

В целях удовлетворения различных требований к услугам, предъявляемых различными группами пользователей IoT, требуется предусмотреть ранжирование услуг по приоритетам [S1].

ПРИМЕЧАНИЕ. – Предполагается поддержка дифференцированных услуг, чтобы в рамках IoT можно было реализовывать разные соглашения об уровне обслуживания (SLA).

8.4.2 Услуги на семантической основе

Требуется предусмотреть в IoT услуги на семантической основе для поддержки автономного предоставления услуг. Механизмы реализации услуг на семантической основе включают семантическую аннотацию, семантический доступ к услугам и обмен семантическими данными между услугами [S2].

ПРИМЕЧАНИЕ. – Семантическая аннотация услуг обеспечивает возможность их семантического описания. Семантический доступ к услугам может применяться для обращения к услугам через

семантические интерфейсы. Обмен семантическими данными между услугами – это механизм, позволяющий услугам предоставлять семантические данные и обмениваться ими для поддержки автоматического создания новых услуг.

8.4.3 Составные услуги

Требуется предусмотреть формирование составных услуг для поддержки гибкого создания услуг в IoT [S3].

ПРИМЕЧАНИЕ 1. – Элементарные услуги – это набор базовых операций, которые не позволяют непосредственно удовлетворить некоторые требования приложений IoT. Формирование составных услуг может применяться в качестве одного из методов автоматического создания более сложных услуг на базе элементарных услуг для удовлетворения всевозможных требований, предъявляемых приложениями IoT.

ПРИМЕЧАНИЕ 2. – Потребности в составных услугах могут, среди прочего, обеспечиваться существующими технологиями гибкого предоставления услуг, такими как платформа доставки услуг (SDP).

8.4.4 Услуги мобильности

Требуется предусмотреть услуги мобильности для поддержки в IoT мобильности услуг, пользователей и устройств с точки зрения предоставления услуг. Пример: в условиях, когда поддерживается мобильность услуг, предоставление услуги не ограничивается местом первоначального доступа к обслуживанию [S4].

8.4.5 Надежность и безопасность услуг, предполагающих физическое взаимодействие с организмом человека

При предоставлении услуг, предполагающих физическое взаимодействие с организмом человека, требуется обеспечить высокий уровень надежности и безопасности [S5].

ПРИМЕЧАНИЕ. – В разных странах требования законов и других нормативных актов к этим услугам могут различаться.

8.4.6 Автономные услуги

Требуется предусмотреть в IoT автономные услуги для поддержки автоматического сбора, передачи и обработки данных о вещах на основании правил, составленных поставщиками услуг или настроенных в индивидуальном порядке пользователями IoT [S6].

ПРИМЕЧАНИЕ. – Предполагается поддержка как централизованного, так и децентрализованного управления автономными услугами, чтобы обеспечить в IoT возможность централизованных и децентрализованных действий в автоматическом режиме.

Требуется предусмотреть услуги на основе определения местоположения, а также контекстно зависимые услуги, чтобы сделать возможным предоставление в IoT гибких, настраиваемых пользователями и автономных услуг на основании информации о местоположении и соответствующего контекста, в котором работают вещи и/или действуют пользователи [S7].

8.4.7 Управление услугами

Требуется предусмотреть управление услугами для поддержки предоставления услуг с высоким уровнем эксплуатационной готовности и надежности [S8].

ПРИМЕЧАНИЕ. – К управлению услугами, среди прочего, относится управление жизненным циклом услуг и проверка целостности услуг. Управление жизненным циклом услуг может помочь в повышении их эксплуатационной готовности, а проверка целостности – в повышении надежности их предоставления.

8.4.8 Услуги обнаружения

Требуется предусмотреть услуги обнаружения, чтобы обеспечить возможность обнаружения поставщиками услуг или пользователями IoT пользователей, услуг, устройств и данных о вещах [S9].

ПРИМЕЧАНИЕ. – Поставщик услуг или пользователь IoT может обнаруживать конкретных пользователей, услуги, устройства и данные о вещах по различным критериям, таким как географическое местоположение, тип устройства и так далее.

8.4.9 Поддержка абонирования услуг

Требуется предусмотреть поддержку абонирования услуг, чтобы сеть IoT могла предоставить пользователю IoT возможность абонирования необходимых ему услуг и соответствующих данных о вещах [S10].

8.4.10 Именование и адресация

Требуется предусмотреть стандартизированные способы именования и адресации вещей и услуг [S11].

8.4.11 Виртуальное хранение и обработка

Требуется предусмотреть возможности виртуального хранения и обработки для поддержки хранения и обработки больших объемов данных (больших данных) [S12].

8.5 Требования к связи

Под требованиями к связи подразумеваются функциональные требования, относящиеся к обмену сообщениями между пользователем, поставщиком услуг, менеджером данных и вещами в IoT. Эти требования распространяются на все действующие объекты IoT.

8.5.1 Режимы связи

Требуется обеспечить поддержку режимов связи на основе событий, периодической связи и автоматической связи между устройствами или между пользователями IoT [C1].

Требуется обеспечить поддержку режима одноадресной связи (например, связи между пользователями или устройствами IoT). Требуется обеспечить поддержку режимов многоадресной связи, широковещательной связи и связи с любым устройством группы, чтобы сделать возможным в IoT предоставление различных услуг связи внутри группы пользователей или устройств IoT (например, для поддержки взаимодействия между пользователями или устройствами IoT) [C2].

ПРИМЕЧАНИЕ. – Рекомендуется обеспечить поддержку режимов связи на основе событий, периодической и автоматической связи между устройствами или между пользователями IoT без потерь в производительности сети за счет реализации механизмов предотвращения возможности перегрузки сети.

Требуется обеспечить поддержку связи, инициируемой устройством для удовлетворения требований автоматической связи [C3].

8.5.2 Управление связью

Требуется обеспечить поддержку обнаружения и исправления ошибок в процессе связи, чтобы сделать возможным, например, сохранение работоспособности IoT в условиях помех между устройствами [C4].

Требуется обеспечить поддержку связи, критичной по времени, чтобы сделать возможной в IoT обработку и доставку критичных по времени сообщений [C5].

8.5.3 Интеллектуальная связь

Требования к интеллектуальной связи включают требования к организации автономных сетей [ITU-T Y.2060], контентно зависимой связи и связи на основе определения местоположения.

Требуется предусмотреть в IoT организацию автономных сетей для поддержки возможностей автоматического конфигурирования, самовосстановления, автоматической оптимизации и автоматической защиты на сетевом уровне для адаптации к различным областям применения и средам связи, а также большому количеству разнотипных устройств [C6].

Требуется предусмотреть контентно зависимую связь, чтобы, например, обеспечить в IoT поддержку выбора маршрута связи в зависимости от контента [C7].

Требуется предусмотреть связь на основе определения местоположения, чтобы обеспечить в IoT поддержку взаимодействий между участниками IoT, зависящих от их местоположения [C8].

ПРИМЕЧАНИЕ. – Предполагается автоматический сбор и отслеживание информации о местоположении.

8.5.4 Поддержка разнородных технологий связи

Связь может осуществляться на уровне устройств (см. [ITU-T Y.2060]) с применением разнообразных проводных или беспроводных технологий, таких как шина локальной сети контроллеров (CAN), ZigBee, Bluetooth, Wi-Fi и т. д. Требуется обеспечить поддержку разнородных технологий связи на уровне устройств [C9].

Связь может осуществляться на сетевом уровне (см. [ITU-T Y.2060]) с применением разнообразных технологий, таких как второе поколение/третье поколение (2G/3G), долгосрочное развитие (LTE), Ethernet, цифровая абонентская линия (DSL) и т. д.

Требуется обеспечить поддержку разнородных технологий связи на сетевом уровне [C10].

8.6 Требования к устройствам

Под требованиями к устройствам подразумеваются функциональные требования к элементам оборудования, соединенным с вещами. Эти требования относятся к участникам типа "пользователь IoT" и "вещь".

8.6.1 Возможность установления соединений с вещами

Требуется обеспечить в IoT поддержку установления соединений между вещью и IoT на основании идентификатора этой вещи [D1].

ПРИМЕЧАНИЕ. – Предполагается унифицированная обработка разнородных идентификаторов вещей (см. [ITU-T Y.2060]).

8.6.2 Управление устройствами и конфигурирование устройств

Требуется обеспечить поддержку удаленного мониторинга, управления и конфигурирования устройств в целях повышения степени управляемости устройств в IoT [D2].

Требуется обеспечить поддержку автоматического конфигурирования в IoT, чтобы сделать возможным оперативное создание, формирование или получение основанных на семантике конфигураций для бесшовной интеграции и взаимосвязи вещей с приложениями, а также для удовлетворения требований приложений (см. [ITU-T Y.2060]) [D3].

8.6.3 Мониторинг вещей

Требуется предусмотреть автоматическое уведомление о состоянии вещей и его изменениях для оперативного мониторинга вещей [D4].

8.6.4 Мобильность устройств

Требуется предусмотреть мобильность устройств для поддержки в IoT мобильности вещей, соединенных с устройствами [D5].

8.6.5 Проверка целостности устройств

Требуется предусмотреть проверку целостности устройств для содействия обеспечению их высокой эксплуатационной готовности [D6].

8.7 Требования к управлению данными

Под требованиями к управлению данными подразумеваются функциональные требования к хранению, агрегированию, передаче и обработке данных IoT. Эти требования относятся к участникам типа "менеджер данных" и "пользователь IoT".

8.7.1 Хранение данных

Требуется обеспечить поддержку хранения данных о вещах на основе предопределенных правил и общих принципов [DM1].

8.7.2 Обработка данных

Требуется обеспечить поддержку слияния и интеллектуального анализа поступающих от вещей данных на основе предопределенных правил и общих принципов [DM2].

8.7.3 Запрос данных

Требуется обеспечить поддержку запроса хранящихся ретроспективных данных о вещах, чтобы сделать возможным предоставление в IoT информации о вещах за предшествующие периоды времени [DM3].

8.7.4 Контроль доступа к данным

Требуется обеспечить в IoT поддержку контроля доступа владельца данных к своим данным, чтобы пользователи IoT могли контролировать доступ к их данным со стороны других пользователей IoT [DM4].

8.7.5 Обмен данными

Требуется обеспечить поддержку обмена данными с объектами, находящимися за пределами IoT, чтобы сделать возможным предоставление в IoT доступа к внешним источникам данных, например медицинским базам данных за пределами IoT [DM5].

8.7.6 Проверка корректности данных

Требуется обеспечить поддержку проверки целостности и управления жизненным циклом данных о вещах для обеспечения в IoT высокого уровня готовности и надежности этих данных [DM6].

8.7.7 Семантическая аннотация данных о вещах и семантический доступ к этим данным

Требуется предусмотреть семантическую аннотацию данных о вещах. Требуется предусмотреть семантический доступ к данным о вещах для поддержки автоматического запроса этих данных [DM7].

8.7.8 Хранение, передача и агрегирование данных о вещах на семантической основе

Требуется предусмотреть хранение, передачу и агрегирование данных о вещах на семантической основе, чтобы обеспечить возможность автоматического хранения, передачи и агрегирования этих данных в соответствии с требованиями пользователей или приложений IoT [DM8].

8.8 Требования к обеспечению безопасности и защите конфиденциальности

Под требованиями безопасности и защиты конфиденциальности понимаются функциональные требования, предъявляемые в процессе сбора, хранения, передачи, агрегирования и обработки данных о вещах, а также оказания услуг с использованием вещей. Эти требования распространяются на всех участников IoT.

8.8.1 Безопасность связи

Требуется предусмотреть возможность надежной связи с обеспечением безопасности и защиты конфиденциальности, с тем чтобы предотвратить несанкционированный доступ к содержимому данных, гарантировать целостность данных и защитить их конфиденциальное содержимое при передаче или переносе данных в среде IoT [SP1].

8.8.2 Безопасность управления данными

Требуется предусмотреть возможность надежного управления данными с обеспечением безопасности и защиты их конфиденциальности, с тем чтобы предотвратить несанкционированный доступ к содержимому данных, гарантировать целостность данных и защитить их конфиденциальное содержимое при хранении или обработке данных в среде IoT [SP2].

8.8.3 Безопасность предоставления услуг

Требуется предусмотреть возможность надежного предоставления услуг с обеспечением безопасности и защиты конфиденциальности, с тем чтобы предотвратить несанкционированный доступ к услугам и оказание услуг в мошеннических целях, а также защитить конфиденциальную информацию, касающуюся пользователей IoT [SP3].

8.8.4 Интеграция общих принципов и методов обеспечения безопасности

Требуется предусмотреть возможность интеграции различных принципов и методов обеспечения безопасности, с тем чтобы обеспечить единообразное управление безопасностью разнородных устройств и пользовательских сетей в среде IoT [SP4].

8.8.5 Взаимная аутентификация и авторизация

Прежде чем предоставлять устройству (или пользователю IoT) доступ к IoT, требуется провести взаимную аутентификацию и авторизацию между устройством (или пользователем IoT) и IoT в соответствии с заранее установленными общими принципами обеспечения безопасности [SP5].

8.8.6 Аудит безопасности

Требуется, чтобы в IoT поддерживался аудит безопасности. Необходимо обеспечить полную прозрачность, прослеживаемость и воспроизводимость любого доступа к данным или попыток доступа к приложениям IoT согласно соответствующим нормативными актам и законам. В частности IoT должен поддерживать аудит безопасности в отношении передачи, хранения и обработки данных, а также доступа к приложениям [SP6].

Приложение A

Перечень общих требований к IoT

(Данное Приложение является неотъемлемой частью настоящей Рекомендации)

В приведенной ниже таблице сведены и пронумерованы требования, описываемые в разделе 8 "Общие требования к IoT".

Номер требования	Категория требования	Описание требования	Краткое изложение требования
N1	Нефункци-ональные требования	Требуется обеспечить функциональную совместимость между разнородными реализациями IoT	Требуется функциональная совместимость
N2	Нефункци-ональные требования	Требуется обеспечить в IoT масштабируемость для работы с большим количеством устройств, приложений и пользователей	Требуется масштабируемость
N3	Нефункци-ональные требования	Требуется обеспечить надежность в плане возможностей IoT – в частности надежность связи, услуг и управления данными	Требуется надежность
N4	Нефункци-ональные требования	Требуется обеспечить в IoT высокую эксплуатационную готовность при предоставлении услуг, управлении данными, связи, считывании данных и обеспечении срабатывания устройств	Требуется высокая эксплуатационная готовность
N5	Нефункци-ональные требования	Требуется предусмотреть в IoT возможность адаптации к новым технологиям, которые могут появиться в будущем	Требуется возможность адаптации
N6	Нефункци-ональные требования	Требуется предусмотреть в IoT управляемость для обеспечения нормальной работы	Требуется управляемость
A1	Требования по поддержке приложений	Требуется предусмотреть процедуру стандартизации программируемых интерфейсов для предоставления открытого доступа к возможностям поддержки приложений	Требуются стандартизованные программируемые интерфейсы
A2	Требования по поддержке приложений	Требуется предусмотреть в IoT поддержку управления группами, в частности отображение, создание, изменение и удаление групп IoT, а также отображение, добавление, изменение и удаление членов групп IoT	Требуется управление группами
A3	Требования по поддержке приложений	Требуется обеспечить надежную временну́ю синхронизацию для простановки глобальных временных меток в IoT	Требуется надежная временна́я синхронизация
A4	Требования по поддержке приложений	Требуется предусмотреть взаимодействие между услугами или устройствами, осуществляющими доступ с одной и той же целью к приложениям IoT	Требуется взаимодействие

Номер требования	Категория требования	Описание требования	Краткое изложение требования
A5	Требования по поддержке приложений	Требуется предусмотреть управление пользователями IoT, в том числе их создание, аутентификацию, авторизацию и учет	Требуется управление пользователями
A6	Требования по поддержке приложений	Требуется предусмотреть учет потребления ресурсов IoT отдельно для каждого приложения	Требуется учет потребления ресурсов
S1	Требования к услугам	В целях удовлетворения различных требований к услугам, предъявляемых различными группами пользователей IoT, требуется предусмотреть ранжирование услуг по приоритетам	Требуется ранжирование услуг по приоритетам
S2	Требования к услугам	Требуется предусмотреть в IoT услуги на семантической основе для поддержки автономного предоставления услуг	Требуются услуги на семантической основе
S3	Требования к услугам	Требуется предусмотреть составные услуги для поддержки гибкого создания услуг в IoT	Требуется формирование составных услуг
S4	Требования к услугам	Требуется предусмотреть услуги мобильности для поддержки мобильности услуг, пользователей и устройств в IoT	Требуются услуги мобильности
S5	Требования к услугам	При предоставлении услуг, предполагающих физическое взаимодействие с организмом человека, требуется обеспечить высокий уровень надежности и безопасности	Требуется высокий уровень надежности и безопасности услуг, предполагающих физическое взаимодействие с организмом человека
S6	Требования к услугам	Требуется предусмотреть в IoT автономные услуги для поддержки автоматического сбора, передачи и обработки данных о вещах на основе правил, заданных поставщиками услуг или созданных в индивидуальном порядке пользователями IoT	Требуются автономные услуги
S7	Требования к услугам	Требуется предусмотреть услуги на основе местоположения, а также контекстно зависимые услуги, чтобы сделать возможным предоставление в IoT гибких, заказываемых пользователями и автономных услуг на основе информации о местоположении и соответствующего контекста работы вещей и/или пользователей	Требуются услуги на основе местоположения и контекстно зависимые услуги
S8	Требования к услугам	Требуется предусмотреть управление услугами для поддержки предоставления услуг с высоким уровнем эксплуатационной готовности и надежности	Требуется управление услугами

Номер требования	Категория требования	Описание требования	Краткое изложение требования
S9	Требования к услугам	Требуется предусмотреть услуги обнаружения, чтобы обеспечить возможность обнаружения поставщиками услуг или пользователями IoT пользователей, услуг, устройств и данных о вещах в IoT	Требуются услуги обнаружения
S10	Требования к услугам	Требуется предусмотреть абонирование услуг, чтобы предоставить IoT средство, позволяющее пользователю IoT абонировать нужные ему услуги и получать соответствующие данные о вещах	Требуется поддержка абонирования услуг
S11	Требования к услугам	Требуется предусмотреть стандартизованные способы именования и адресации вещей и услуг	Требуются стандартизованные способы именования и адресации
S12	Требования к услугам	Требуется предусмотреть возможности виртуального хранения и обработки для поддержки хранения и обработки больших объемов данных (больших данных)	Требуются возможности виртуального хранения и обработки
C1	Требования к связи	Требуется обеспечить в IoT поддержку связи на основе событий, периодической и автоматической связи между устройствами или между пользователями IoT	Требуется поддержка режимов связи на основе событий, периодической связи и автоматической связи
C2	Требования к связи	Требуется обеспечить поддержку режима одноадресной связи (например, связи между пользователями или устройствами IoT). Требуется обеспечить поддержку режимов многоадресной, широковещательной связи и связи с любыми устройствами, чтобы сделать возможным в IoT предоставление различных услуг связи внутри группы пользователей или устройств IoT (например, для поддержки взаимосвязи между пользователями или устройствами IoT)	Требуется поддержка режимов одноадресной, многоадресной, широковещательной связи и связи с любыми устройствами
C3	Требования к связи	Требуется обеспечить поддержку связи, инициируемой устройствами для удовлетворения требований автоматической связи	Требуется поддержка связи, инициируемой устройствами
C4	Требования к связи	Требуется обеспечить поддержку функции обнаружения и исправления ошибок, чтобы сеть IoT могла, например, справляться с проблемами помех между устройствами	Требуется поддержка функции обнаружения и исправления ошибок связи
C5	Требования к связи	Требуется обеспечить в IoT обработку и доставку критичных по времени сообщений	Требуется поддержка критичной по времени связи

Номер требования	Категория требования	Описание требования	Краткое изложение требования
C6	Требования к связи	Требуется предусмотреть в IoT возможности автоматического конфигурирования, самовосстановления, автоматической оптимизации и автоматической защиты на сетевом уровне	Требуется организация автономных сетей
C7	Требования к связи	Требуется предусмотреть контентно зависимую связь, чтобы, например, обеспечить в IoT поддержку выбора трассы/маршрута связи в зависимости от контента	Требуется контентно зависимая связь
C8	Требования к связи	Требуется обеспечить в IoT поддержку взаимодействий между участниками IoT на основе местоположения	Требуется связь на основе местоположения
C9	Требования к связи	Связь может осуществляться на уровне устройств (см. [ITU-T Y.2060]) с применением разнообразных проводных и беспроводных технологий, таких как шина локальной сети контроллеров (CAN), ZigBee, Bluetooth, Wi-Fi и т. д.	Требуется поддержка разнородных технологий связи на уровне устройств
C10	Требования к связи	Связь может осуществляться на сетевом уровне (см. [ITU-T Y.2060]) с применением разнообразных технологий, таких как второе поколение/третье поколение (2G/3G), долгосрочное развитие (LTE), Ethernet, цифровая абонентская линия (DSL) и т. д.	Требуется поддержка разнородных технологий связи на сетевом уровне
D1	Требования к устройствам	Требуется обеспечить в IoT поддержку установления соединений между вещью и IoT на основании идентификатора этой вещи	Требуется возможность установления соединений между вещью и IoT на основе идентификации
D2	Требования к устройствам	Требуется обеспечить поддержку удаленного мониторинга, управления и конфигурирования устройств в целях повышения управляемости устройств в IoT	Требуется удаленный мониторинг, управление и конфигурирование устройств
D3	Требования к устройствам	Требуется обеспечить поддержку автоматического конфигурирования в IoT, чтобы сделать возможным оперативное создание основанных на семантике конфигураций устройств	Требуется возможность автоматического конфигурирования
D4	Требования к устройствам	Требуется предусмотреть автоматическое уведомление о состоянии вещей и его изменениях для своевременного мониторинга вещей	Требуется своевременный мониторинг вещей
D5	Требования к устройствам	Требуется обеспечить в IoT поддержку мобильности вещей	Требуется мобильность устройств
D6	Требования к устройствам	Требуется предусмотреть проверку целостности устройств для поддержки высокой эксплуатационной готовности устройств	Требуется проверка целостности устройств

Номер требования	Категория требования	Описание требования	Краткое изложение требования
DM1	Требования к управлению данными	Требуется обеспечить поддержку хранения данных о вещах на основе предопределенных правил и общих принципов	Требуется поддержка хранения данных о вещах
DM2	Требования к управлению данными	Требуется обеспечить поддержку слияния и интеллектуального анализа данных на основе предопределенных правил и общих принципов	Требуется поддержка обработки данных о вещах
DM3	Требования к управлению данными	Требуется предусмотреть в IoT предоставление информации о вещах за предшествующие периоды времени	Требуется поддержка запроса ретроспективных данных о вещах
DM4	Требования к управлению данными	Требуется обеспечить в IoT поддержку контроля доступа владельца данных к своим данным, чтобы пользователи IoT могли контролировать доступ к их данным со стороны других пользователей IoT	Требуется поддержка контроля доступа владельцев данных к своим данным
DM5	Требования к управлению данными	Требуется предусмотреть в IoT предоставление доступа к внешним источникам данных, например медицинским базам данных за пределами IoT	Требуется поддержка обмена данными с объектами, находящимися за пределами IoT
DM6	Требования к управлению данными	Требуется обеспечить поддержку проверки целостности и управления жизненным циклом данных о вещах для обеспечения в IoT высокого уровня готовности и надежности этих данных	Требуется проверка целостности и управление жизненным циклом данных о вещах
DM7	Требования к управлению данными	Требуется предусмотреть семантическую аннотацию данных о вещах. Требуется предусмотреть семантический доступ к данным о вещах для поддержки автоматических запросов этих данных	Требуется семантическая аннотация данных о вещах и семантический доступ к этим данным
DM8	Требования к управлению данными	Требуется обеспечить возможность автоматического хранения, передачи и агрегирования данных о вещах в соответствии с требованиями пользователей или приложений IoT	Требуются хранение, передача и агрегирование данных о вещах на семантической основе
SP1	Требования к обеспечению безопасности и защите конфиден-циальности	Требуется предусмотреть в IoT возможность надежной связи с обеспечением безопасности и защитой конфиденциальности	Требуется обеспечить безопасность связи
SP2	Требования к обеспечению безопасности и защите конфиден-циальности	Требуется предусмотреть в IoT возможность надежного управления данными с обеспечением безопасности и защитой конфиденциальности	Требуется обеспечить безопасность управления данными
SP3	Требования к обеспечению безопасности и защите конфиден-циальности	Требуется предусмотреть в IoT возможность надежного предоставления услуг с обеспечением безопасности и защитой конфиденциальности	Требуется обеспечить безопасность предоставления услуг

Номер требования	Категория требования	Описание требования	Краткое изложение требования
SP4	Требования к обеспечению безопасности и защите конфиден-циальности	Требуется предусмотреть возможность интеграции различных принципов и методов обеспечения безопасности для разнородных устройств и пользовательских сетей в среде IoT	Требуется интеграция различных принципов и методов обеспечения безопасности
SP5	Требования к обеспечению безопасности и защите конфиден-циальности	Прежде чем предоставлять устройству (или пользователю IoT) доступ к IoT, требуется провести взаимную аутентификацию и авторизацию в соответствии с заранее установленными общими принципами обеспечения безопасности	Требуется взаимная аутентификация и авторизация
SP6	Требования к обеспечению безопасности и защите конфиден-циальности	Требуется обеспечить полную прозрачность, прослеживаемость и воспроизводимость любого доступа к данным или попыток доступа к приложениям IoT, как того требуют применимые нормативные акты и законы	Требуется поддержка в IoT аудита безопасности

Дополнение I

Характерные сценарии использования IoT

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

В данном Дополнении описываются некоторые характерные сценарии использования IoT, которые аннотируются и классифицируются на основе сценариев использования приложений в тех или иных областях применения или на стыке областей применения.

I.1 Видеонаблюдение

Видеонаблюдение – это типичный класс сценариев использования, присутствующий в многочисленных приложениях IoT. Например, в приложениях "умный город" видеокамеры применяются для слежения за перемещениями людей в целях безопасности. При контроле загрязнения окружающей среды видеонаблюдение позволяет зафиксировать потоки загрязненной воды из канализационных стоков предприятия. В больницах осуществляется дистанционное видеонаблюдение за состоянием пациентов.

Как правило, видеонаблюдение требует большого объема ресурсов – например, широкой полосы пропускания канала связи для передачи видеоинформации, хранилищ большой емкости для хранения копий видеозаписи и мощных процессоров для поиска и обработки видеоданных.

I.2 Экстренное оповещение

Экстренное оповещение – это обобщение из большого количества конкретных сценариев использования. Примерами могут служить передача тревожного сообщения о развитии у пациента сердечного приступа, оповещения о возможном скором отказе или об уже случившемся отказе транспортного средства, оповещения о произошедшем дорожно-транспортном происшествии или предупреждающего сообщения при превышении порогового значения артериального давления у пациента.

Такие сценарии использования требуют высокоприоритетной и надежной передачи данных с минимальной задержкой, а также требуют обеспечения возможностей связи, инициируемой самим устройством.

I.3 Сбор данных

Этот класс сценариев использования включает в себя целый ряд сценариев – например, учет потребления газа, воды и электроэнергии, мониторинг качества воды, передачу данных от терминалов по продаже автобусных билетов и т. д. Данные во всех этих случаях передаются через регулярные интервалы времени.

Эти сценарии использования требуют механизмов для обеспечения периодической передачи данных. Передача может инициироваться автоматически в соответствии с заданной процедурой. Как правило, в большинстве этих сценариев использования пропускная способность канала передачи данных низкая.

I.4 Дистанционное управление

К этому классу сценариев использования относятся сценарии из нескольких областей применения – в частности это домашняя автоматизация, производство и интеллектуальные транспортные системы (ИТС). В этих случаях приложение IoT требует обеспечения возможности для пользователя управлять устройствами дистанционно.

Данные для удаленного управления устройствами в таких сценариях использования передаются с перерывами и необязательно через регулярные интервалы времени. Эти сценарии использования требуют механизмов, позволяющих устанавливать соединения между контроллерами и удаленными устройствами по инициативе контроллеров или устройств только тогда, когда требуется передача данных.

I.5 Передача информации о событиях между различными областями применения

Во многих приложениях IoT, таких как "умные" города и управление операциями в случае экстренных ситуаций, информация о событиях, зарегистрированных в одной области применения, передается в другие соответствующие области применения. На основании переданной таким образом информации о событиях различные приложения могут работать в совместном режиме, обеспечивая предоставление более широкого ассортимента функций и услуг, нежели тот, который существует в одной области применения. Примерами таких сценариев использования может служить передача информации о событиях между приложениями для обслуживания дорог и мостов, приложениями для управления дорожным движением и для вождения автомобилей, приложениями для прогнозирования погоды и для предотвращения наводнений и т. д.

В этих сценариях использования требуется, чтобы события описывались в стандартизованном формате, который воспринимается различными приложениями IoT. Кроме того, следует обеспечить надежную и безопасную передачу информации о событиях.

I.6 Совместное использование данных в различных областях применения

Некоторые данные весьма важны не только в том приложении IoT, где они собираются, но и в других приложениях IoT. К ним относятся данные о географическом местоположении, дорожном движении и т. д. В соответствии с применимыми законами и другими нормативными актами может быть организовано совместное использование таких данных в различных областях применения, что позволяет предоставлять более широкий ассортимент функций и услуг. Например, данные о географическом местоположении мобильных телефонов могут использоваться для расчета параметров дорожного движения.

В этих сценариях использования необходимо иметь стандартизованные форматы представления данных из различных областей применения IoT, чтобы эти данные можно было совместно использовать в разных областях применения.

I.7 Интегрированный центр оперативного управления "умным" городом

"Умные" города на базе инфраструктуры IoT становятся все более актуальной тенденцией градоустройства по всему миру. В будущем таким городам понадобится интеллектуальная "мозговая" система для анализа различных видов данных, собираемых устройствами IoT, принятия решений по результатам произведенного анализа и выполнения других связанных с этим действий. Такую "мозговую" систему можно назвать интегрированным центром оперативного управления "умным" городом.

Для работы такого центра требуется прежде всего совместное использование, агрегирование и обработка данных в различных областях применения. Например, для практической реализации подобного центра обычно требуется интегрировать сбор данных о состоянии городской инфраструктуры в реальном времени с мониторингом событий, анализом данных, интеллектуальным ранним предупреждением и информированием, интеллектуальным принятием решений, а также интегрированным управлением и диспетчеризацией.

I.8 Развернутое описание конкретного сценария использования – сбор информации о дорожно-транспортном происшествии

Пусть станция ИТС (ИТС-С) на борту транспортного средства, непосредственно вовлеченного в дорожно-транспортное происшествие (ДТП) или случайно проезжающего мимо, обнаруживает, что произошло столкновение, и автоматически запускает процесс извещения о ДТП. Эта станция предпринимает попытку соединения со средой IoT и затем передает ей извещение. Система IoT принимает и проверяет присланное извещение, а результаты его анализа передаются абонентам соответствующей службы, например в полицейский участок и отделение службы спасения.

Абоненты соответствующей службы могут запросить у сети IoT дополнительные сведения о происшествии. Сеть IoT получает эти запросы и затем поручает станциям ИТС собрать дополнительную информацию в соответствии с полученными запросами от абонентов. Станции ИТС, находящиеся поблизости от места ДТП, принимают, проверяют, анализируют и выполняют полученные команды – например, делают фотографии, регистрируют текущее состояние дорожного

движения, составляют отчеты, подписывают их и передают подписанные отчеты в IoT. Сеть IoT собирает и проверяет отчеты, переданные станциями ИТС, и затем составляет отчет с визуальной информацией о месте ДТП для службы спасения и отчет о дорожной обстановке вблизи от места ДТП. Эти отчеты снова передаются в отделение службы спасения и в полицейский участок соответственно.

В службе спасения анализируется отчет о месте ДТП и вырабатывается конкретный план спасательных мероприятий. В полицейском участке анализируется отчет о дорожной обстановке и вырабатывается конкретный план мероприятий по управлению дорожным движением.

Этот сценарий использования требует предоставления возможностей связи, инициируемой самим устройством, надежной и безопасной связи, а также взаимодействия различных приложений на основе конкретных событий.

Библиография

[b-ITU-T Y.2061] Рекомендация МСЭ-Т Y.2061 (2012 год), *Требования к поддержке приложений машинно-ориентированной связи в среде сетей последующих поколений*

[b-IoT-A D6.2] The Internet of Things Architecture – IoT-A (2011), *Project Deliverable D6.2 – Updated Requirements List*. http://www.iot-a.eu/public/public-documents/documents-1

[b-UML] ISO/IEC 19505-2:2012, *Information technology – Object Management Group Unified Modeling Language (OMG UML) – Part 2: Superstructure*. http://www.iso.org/iso/catalogue_detail.htm?csnumber=52854

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Оконечное оборудование, субъективные и объективные методы оценки
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных, взаимосвязь открытых систем и безопасность
Серия Y	**Глобальная информационная инфраструктура, аспекты межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города**
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2019 г.