Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Y.2074

(01/2015)

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

Сети последующих поколений – Структура и функциональные модели архитектуры

Требования к устройствам интернета вещей и функционированию приложений интернета вещей в условиях бедствия

Рекомендация МСЭ-Т Y.2074

ITU-T

ITU Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Y

**ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА,
АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ**

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 СПП	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
Будущие 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

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

Рекомендация МСЭ-Т Y.2074

Требования к устройствам интернета вещей и функционированию приложений интернета вещей в условиях бедствия

Резюме

В Рекомендации МСЭ-Т Y.2074 приведены требования к устройствам интернета вещей (IoT), используемым для функционирования приложений IoT, в контексте бедствий, в дополнение к общим требованиям к IoT, изложенным в Рекомендации МСЭ-Т Y.2066. В Рекомендации также содержатся требования к функционированию приложений IoT в условиях бедствий.

Данные требования должны быть определены для использования устройств и приложений IoT во время бедствий при эвакуации и спасательных операциях.

В Дополнении I описаны методы обеспечения целостности и достоверности данных, полученных с помощью устройств IoT во время бедствия.

Настоящая Рекомендация актуальна для разработчиков приложений IoT и поставщиков услуг IoT, а также для аварийно-спасательных служб.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т Y.2074	13.01.2015 г.	13-я	11.1002/1000/12421

Ключевые слова

Бедствие, интернет вещей (IoT), приложение IoT, устройство IoT, требования, системы безопасности.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: http://handle.itu.int/, после которого укажите 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

Введение

Все новые информационно-коммуникационные технологии (ИКТ) предназначены для того, чтобы быть для пользователей полезными и применяемыми. Это означает, что даже в условиях бедствия ИКТ должны служить для поддержки в спасении пользователей в опасных ситуациях. В реальности пользователи зачастую не имеют времени на ожидание команды спасателей или помощь извне. В этих случаях единственное выход для пользователей заключается в том, чтобы действовать самостоятельно и пытаться покинуть зону бедствия как можно скорее. Следовательно, необходимо разработать требования к устройствам интернета вещей (IoT), а также требования к функционированию приложений IoT в условиях бедствия независимо от обычной работы этих приложений. На самом деле приложения IoT обычно становятся практически бесполезными во время бедствий, когда первоочередной задачей пользователей IoT является спасение. Учитывая, что инфраструктура IoT уже широко развернута, ее технические ресурсы могли бы стать весьма полезными для спасения человеческих жизней.

Разработать и успешно внедрить новую систему безопасности для работы в чрезвычайной ситуации с практической точки зрения чрезвычайно трудно из-за сложности процедур стандартизации и сертификации, требуемых для управления операциями в случае бедствий. Однако довольно несложно расширить функциональные средства существующих систем безопасности, введя возможности для поддержки работы приложений IoT в условиях бедствия. Кроме того, услуги на базе IoT могут быть объединены с существующими системами безопасности и использоваться этими системами безопасности во время бедствия.

Важно понимать, что новые интеллектуальные системы IoT никогда не заменят существующие проверенные и сертифицированные системы, в течение многих лет доказывающие свою пригодность; тем не менее новые интеллектуальные системы IoT могут поддерживать возможность взаимодействия с существующими системами безопасности. Технически возможно будет во время бедствия управлять приложениями IoT из административного центра существующих систем безопасности.

Ожидается, что взаимодействие этих усовершенствованных приложений IoT с существующими системами безопасности будет полезным при выполнении спасательных операций, таких как оповещение и эвакуация.

\

Рекомендация МСЭ-T Y.2074

Требования к устройствам интернета вещей и функционированию приложений интернета вещей в условиях бедствия

1 Сфера применения

В настоящей Рекомендации приведены требования к устройствам IoT, которые могут использоваться для функционирования приложений IoT в контексте бедствий, в дополнение к общим требованиям к IoT [ITU-T Y.2066]. Приведены также конкретные требования к функционированию приложений IoT во время бедствий.

Сфера применения настоящей Рекомендации включает требования к:

- устройствам IoT в контексте бедствий;
- функционированию приложений IoT в условиях бедствия (для каждой из трех определенных стратегий работы).

В Дополнении I описаны методы обеспечения целостности и достоверности данных, полученных с помощью устройств IoT во время бедствия.

Настоящая Рекомендация актуальна для разработчиков приложений IoT и поставщиков услуг IoT, а также для аварийно-спасательных служб.

2 Справочные материалы

В нижеследующих Рекомендациях МСЭ-T и других справочных документах содержатся положения, которые, посредством ссылок в настоящем тексте, составляют положения настоящей Рекомендации. На время публикации указанные здесь издания были действительными. Все Рекомендации и другие справочные документы постоянно пересматриваются, поэтому всем пользователям данной Рекомендации настоятельно рекомендуется изучить возможность использования последних изданий перечисленных ниже Рекомендаций и других справочных документов. Перечень действующих на настоящий момент Рекомендаций МСЭ-T регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

[ITU-T X.1303] Recommendation ITU-T X.1303 (2007), *Common alerting protocol (CAP 1.1)*.

[ITU-T Y.1271] Рекомендация МСЭ-T Y.1271 (2004 г.), *Концептуальные требования и сетевые ресурсы для обеспечения экстренной связи по сетям связи, находящимся в стадии перехода от коммутации каналов к коммутации пакетов*.

[ITU-T Y.2066] Рекомендация МСЭ-T Y.2066 (2014 г.), *Общие требования к интернету вещей (IoT)*.

[ITU-T Y.2205] Рекомендация МСЭ-T Y.2205 (2011 г.), *Сети последующих поколений – Электросвязь в чрезвычайных ситуациях – Технические соображения*.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 оповещение (alert) [b-ITU-T X.674]: Сообщение, предназначенное для предупреждения или оповещения о грозящей опасности или возможной проблеме.

3.1.2 устройство (device) [b-ITU-T Y.2060]: Применительно к интернету вещей – это элемент оборудования с обязательными возможностями связи и дополнительными возможностями измерения, срабатывания, а также сбора, хранения и обработки данных.

3.1.3 электросвязь в чрезвычайных ситуациях (emergency telecommunications (ET)) [ITU-T Y.2205]: ET означает любую связанную с чрезвычайными ситуациями службу, для которой требуется специальный режим со стороны сетей последующих поколений (СПП) по сравнению с другими службами. К таким службам относятся уполномоченные властями экстренные службы и службы общественной безопасности.

3.1.4 интернет вещей (Internet of things (IoT)) [b-ITU-T Y.2060]: Глобальная инфраструктура для информационного общества, которая обеспечивает возможность предоставления более сложных услуг путем присоединения (физического и виртуального) 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 для 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 сети последующих поколений (СПП) (next generation network (NGN)) [b-ITU-T Y.2001]: Сети с пакетной коммутацией, пригодные для предоставления услуг электросвязи и для использования нескольких широкополосных технологий транспортировки с включенной функцией QoS, в которой связанные с обслуживанием функции не зависят от применяемых технологий, обеспечивающих транспортировку. Эти сети делают возможным свободный доступ пользователей к сетям и конкурирующим поставщикам услуг и/или услугам по своему выбору. Они поддерживают универсальную мобильность, которая обеспечивает постоянное и повсеместное предоставление услуг пользователям.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины:

Не имеется.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

CAP	Common Alerting Protocol	Протокол общего оповещения
ET	Emergency Telecommunications	Электросвязь в чрезвычайных ситуациях
ICT	Information and Communication technology	Информационно-коммуникационные технологии
IoT	Internet of Things	Интернет вещей
NGN	Next Generation Network	Сети последующих поколений

5 Условные обозначения

В настоящей Рекомендации:

ключевое слово "требуется" означает 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, но не является абсолютно необходимым. Таким образом, для заявления о соответствии этому документу данное требование не является обязательным;

ключевые слова "может факультативно" и "может" означают необязательное требование, которое допустимо, но не имеет рекомендательного значения. Эти термины не означают, что вариант реализации поставщика должен обеспечивать выполнение соответствующей функции, активируемой по желанию оператора сети/поставщика услуг. Это означает лишь, что поставщик может предоставлять данную функцию факультативно и по-прежнему заявлять о соответствии спецификации.

Ключевое слово "бедствие" означает критическую или чрезвычайную ситуацию любого вида, которая вызвана естественными или антропогенными причинами.

Ключевые слова "устройство IoT" означает устройство в среде IoT.

6 Требования к устройствам IoT в контексте бедствия

6.1 Общие требования, связанные с бедствием

Вопросам электросвязи в условиях бедствия посвящены следующие Рекомендации:

– [ITU-T Y.1271], содержащая требования к сетям и описание возможностей сетей для обеспечения электросвязи в чрезвычайных ситуациях (ЕТ);

– [ITU-T Y.2205], содержащая технические соображения, которые в необязательном порядке могут применяться в сетях последующих поколений (СПП) для обеспечения ЕТ. Кроме того, в этой Рекомендации приводятся основополагающие технические принципы, используемые при обеспечении ЕТ.

В этих Рекомендациях рассматриваются требования к электросвязи в чрезвычайных ситуациях и технические аспекты электросвязи в чрезвычайных ситуациях. Предполагая, что приложения IoT будут использовать в условиях бедствий СПП в качестве инфраструктуры электросвязи, эти требования являются применимыми к ним в полной мере.

Согласно [ITU-T Y.2205] рекомендуется использовать протокол общего оповещения (CAP), определенный в [ITU-T X.1303] для обеспечения информационного взаимодействия между системами оповещения.

6.2 Соображения, касающиеся протоколов транспортирования

Все выпускаемые устройства IoT должны проходить процедуры тестирования.

Эти процедуры должны включать тестирование устройств IoT в условиях, выходящих за рамки эксплуатационного диапазона (например, температура, давление, излучение), с тем чтобы проверить безопасность этих устройств для окружающей среды и человека в период бедствий. Устройства IoT не должны вызывать осложнений или возникновения чрезвычайных ситуаций любых типов.

Условия тестирования следует выбирать на основании характеристик возможных чрезвычайных ситуаций в зоне развертывания устройств.

Результаты тестирования и потенциальные опасности, вызываемые устройствами за пределами эксплуатационного диапазона, следует включать в технические характеристики устройств.

Рекомендуется разрабатывать новые устройства IoT с расширенным диапазоном эксплуатационных характеристик (например, рабочая температура, влажность, давление). Требование о расширении диапазона эксплуатационных характеристик устройств IoT важно для приложений IoT, функционирование которых может быть потенциально нарушено вследствие неопределенности изменения условий окружающей среды и их воздействия на устройства IoT во время бедствия.

Рекомендуется распространить эту практику на устройства IoT широко используемых типов. Функционирование устройств IoT, осуществляющих измерения в условиях бедствий могут обеспечить базу данных параметров окружающей среды во время бедствий различного происхождения. Такие измерения помогут сделать важные заключения об этапах развития бедствий и позволят учитывать эту информацию на этапе разработки устройств IoT.

7 Требования к функционированию приложений IoT в условиях бедствия

В данном разделе изложены требования к приложениям IoT, касающиеся их функционирования в условиях бедствия. В частности, в пп. 7.1–7.3 представлены требования для каждой из трех определенных стратегий работы приложений IoT в условиях бедствия, а в п. 7.4 описано переключение между двумя и более стратегиями работы в условиях бедствия.

В целях повышения эффективности ресурсов инфраструктуры, связанных с работой приложений IoT, рекомендуется, чтобы в приложениях IoT была реализована одна или несколько следующих стратегий работы в условиях бедствия.

Для всех стратегий принимается, что в условиях бедствия приложения IoT не продолжают штатно функционировать, а выполняют вместо этого только задачи, связанные со спасением людей.

Возможны ложные оповещения о чрезвычайной ситуации: состояние чрезвычайной ситуации может быть отменено (например, в случае ложного определения чрезвычайной ситуации) и в этом случае приложение IoT переключается обратно в штатный режим работы. Период времени, необходимый для принятия решения о ложном оповещении (продолжение текущего функционирования или возврат в штатный режим работы), определяется каждой конкретной реализацией и зависит от ее сложности.

7.1 Приложения IoT со специальным режимом работы

Если приложение IoT имеет специальный режим работы, который может быть активирован в случае чрезвычайной ситуации, это приложение может использоваться без какого-либо дополнительного действия или внешнего управления. На рисунке 1 показано изменение режима работы приложений IoT в соответствии с этой стратегией.

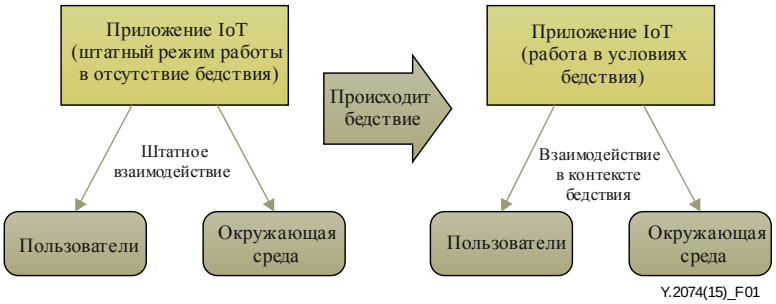

Рисунок 1 – Изменение режима работы приложений IoT, имеющих специальный режим работы, активируемый во время бедствия

Весьма эффективными для самостоятельной эвакуации из здания в случае пожара, землетрясения или иного бедствия могут быть приложения на основе сенсорных сетей, разработанные для определения местоположения пользователей в здании и имеющие специальные режимы работы, активируемые в условиях бедствия.

Другим примером данной стратегии работы является возможность работы одного из приложений IoT в качестве системы безопасности.

ПРИМЕЧАНИЕ. – Существуют прототипы таких систем безопасности, базирующиеся на беспроводных сенсорных технологиях (например, описанные в [b-ITU-T Y.2222]), но они не имеют широкого распространения в силу длительных и сложных процессов стандартизации и сертификации, требуемых для оборудования системы безопасности.

Требуется, чтобы приложения IoT со специальным режимом работы, активируемым во время бедствия, соответствовали всем применимым нормативным правилам.

7.2 Приложения IoT, временно предоставляющие ресурсы для внешних систем безопасности

Как правило, приложения IoT имеют конкретное назначение и по большей части не предназначены для оказания поддержки или помощи пользователям во время бедствия. Следовательно, ресурсы приложений IoT должны поддерживаться внешними системами безопасности, для того чтобы повысить эффективность процесса управления операциями в случае бедствий. На рисунке 2 показано изменение режима работы приложений IoT в соответствии с этой стратегией.

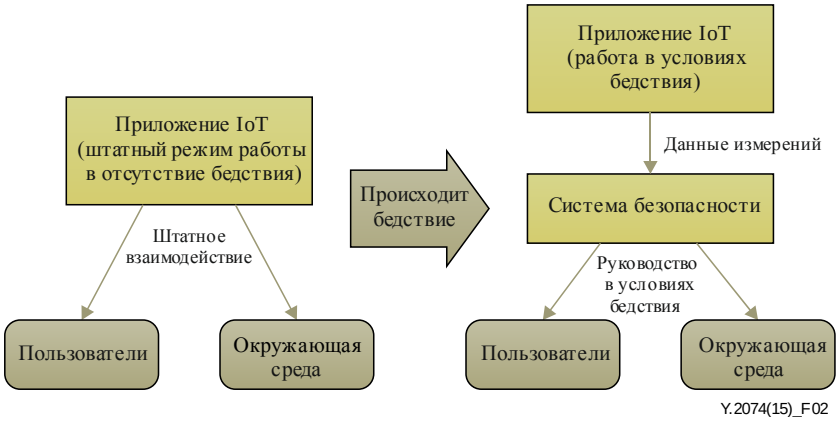

Рисунок 2 – Изменение режима работы приложений IoT, временно предоставляющих ресурсы для внешних систем безопасности во время бедствия

Приложения IoT, разработанные для пользователей, которые находятся в здании или ином месте, оснащенном системой безопасности, должны временно (во время бедствия) использовать совместно с системой безопасности возможности управления приложений IoT и все виды данных измерений. Эти ресурсы могут быть полезными для работы системы безопасности, например данные от различных датчиков, таких как датчики температуры и давления, во время пожара.

В целях упрощения интеграции приложений IoT и внешних систем безопасности рекомендуется использовать для взаимодействия приложений IoT и внешних систем безопасности CAP [ITU-T X.1303]. CAP – это протокол двусторонней связи, который обеспечивает возможность как передачи данных от приложений IoT системам безопасности, так и передачи предупреждающих сообщений от систем безопасности приложениям IoT.

Основным недостатком данной стратегии работы является вероятность отказа функциональных компонентов инфраструктуры IoT, если их проект не предусматривает корректного функционирования в условиях бедствия. Такие отказы, если эти функциональные компоненты необходимы для управления операциями в случае бедствия, могут вызвать негативные последствия. Эти отказы могут быть обусловлены, в отличие от сертифицированных процедур систем безопасности, отсутствием специальных процедур сертификации для функциональных компонентов инфраструктуры IoT, которые служат для обеспечения корректного функционирования в условиях бедствия.

7.3 Приложения IoT с внешним управлением работой во время бедствия

Третья стратегия работы приложений во время бедствия включает полную передачу возможностей управления и данных измерений от приложений IoT внешним системам безопасности или внешним центрам управления.

ПРИМЕЧАНИЕ 1. – Полная передача возможностей управления подразумевает прекращение процесса управления ресурсами самим приложением IoT.

ПРИМЕЧАНИЕ 2. – Внешний центр управления может быть, например, организацией или функциональной единицей организации, которая несет полную юридическую и административную ответственность за надлежащее управление операциями в случае бедствия в данной зоне.

На рисунке 3 показано изменение режима работы приложений IoT в соответствии с этой стратегией.

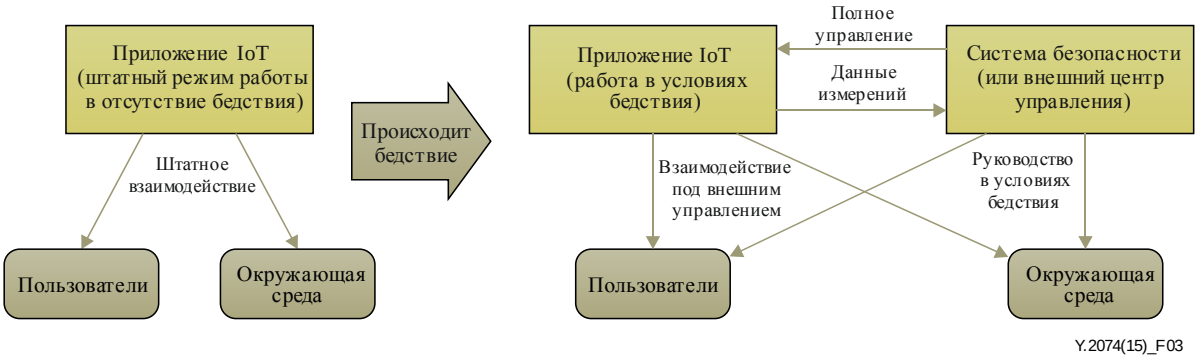

Рисунок 3 – Изменение режима работы приложений IoT с внешним управлением работы во время бедствия

В рамках данной стратегии работы, в отношении приложений IoT, действующих в соответствии с режимом работы, описанным в п. 7.1, поведение пользователей во время бедствия полностью находится под управлением внешних систем безопасности и оповещений.

Основная цель данной стратегии работы заключается в обеспечении того, что системами безопасности или внешними центрами управления осуществляется наиболее эффективное использование всех имеющихся ресурсов приложений IoT благодаря надлежащему управлению ресурсами.

В Дополнении I описаны методы обеспечения целостности и достоверности данных, поступающих от устройств IoT. Центр контроля устройств IoT и управления устройствами IoT, описанный в Дополнении I, может действовать в данной стратегии работы как внешний центр управления для приложений IoT.

Аналогично стратегии работы, описанной в п. 7.2, в рамках данной стратегии рекомендуется использовать CAP [ITU-T X.1303] для взаимодействия между приложениями IoT и внешними системами безопасности или внешними центрами управления.

7.4 Переключение между двумя и более стратегиями работы во время бедствия

В приложении IoT, в зависимости от его назначения и возможностей, может быть реализован набор из одной и более стратегий работы. Это подразумевает возможность приложения IoT переключаться между стратегиями работы в случае возникновения определенных внешних условий, таких как получение сигналов управления, превышение заданного уровня показаний датчика и т. д.

Работа приложения IoT может быть реализована, например, следующим образом.

Рассмотрим приложение IoT (в пределах некоторой географической зоны), оснащенное системой безопасности (внешней по отношению к приложению IoT). Если мониторинг данных устройства показывает возникновение чрезвычайной ситуации во время штатной работы, приложение IoT автоматически переключается в специальный режим работы, предназначенный для работы в условиях бедствия, и реализует стратегию, описанную в п. 7.1.

По истечении времени принятия решения о ложном оповещении приложение IoT продолжает функционировать в специальном режиме работы или переключается обратно в штатный режим работы (в случае ложного оповещения). Если функционирование в специальном режиме работы продолжается до катастрофической фазы бедствия, приложение IoT генерирует настраиваемую для каждого находящегося в зоне бедствия человека информацию, для того чтобы руководить его/ее спасением.

При наступлении катастрофической фазы, когда приложение IoT уже не может управлять ресурсами вследствие ограниченных возможностей, приложение IoT переключается на стратегию работы, описанную в п. 7.2 (контроль и передача собранных данных внешней системе безопасности). Этот режим работы может помочь спасению жизней во время последующего этапа аварийно-спасательных работ и будет контролировать развитие бедствия.

Дополнение I

Методы обеспечения целостности и достоверности данных, поступающих от устройств IoT во время бедствия

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Повсеместно распространенные устройства IoT могут играть важную роль в повседневной жизни человека, влияя на его решения и действия. Таким образом, люди могут зависеть от своих устройств IoT, в частности от их информации и показаний датчиков, а также производных действий, влияющих на окружающую среду. Следовательно, целостность и достоверность данных, поступающих от устройств IoT, являются важнейшими вопросами для IoT в целом.

Проблема целостности и достоверности данных, поступающих от устройств IoT, становится особенно актуальной во время стихийных или антропогенных бедствий, когда не может быть гарантирована целостность самих устройств IoT.

Для сохранения целостности и достоверности данных, поступающих от устройств IoT, необходимо создать для работы устройств IoT безопасную среду. Для этой цели важно определить сферу ответственности за поведение устройств IoT в целом, например за неверные показания датчиков. Существует два метода достижения этой цели:

1 производитель устройств IoT несет полную ответственность за любое нарушение функционирования произведенного им устройства IoT и гарантирует надлежащее поведение устройства IoT;

2 независимый уполномоченный центр несет полную ответственность за любое нарушение функционирования находящегося под его контролем (под его юрисдикцией) устройства IoT и гарантирует надлежащее поведение устройства IoT.

Первый метод менее эффективен из-за сложности взаимодействия пользователей и производителей, ответственных за принадлежащие пользователям устройства IoT, что обусловлено вероятным разнообразием используемых в пределах той же зоны развертывания устройств IoT от различных производителей. Эта проблема становится особенно актуальной в условиях бедствия, когда целостность и достоверность данных, поступающих от устройств IoT, становится вопросом защиты человеческих жизней. Во время бедствия ни пользователи, ни спасательные службы, или же устройства IoT не смогут вступить в контакт с производителем каждого конкретного устройства IoT, для того чтобы подтвердить целостность и достоверность поступающих от него данных.

Второй метод значительно более конкретен в том, что он подразумевает создание центров контроля и управления для устройств IoT. Эти центры будут нести ответственность за надлежащее функционирование находящихся под их юрисдикцией устройств IoT.

I.1 Общий обзор центра контроля и управления для устройств IoT

Центр контроля и управления (Центр) для устройств IoT – это организация или функциональная единица организации, которая несет полную юридическую и административную ответственность за надлежащее функционирование находящихся под ее юрисдикцией устройств IoT. Она также контролирует устройства IoT и сохраняет информацию об операциях во время бедствия. Основная задача центра контроля и управления для устройств IoT заключается в проверке целостности и достоверности информации, поступающей от находящихся под его юрисдикцией устройств IoT. Кроме того, Центр несет ответственность за своевременное оповещение пользователей и/или владельцев устройств IoT при обнаружении нарушения функционирования какого-либо устройства IoT.

В случае угрозы бедствия Центр несет ответственность за:

- контроль состояния находящихся под его юрисдикцией устройств IoT и их выходных данных (например, показания датчиков);
- определение ненадлежащим образом функционирующих устройств IoT и своевременное оповещение пользователей и/или владельцев о нарушении функционирования;

- определение зоны бедствия, а также природы и параметров бедствия с учетом информации, полученной от находящихся под его юрисдикцией устройств IoT и поступающей из внешних источников (например, агентства по чрезвычайным ситуациям);
- управление находящимися под его юрисдикцией устройствами IoT для осуществления безопасной эвакуации людей из зоны бедствия;
- запись и хранение информации, полученной во время бедствия, и истории операций во время бедствия.

I.2 Распределение обязанностей центра контроля и управления среди местных центров

Повсеместно распространенные устройства IoT присутствуют в большом количестве в квартирах, жилых домах, организациях, на улицах, в общественных местах и т. д.

В случае наличия центра контроля и управления для устройств IoT возможно, чтобы все устройства IoT в данном жилом доме или здании находились под юрисдикцией одного местного центра. Аналогично, все устройства IoT в других зонах, например на той же улице, могут находиться под управлением других местных центров. Все эти местные центры могут быть объединены в инфраструктуру основного Центра.

Инфраструктура основного Центра может быть организована по принципу многоуровневой иерархии, содержащей узлы контроля и управления разных уровней, которые отвечают за устройства IoT, находящиеся в разных зданиях (местные центры), городах (муниципальные центры), регионах (региональные центры) и странах (федеральные центры).

Кроме того, обязанности местных центров могут быть распределены по назначению устройств IoT. Например, Центр может управлять несколькими местными центрами, один из которых несет ответственность за устройства IoT, предназначенные для бытовых целей, другой – за устройства IoT, предназначенные для целей управления дорожным движением, третий – за устройства IoT, предназначенные для целей системы безопасности, и т. д.

В нижеследующих пунктах описаны возможные сценарии работы центра контроля и управления.

I.3 Сценарии работы центра контроля и управления

Основная задача центра контроля и управления для устройств IoT заключается в проверке целостности и достоверности информации, поступающей от находящихся под его юрисдикцией устройств IoT. Эту задачу возможно выполнить несколькими способами:

1 сравнение показаний датчиков устройств IoT, находящихся под юрисдикцией Центра, с показаниями автономных (дублированных) сенсорных сетей;

2 интеллектуальный контроль показаний датчиков, находящихся под юрисдикцией Центра, который включает сбор данных и математический анализ (интеллектуальный анализ данных) полученной информации, позволяющий обнаруживать нарушение функционирования устройств IoT.

Оба метода могут быть реализованы и использоваться в сочетании в соответствующей пропорции.

Определенные выше методы более подробно описаны в пп. I.3.1 и I.3.2.

I.3.1 Автономная сенсорная сеть

Центр разворачивает автономные сенсорные сети, содержащие датчики различных физических параметров, которые дублируют датчики устройств IoT, находящихся под юрисдикцией Центра.

Автономная сенсорная сеть должна покрывать всю зону, находящуюся под юрисдикцией Центра. Например, местный внутренний центр должен задействовать сенсорную сеть, покрывающую внутреннюю зону, в которой расположены устройства IoT, находящиеся под юрисдикцией Центра.

Датчики этой автономной сенсорной сети рассматриваются как эталонные датчики, то есть их показания принимаются в качестве эталонных значений физических параметров в этой зоне. Ожидается, что эталонные датчики сертифицированы доверенной и надлежащим образом сертифицированной организацией.

Центр собирает данные от находящихся под его юрисдикцией устройств IoT и сравнивает их с эталонными значениями. На основании этого сравнения Центр принимает решение о целостности и достоверности данных, поступающих от устройств IoT.

Преимуществом данного метода является потенциально высокая надежность эталонных датчиков, не зависимых от устройств IoT. Таким образом, нарушение функционирования устройств IoT выявляется с высокой точностью.

Недостатком данного метода является стоимость и сложность развертывания автономных сенсорных сетей и возможные отказы эталонных датчиков в условиях бедствия.

I.3.2 Интеллектуальный контроль

Интеллектуальный контроль касается сбора информации об устройствах и показаний датчиков от находящиеся под юрисдикцией Центра устройств IoT и математический анализ этой информации. Такой анализ включает, в том числе, методы статистического анализа и обработку сигнала корреляции.

Интеллектуальный контроль позволяет выявлять неисправные устройства IoT или их датчики в рамках группы аналогичных устройств.

Преимуществом данного метода является полная независимости от внешних параметров окружающей среды, что позволяет работать в любой ситуации во время бедствия.

Недостатком данного метода является необходимость иметь группу аналогичных устройств IoT для более надежного определения нарушения функционирования.

I.4 Использование сохраненных данных

Центр осуществляет контроль, запись и хранение информации об устройствах и показаний датчиков, полученных от находящихся под его юрисдикцией устройств IoT, включая данные, полученные непосредственно перед и во время бедствия.

Эта функциональная возможность обеспечивает Центру возможность работать в случае чрезвычайной ситуации как "черный ящик". Назначением Центра является помощь в определении причин чрезвычайной ситуации аналогично тому, что делает "черный ящик" на борту воздушного судна.

Ретроспективные данные, собранные в хранилище данных Центра, могут использоваться для совершенствования методов интеллектуального контроля и разработки методов управления и контроля устройств IoT в условиях угрозы бедствия или во время бедствия, с тем чтобы обеспечить безопасную эвакуацию из зоны бедствия возможно большего числа людей.

Библиография

[b-ITU-T X.674] Recommendation ITU-T X.674 (2011), *Procedures for the registration of arcs under the Alerting object identifier arc*.

[b-ITU-T Y.2001] Рекомендация МСЭ-Т Y.2001 (2004 г.), *Общий обзор СПП*.

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

[b-ITU-T Y.2222] Recommendation ITU-T Y.2222 (2013), *Sensor control networks and related applications in a next generation network environment*.

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
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, 2016 г.