Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1368

(01/2021)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасные приложения и услуги (2) –
Безопасность интернета вещей (IoT)

Безопасное обновление микропрограммного или программного обеспечения устройств интернета вещей

Рекомендация МСЭ-Т X.1368

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (1)	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности (1)	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (2)	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1319
Безопасность "умных" электросетей	X.1330–X.1339
Сертифицированная электронная почта	X.1340–X.1349
Безопасность интернета вещей (IoT)	**X.1360–X.1369**
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1379
Безопасность технологии распределенного реестра	X.1400–X.1429
Безопасность технологии распределенного реестра	X.1430–X.1449
Протоколы безопасности (2)	X.1450–X.1459
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699
КВАНТОВАЯ СВЯЗЬ	
Терминология	X.1700–X.1701
Квантовый генератор случайных чисел	X.1702–X.1709
Структура безопасности QKDN	X.1710–X.1711
Проектирование безопасности QKDN	X.1712–X.1719
Методы обеспечения безопасности QKDN	X.1720–X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	
Безопасность больших данных	X.1750–X.1759
БЕЗОПАСНОСТЬ СЕТЕЙ 5G	X.1800–X.1819

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

Рекомендация МСЭ-Т X.1368

Безопасное обновление микропрограммного или программного обеспечения устройств интернета вещей

Резюме

В Рекомендации МСЭ-Т X.1368 определены: 1) базовые модели и процедуры, предназначенные для безопасного обновления микропрограммного или программного обеспечения (FW/SW) устройств интернета вещей (IoT); и 2) требования и возможности для обновления FW IoT.

Единая процедура безопасного обновления определена с использованием общих требований. Эта процедура обеспечивает безопасную реализацию общих обновлений SW/FW IoT заинтересованными сторонами в среде IoT, такими как разработчики устройств IoT и поставщики систем/услуг IoT.

Настоящая Рекомендация ориентирована на обновление FW, но она применима для обновления любого иного SW устройств IoT.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1368	07.01.2021 г.	17-я	11.1002/1000/14445

Ключевые слова

IoT, безопасность, обновление программного обеспечения.

* Для доступа к Рекомендации наберите в адресном поле вашего веб-навигатора 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

Кибератаки на устройства или системы интернета вещей (IoT) становятся все более изощренными, высокоорганизованными и разнообразными. Ранее функции большинства устройств IoT исправлялись поставщиками устройств IoT на начальном этапе выпуска. Однако в последнее время устройства подключаются к интернету для предоставления расширенного набора услуг IoT. Вследствие этого используемые устройства IoT сталкиваются с киберугрозами или атаками. Следует признать, что для устранения уязвимостей и слабых мест микропрограммного или программного обеспечения (FW/SW) устройств IoT его необходимо безопасно обновлять. Некоторые производители устройств уже начали предоставлять услуги по обновлению микропрограммного обеспечения по своим собственным схемам.

В настоящей Рекомендации представлены базовые модели и процедуры безопасного обновления SW/FW IoT, а также связанные с ними требования и возможности. Благодаря базовым моделям и единой процедуре обновления SW/FW IoT можно безопасно распространять среди заинтересованных сторон в среде IoT, поощряя эти заинтересованные стороны к обновлению устаревшего SW/FW IoT.

Рекомендация МСЭ-Т X.1368

Безопасное обновление микропрограммного или программного обеспечения устройств интернета вещей

1 Сфера применения

В настоящей Рекомендации определены базовые модели и процедуры безопасного обновления микропрограммного или программного обеспечения (FW/SW) устройств IoT. В ней также определены требования и возможности, связанные с обновлениями FW/SW IoT. Настоящая Рекомендация ориентирована на обновление FW, но она применима для обновления любого иного программного обеспечения устройств IoT.

2 Справочные документы

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

Отсутствуют.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины:

3.2.1 автор (author): Объект, создающий образы микропрограммного обеспечения (FW) и программного обеспечения (SW) для устройств интернета вещей. Примерами могут служить отдельный человек или группа, такая как компания или организация любого другого типа. Он может закачивать образ в один или несколько серверов FW, которые могут быть незащищенными.

3.2.2 потребитель микропрограммного обеспечения (firmware consumer): Объект, который хранит, проверяет и запускает образы микропрограммного обеспечения (FW) на устройстве интернета вещей (IoT). Он решает вопрос о запуске текущих образов FW. У IoT-устройства имеется один или несколько потребителей FW.

3.2.3 сервер микропрограммного обеспечения (firmware server): Объект, распространяющий образы микропрограммного обеспечения **(**FW). Он может принимать образы FW от нескольких авторов; он может быть репозиторием определенного поставщика или репозиторием, принимающим данные разных поставщиков. В идеале сервер FW защищен, но может быть и незащищенным; он может пытаться просматривать или изменять пакеты FW, полученные от авторов.

3.2.4 манифест (manifest): Запись, содержащая метаданные образа микропрограммного обеспечения.

3.2.5 инспектор состояния (status tracker): Объект, который проверяет и отслеживает состояние образов FW в одном или нескольких потребителях FW и при необходимости инициирует обновления FW. Это предполагает детальный контроль изменений в устройстве, например версии запущенных образов FW и состояния цикла обновления FW, в котором устройство находится в данный момент времени. Инспектор состояния может располагаться внутри устройства интернета вещей, в интрасети или в интернете.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

DLT	Distributed Ledger Technology	Технология распределенного реестра
FW	Firmware	Микропрограммное обеспечение
IoT	Internet of Things	Интернет вещей
SW	Software	Программное обеспечение
URL	Uniform Resource Locator	Унифицированный указатель ресурса

5 Соглашения

В настоящей Рекомендации соблюдаются следующие соглашения, соответствующие [b-IETF RFC 2119].

"Должен" Это слово означает требование, которое является абсолютно обязательным в рамках данной Рекомендации.

"Не должен" Это выражение означает абсолютный запрет в рамках данной Рекомендации.

"Следует" Это слово означает, что в определенных обстоятельствах могут существовать веские причины, которые позволяют игнорировать данный аспект, но, прежде чем принять данное решение, следует в полной мере взвесить все последствия и тщательно проанализировать ситуацию.

"Не следует" Это слово означает, что могут существовать веские причины, когда в определенных обстоятельствах указанный образ действий допустим и даже полезен, но при осуществлении действия, отличного от рекомендованного, ситуация должна быть тщательно проанализирована, а последствия этого должны быть осознаны.

"Можно" Это слово означает, что данный аспект действительно не является обязательным. Конкретный продавец может рассматривать данный аспект как желательный в конкретных условиях рынка или в целях улучшения продукта, другие продавцы могут игнорировать данное требование.

6 Базовая модель

Сетевая архитектура устройств IoT может быть разной, но во всех случаях следует использовать четыре функциональных объекта: потребитель FW (см. раздел 3.2.2), инспектор состояния (см. раздел 3.2.5), автор (см. раздел 3.2.1) и сервер FW (см. раздел 3.2.3). Отметим, что внутри одного узла могут находиться несколько функциональных объектов. Например, в устройстве веб-камеры содержатся несколько потребителей FW и инспектор состояния, а в веб-сервере – инспектор состояния и сервер FW. Несколько потребителей FW могут находиться в одной сети и контролироваться инспектором состояния, реализованным внутри шлюза. Конструкции могут различаться в зависимости от ограниченности устройств IoT. Типичные практические модели описаны в разделе 8.

В базовой модели эти объекты играют незаменимую роль в обновлении SW/FW IoT. Базовый сценарий для этой модели прост: *инспектор состояния, признавший необходимость обновления SW/FW IoT, инициирует процедуру обновления SW/FW, которая позволяет потребителям FW получить от автора образ SW/FW через сервер FW.*

7 Процедуры обновления

На рисунке 1 показана базовая процедура обновления FW. Перед началом процедуры обновления FW автору необходимо загрузить на сервер FW новый образ FW. Желательно, чтобы образ сопровождался цифровой подписью и был зашифрован автором.

Когда инспектор состояния получает запрос на обновление образа FW с указанием его местоположения [например, его унифицированного указателя ресурсов (URL)], он проверяет запрос, а затем, если запрос действителен, проверяет состояние FW, устанавливая связь с потребителем FW для подтверждения необходимости обновления FW. Некоторые типичные способы передачи таких запросов перечислены в разделе 9.

Если необходимость обновления FW подтверждается, потребитель FW инициирует обновление FW, сообщая местонахождение доступного FW. Затем потребитель FW запрашивает обновленный образ FW с сервера FW. Сервер FW предоставляет образ FW потребителю FW при условии, что у потребителя FW имеется законное право на получение обновления. В противном случае сервер отправляет сообщение с кодом ошибки обновления.

Получив сообщение с обновлением, потребитель FW проверяет образ. Если ошибки не обнаружены, потребитель FW устанавливает FW и передает информацию о состоянии в инспектор состояния. Отметим, что мощность множества вышеупомянутых четырех функциональных объектов – "много ко многим", то есть многие инспекторы состояния могут взаимодействовать со многими потребителями FW, которые в свою очередь могут взаимодействовать со многими серверами FW, а те – со многими авторами.

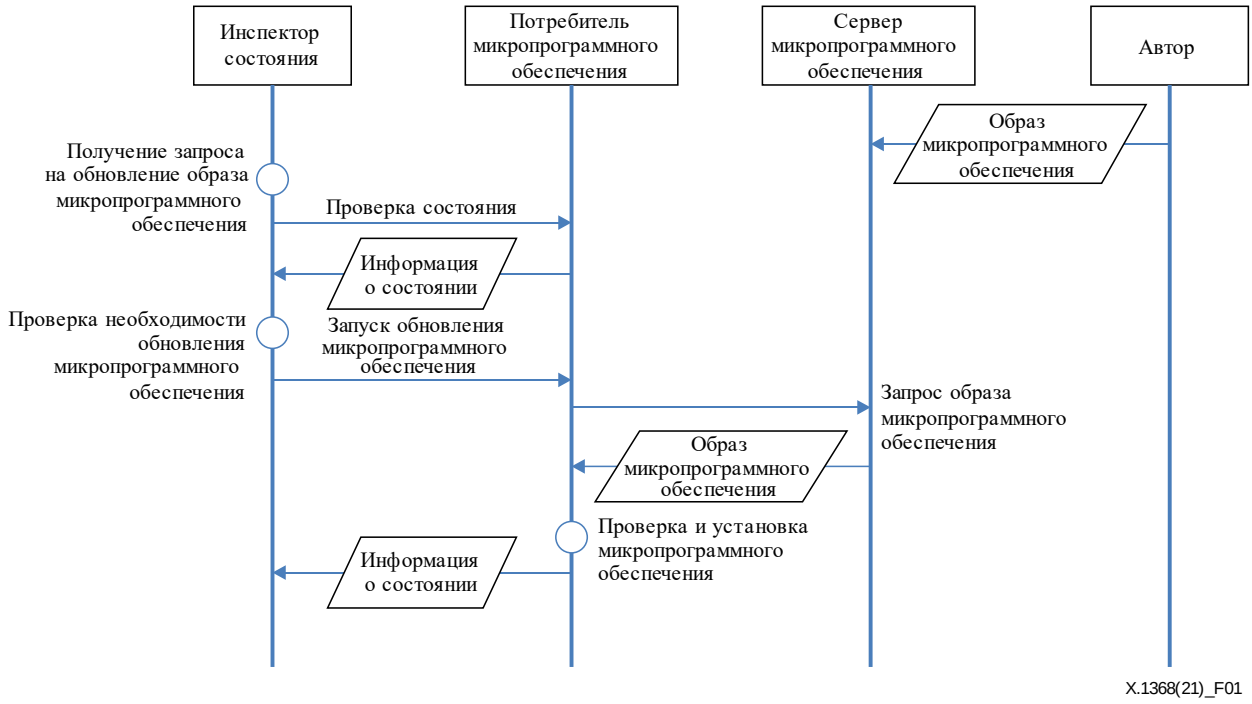

Рисунок 1 – Процедура протокола

8 Сценарии развертывания

Как упоминалось в разделе 6, внутри одного узла могут находиться несколько функциональных объектов и несколько объектов могут служить функциональным объектом; сценарии развертывания могут различаться в зависимости от обстоятельств. В этом разделе иллюстрируются несколько сценариев развертывания.

8.1 Внутренние функциональные объекты устройств IoT

На рисунке 2 показаны устройства IoT четырех типов. В устройстве IoT должен присутствовать по крайней мере один потребитель FW, так как естественно, что устройство IoT содержит несколько образов FW.

В устройстве IoT должен присутствовать по крайней мере один инспектор состояния. В нем может содержаться несколько инспекторов состояния для обслуживания нескольких потребителей FW, но нормально работает и один инспектор состояния, обслуживающий всех потребителей FW.

Устройство IoT с ограниченными ресурсами может минимизировать функциональные возможности инспектора состояния. В этом случае функция отслеживания состояния распределяется между модулем на стороне клиента и модулем на стороне сервера, установленным вне устройства IoT. На стороне клиента остаются минимальные функциональные возможности, например взаимодействие с FW-потребителем, тогда как остальные функции экспортируются на сторону сервера. Модуль на стороне сервера может обслуживать несколько клиентских модулей. Часто это предпочтительный способ развертывания.

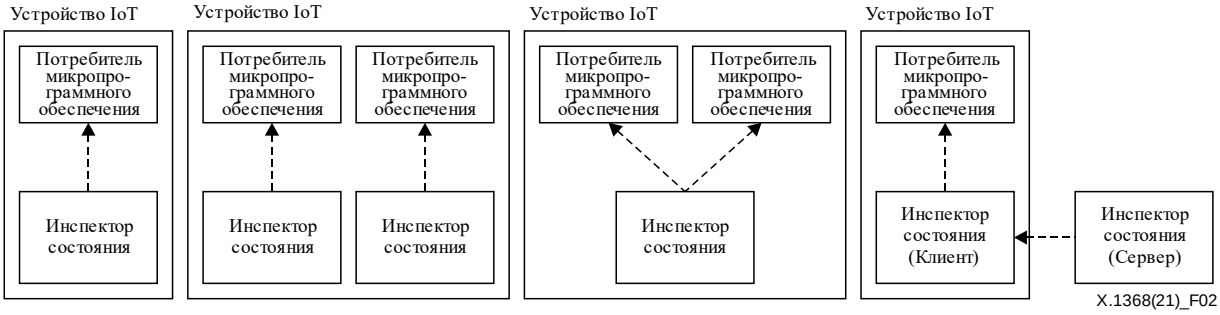

Рисунок 2 – Различные типы устройств IoT

8.2 Способы развертывания инспекторов состояния

Устройства IoT сильно различаются по своим ресурсам; инспектор состояния может находиться и внутри устройства IoT, но в случае устройств IoT с ограниченными ресурсами инспектор может быть отделен для минимизации потребляемых ресурсов. Более того, возможны случаи, когда для удобства предпочтительнее управлять устройствами IoT из одного центрального объекта.

В этих ситуациях функции инспектора состояния могут быть распределены между несколькими модулями и реализовываться иерархическим образом. Несколько модулей могут быть включены в каскад, так что вышестоящий модуль определяет необходимость обновления FW и инициирует соответствующую процедуру через нижестоящие модули.

В пунктах 8.2.1–8.2.3 обсуждаются случаи, когда 1) инспектор состояния внутри устройства IoT взаимодействует непосредственно с сервером FW, 2) инспектор состояния внутри устройства IoT взаимодействует с сервером FW через другой инспектор состояния, находящийся внутри интрасети, и 3) инспектор состояния внутри устройства IoT взаимодействует с сервером FW через ряд инспекторов состояния.

8.2.1 Модель с инспектором состояния внутри устройства

На рисунке 3 показана модель с инспектором состояния, встроенным в устройство. Согласно этой модели, потребитель FW и инспектор состояния находятся внутри устройства IoT. Когда инспектор состояния осознает необходимость обновления FW (см. раздел 9), он запрашивает у потребителя FW получение образов встроенного FW с сервера FW. Отметим, что в этом разделе представлены абстрактные каналы связи, но они могут быть подсоединены через протокол Интернет или другие протоколы либо их комбинацию, для которой требуются мосты для связи между объектами. На рисунке 3 показан интернет, но методы, упомянутые в настоящей Рекомендации, будут работать и с любыми другими сетями.

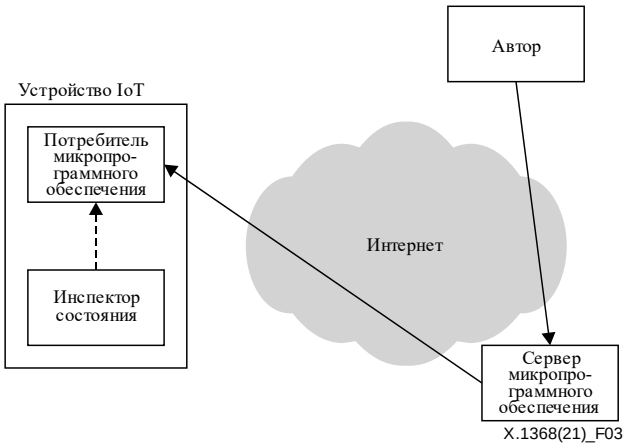

Рисунок 3 − Иллюстрация развертывания модели с инспектором состояния внутри устройства

8.2.2 Модель с инспектором состояния "клиент-сервер"

На рисунке 4 показана модель с инспектором состояния "клиент-сервер". В этой модели функции инспектора состояния распределены между модулями клиента и сервера. Клиентские модули находятся в устройствах IoT, а модуль сервера – внутри сети. Модуль сервера контролирует несколько устройств IoT, взаимодействуя с клиентскими модулями. Клиентские модули просто проверяют сообщение от модуля сервера и действуют в соответствии с ним. Процедуру обновления FW инициирует модуль сервера.

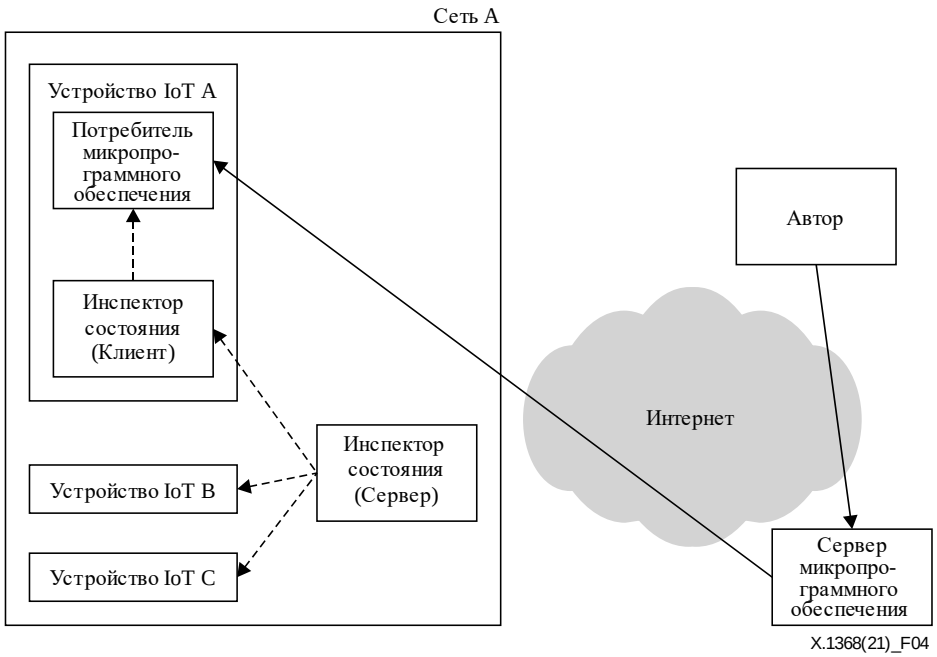

Рисунок 4 − Иллюстрация развертывания модели с инспектором состояния "клиент-сервер"

8.2.3 Иерархическая модель инспектора состояния

На рисунке 5 показана иерархическая модель инспектора состояния. В этой модели функции инспектора состояния распределены между несколькими модулями: клиента, промежуточных модулей и сервера. Клиентские модули находятся в устройствах IoT, а модуль сервера и промежуточные модули – внутри сетей. Промежуточные модули, взаимодействуя с клиентскими модулями, контролируют несколько устройств IoT, а модуль сервера контролирует все клиентские модули, взаимодействуя с промежуточными модулями. Отметим, что для создания дальнейшей иерархии промежуточные модули можно соединять каскадом. Клиентские модули просто проверяют сообщение от модуля сервера и действуют в соответствии с ним. Процедуру обновления FW инициирует модуль сервера.

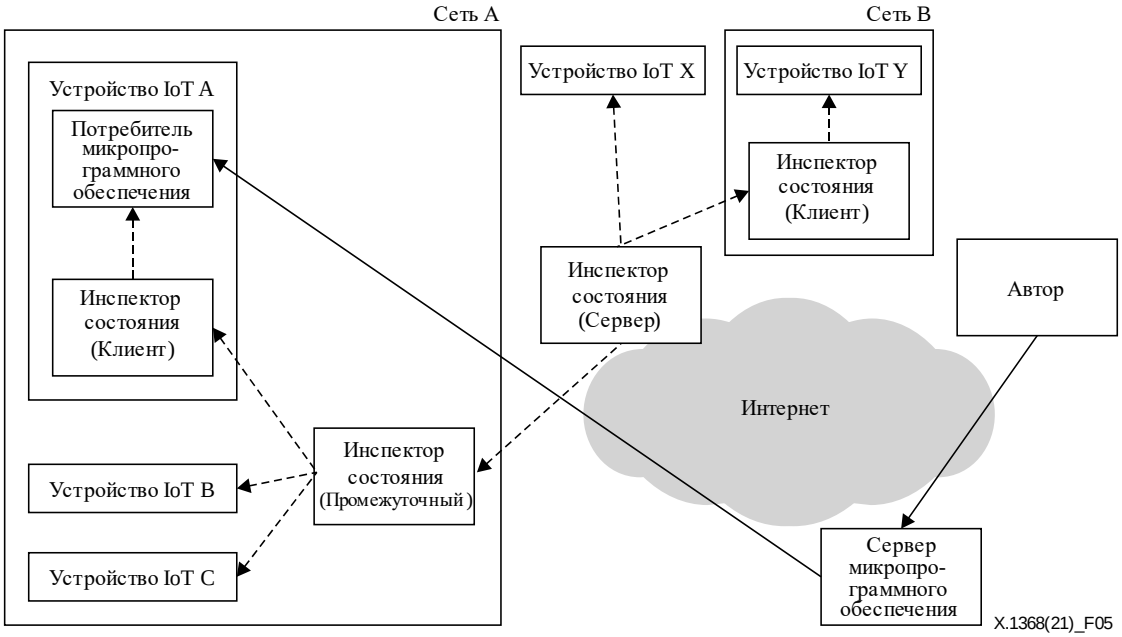

Рисунок 5 − Иллюстрация иерархической модели развертывания инспектора состояния

9 Обнаружение доступных новых образов микропрограммного обеспечения и запуск процедуры

Весь процесс запускается инспектором состояния после получения им запроса на обновление образа FW. Запрос этого типа может принимать различные формы:

a) запрос может отправить автор, публикующий новые версии образа FW;

b) запрос может отправить сервер FW, получивший новую версию образа FW;

c) запрос может отправить администратор устройства IoT, узнавший о выпуске новой версии образов FW;

d) инспектор состояния или один из его вышестоящих инспекторов состояния, периодически опрашивая сервер FW, обнаруживает новую версию образов FW;

e) инспектор состояния или один из его вышестоящих инспекторов состояния узнает о новой версии образа FW, наблюдая за процедурой обновления FW другого устройства IoT, которое он обслуживает.

Запросы могут вызываться и другими событиями, но эти запросы должны сообщать инспектору состояния сведения об URL-адресах образов FW и их версиях. Если инспектор состояния решит, что информация надежна и достоверна, он может инициировать процедуру, определенную в разделе 7.

10 Требования

В этом разделе перечислены функциональные требования, предъявляемые к обновлениям программного обеспечения IoT. Ввиду ограниченности ресурсов применимы не все процедуры обновления программного обеспечения, доступные в среде без ограничений. Часто бывает, что рядом с устройством IoT отсутствует человек-пользователь или оператор. Следовательно, при разработке конкретной процедуры обновления систем безопасности необходимо учитывать эти особенности. Отметим, что конфиденциальность, целостность и готовность четырех функциональных объектов должны сохраняться, и это является предварительным условием обновления программного обеспечения; поэтому они исключены из списка требований в следующем списке.

a) Вредоносное SW/FW распространяться не должно:

   i) вредоносные образы следует выявлять до их закачки или распространения;

   ii) должна проверяться целостность образов FW;

   iii) должен проверяться поставщик образов FW.

b) Уязвимое SW/FW не должно оставаться без принятия надлежащих мер:

i) следует выявлять устаревшие версии SW/FW;

ii) следует выявлять уязвимое SW/FW.

c) Ошибки, произошедшие во время процедуры обновления, должны исправляться:

i) если обновление SW/FW не удалось, следует предусмотреть способы уведомления об этой ситуации;

ii) следует предусмотреть резервные средства или средства защиты на случай отказа в процессе обновления.

d) Следует выполнять только запланированные и необходимые обновления:

i) должны устанавливаться только более новые версии SW/FW IoT;

ii) должны устанавливаться только проверенные образы SW/FW IoT.

e) Должны учитываться ограничения по ресурсам:

i) в целях минимизации сетевых ресурсов процедуру обновления не следует выполнять, если в ней нет необходимости;

ii) в целях минимизации нагрузки на устройства IoT с ограниченными ресурсами функции инспектора состояния могут каскадироваться.

f) Права интеллектуальной собственности авторов должны сохраняться:

i) образы SW/FW должны шифроваться авторами;

ii) должны сохраняться конфиденциальность, целостность и готовность образов SW/FW IoT;

iii) образы SW/FW должны безопасным образом переноситься от автора в конечный пункт назначения.

11 Возможности

В настоящем разделе перечислены возможности функциональных объектов, основанные на требованиях, упомянутых в разделе 10.

11.1 Возможности потребителя микропрограммного обеспечения

a) Потребитель FW должен иметь возможность:

i) проверки успешности предыдущего обновления FW;

ii) передачи информации о текущих образах SW/FW (например, о номере версии) сторонам, запрашивающим эту информацию с законными правами;

iii) применения резервных средств или средств защиты в случае отказа в процессе обновления;

iv) уведомления инспектора состояния о необходимости обновления FW;

v) подтверждения подлинности и целостности образов FW (путем проверки их сертификатов) самостоятельно или другим способом (например, путем делегирования процесса подтверждения других объединениям);

vi) отказа от установки новой версии образов SW/FW.

b) Потребителю FW рекомендуется поддерживать "безопасный режим", в котором устройство IoT работает с минимальными функциональными возможностями и как минимум предоставляет средства для установки/восстановления/обновления FW в ручном режиме.

11.2 Возможности инспектора состояния

Инспектор состояния должен иметь следующие возможности:

a) ведение списков потребителей FW с обновленными и устаревшими образами FW:

i) эти списки должны как минимум содержать их уникальные идентификаторы;

ii) инспектор состояния должен иметь возможность выявлять потребителей FW с устаревшим FW;

b) при определении состояния потребителей FW, находящихся под их контролем, должны иметься средства:

i) для подтверждения того, что потребитель FW (и содержащее его устройство IoT) находится в рабочем состоянии, посредством связи с потребителем FW и проверки журналов сообщений потребителя FW;

ii) для проверки успешности завершения предыдущего сеанса обновления FW у потребителя FW;

iii) позволяющие узнать, какие версии FW используют потребители FW;

c) определение необходимости обновления SW/FW и при ее наличии запуск процедуры обновления FW;

d) проверка подлинности вышестоящего инспектора состояния при иерархической реализации.

Если функциональные возможности инспектора состояния распределены между несколькими модулями, эти модули должны быть способны выполнять следующие функции:

a) сохранение конфиденциальности и целостности связи между ними;

b) проверка подлинности сигналов, отправленных друг другу;

c) хранение информации о своей доступности.

11.3 Возможности сервера микропрограммного обеспечения

Сервер FW должен обладать следующими возможностями:

a) прием образов SW/FW IoT от авторов;

b) предоставление содержащихся в нем образов SW/FW потребителям FW;

c) выявление вредоносных образов SW/FW и принятие соответствующих мер, таких как их удаление из внутреннего хранилища и запрет на прием данных от авторов, приславших такие образы;

d) управление списком авторов и потребителей FW, которые им пользуются;

e) управление версиями образов SW/FW IoT;

f) ведение списка потребителей FW и загруженных ими ранее образов SW/FW;

g) уведомление устройств IoT, ранее загрузивших устаревшие образы SW/FW IoT, о доступности новых версий;

h) проверка географического или логического местоположения устройств IoT, а также разрешение или запрет на загрузку образов SW/FW во избежание их распространения в местах, запрещенных правилами или другими способами.

11.4 Возможности автора

Автор должен иметь возможность обеспечить подлинность, конфиденциальность и целостность созданных им образов FW:

a) недопустимы подмена или взлом FW третьими лицами (подлинность и целостность);

b) должна сохраняться интеллектуальная собственность поставщиков в рамках FW (конфиденциальность);

c) автор должен принять меры для защиты образа FW, который он загружает на серверы FW, так как сервер FW может быть незащищенным.

Дополнение I

Соответствующая деятельность за рамками МСЭ-Т

(Данное дополнение не является неотъемлемой частью настоящей Рекомендации.)

К исследованной за рамками МСЭ-Т деятельности, связанной с обновлениями SW IoT, относятся:

1) семинар IOTSU [b-ISOC iotsu];
2) рабочая группа IETF SUIT [b-IETF suit]:
   - вопрос о файле манифеста [b-IETF manifest];
   - вопрос об архитектуре обновления FW [b-IETF architecture];
3) oneM2M: стандарты M2M и IoT [b-oneM2M], и др.

Дополнение II

Пример сценария обновления программного обеспечения IoT с использованием технологии распределенного реестра

(Данное дополнение не является неотъемлемой частью настоящей Рекомендации.)

II.1 Обзор

Инфраструктура IoT содержит большое количество устройств, которыми должен управлять администратор. Устройство IoT испытывает различные варианты пересмотра в зависимости от особенностей аппаратуры, и для дополнительной платы датчиков может применяться особое FW. Кроме того, в зависимости от версии оборудования поддерживаются разные версии программного обеспечения. Наряду с этим различия в установленных пакетах программного обеспечения могут вызвать проблемы зависимости. Эту проблему можно решить с помощью технологии распределенного реестра (DLT).

В DLT используется "умный" контракт, который позволяет обновлять FW или SW в соответствии с контрактами, заранее составленными администратором. Кроме того, решения проблем уязвимости системы безопасности, которые могут возникнуть в процессе обновления, могут быть основаны на алгоритмах достижения консенсуса и криптографического уровня.

В этом примере описано, как обеспечить безопасные обновления FW/SW на основе DLT в средах с разными версиями оборудования и SW, таких как инфраструктура IoT.

II.2 Процедура обновления программного обеспечения

См. таблицу II.1 и рисунки II.1 и II.2.

Таблица II.1 − Структура блоков обновления программного обеспечения

Заголовок блока	– Размер блока, версия – Хеш заголовка предыдущего блока
Данные блока	– Корень Меркла – Имя поставщика, время публикации, номер версии, хеш-код файла, ссылка на файл, имя файла, размер файла, вспомогательное оборудование, зависимость от программного обеспечения

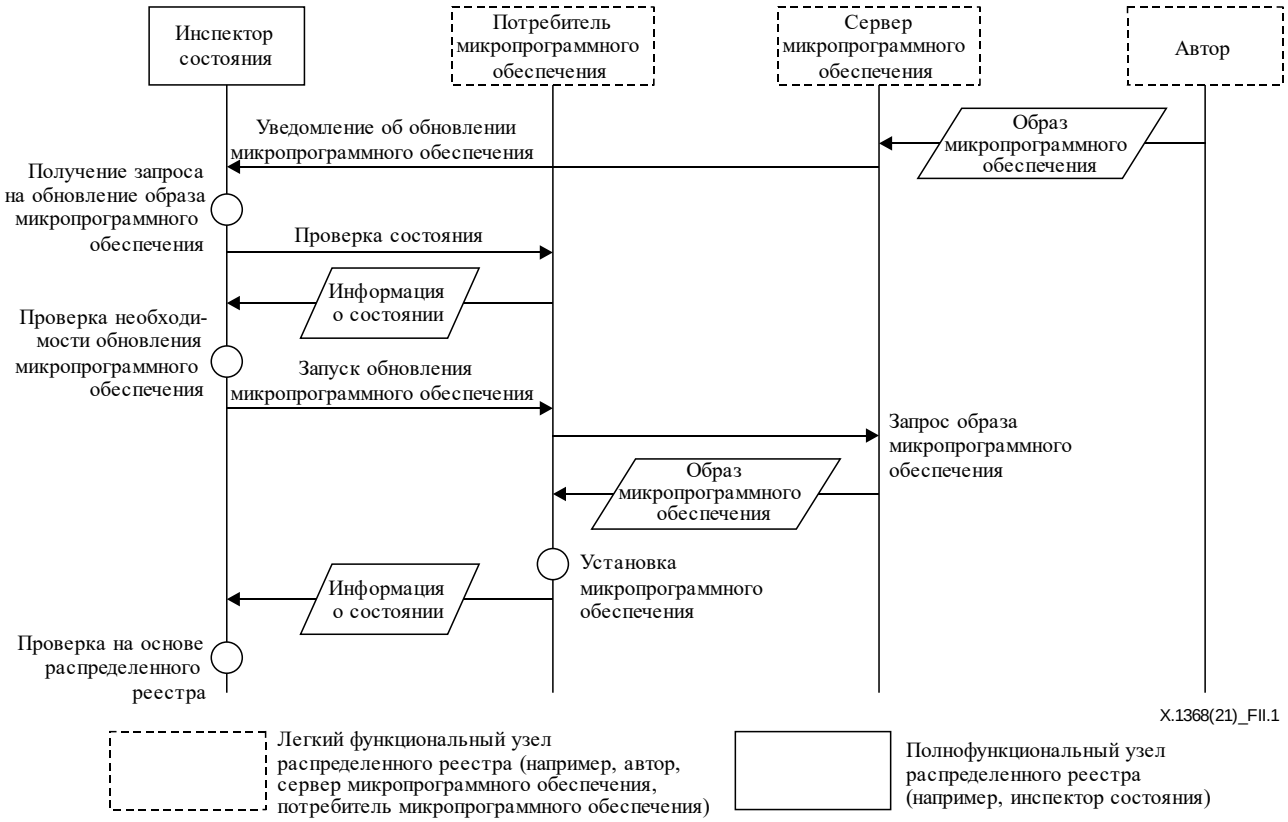

Рисунок II.1 − Процедура обновления программного обеспечения на основе распределенного реестра

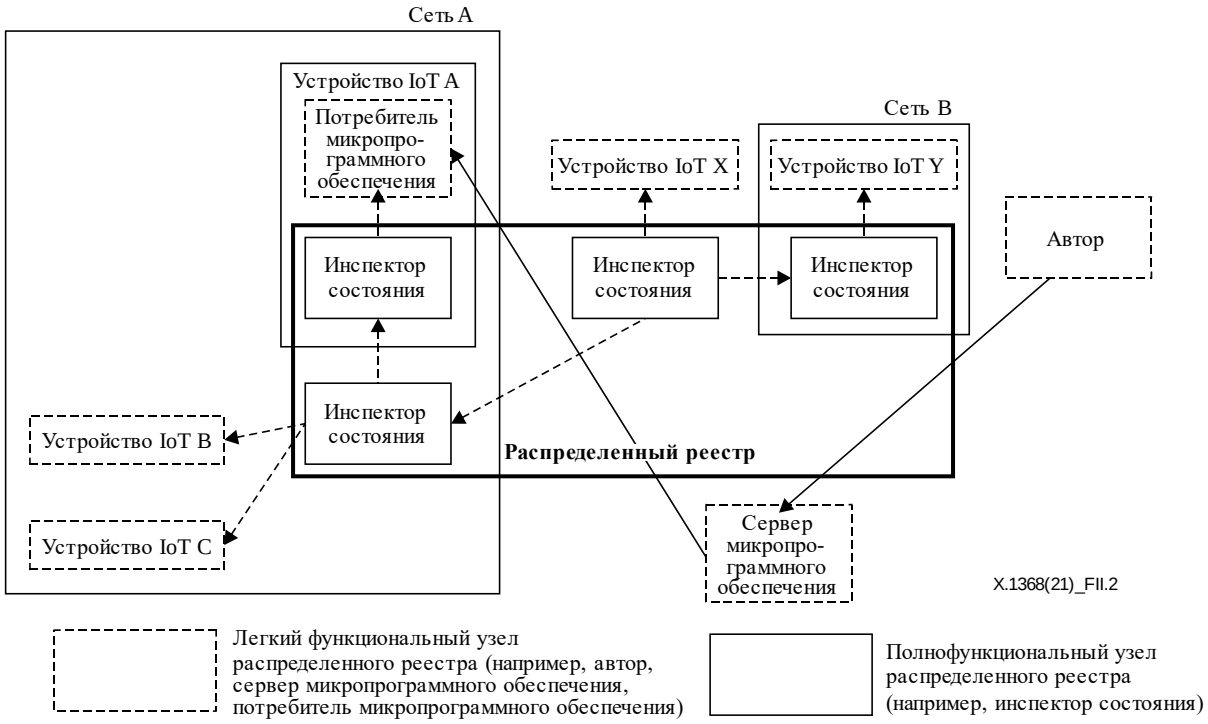

Рисунок II.2 − Обновление программного обеспечения на основе распределенного реестра в нескольких сетях

Библиография

[b-IETF RFC 2119] IETF RFC 2119 (1997), *Key words for use in RFCs to indicate requirement levels.*

[b-IETF architecture] IETF SUIT (2019). *A firmware update architecture for Internet of things*., Wilmington, DE: Internet Engineering Task Force. Available [viewed 2021-02-19] at: https://tools.ietf.org/html/draft-ietf-suit-architecture-08

[b-IETF manifest] Moran, B., Tschofenig, H., Birkholz, H. (2019). *Firmware updates for Internet of things devices – An information model for manifests.* Wilmington, DE: Internet Engineering Task Force. Available [viewed 2021-02-19] at: https://tools.ietf.org/id/draft-ietf-suit-information-model-02.html

[b-IETF suit] IETF (2021). *Software updates for the internet of things (suit)*, version 7.26.0. Wilmington, DE: Internet Engineering Task Force. Available [viewed 2021-02-19] at: https://datatracker.ietf.org/wg/suit/about/

[b-ISOC iotsu] Internet Architecture Board (Internet), *Internet of things software update workshop (IoTSU) 2016*. Reston, VA: Internet Society. Available [viewed 2021-02-20] at: https://www.iab.org/activities/workshops/iotsu/

[b-oneM2M] oneM2M (2017), *Standards for M2M and the Internet of things*. oneM2M. Available [viewed 2021-02-20] at: http://www.onem2m.org/technical/published-drafts

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
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	Качество телефонной передачи, телефонные установки, сети местных линий
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 протокола Интернет, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2021 г.