Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1361

(09/2018)

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

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

Структура безопасности интернета вещей на основе модели с использованием шлюза

Рекомендация МСЭ-Т X.1361

ITU-T

Международный союз электросвязи

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 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 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 сетей (ИТС)	X.1370–X.1389
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/состояния	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

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

Рекомендация МСЭ-Т X.1361

Структура безопасности интернета вещей на основе модели с использованием шлюза

Резюме

В Рекомендации МСЭ-Т X.1361 описывается структура безопасности интернета вещей (IoT) с использованием шлюзов безопасности. IoT – это глобальная инфраструктура для информационного общества, которая делает возможным предоставление перспективных услуг путем присоединения (физического и виртуального) вещей на основании существующих и развивающихся функционально совместимых информационно-коммуникационных технологий.

В настоящей Рекомендации проводится анализ угроз и проблем безопасности в среде интернета вещей и дается описание возможностей обеспечения безопасности, позволяющих снижать эти угрозы и решать проблемы безопасности. Представлена базовая методика определения тех возможностей обеспечения безопасности, которые необходимы для снижения угроз и решения проблем безопасности в сфере интернета вещей.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1361	07.09.2018 г.	17-я	11.1002/1000/13607

Ключевые слова

Интернет вещей, структура безопасности, требования безопасности.

* 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 в целях 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 X.1361

Структура безопасности интернета вещей на основе модели с использованием шлюза

1 Сфера применения

В настоящей Рекомендации описывается структура безопасности интернета вещей (IoT) с использованием шлюзов безопасности.

В частности, в ней проводится анализ угроз и проблем безопасности в среде интернета вещей и дается описание возможностей обеспечения безопасности, позволяющих снижать эти угрозы и решать проблемы безопасности. Представлена методика определения тех возможностей обеспечения безопасности, которые необходимы для снижения угроз и решения проблем безопасности в сфере интернета вещей.

В настоящей Рекомендации основное внимание уделяется возможностям, связанным с использованием шлюзов безопасности, и рассматривается эталонная модель, описанная в [b-ITU-T Y.4401], с упором на технические, а не управленческие аспекты.

2 Справочные документы

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

[ITU-T Y.4100] Recommendation ITU-T Y.4100/Y.2066 (2014), *Common requirements of the Internet of things*.

3 Термины и определения

3.1 Термины, определенные в других документах

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

3.1.1 атака (attack) [b-ISO13491-1]: Попытка злоумышленника получить или изменить на устройстве конфиденциальную информацию или услугу, которую ему не разрешено получать или изменять.

3.1.2 аутентификация (authentication) [b-NIST SP 800-53]: Проверка идентичности пользователя, процесса или устройства, нередко являющаяся необходимым условием обеспечения возможности доступа к ресурсам информационной системы.

3.1.3 возможность (capability) [b-ISO 19440]: Конструкция, представляющая собой совокупность характеристик (выраженных в виде атрибутов способности), либо ресурсов (обеспеченная возможность), либо деятельности предприятия (необходимая возможность).

ПРИМЕЧАНИЕ. – Допускается объединение возможностей.

3.1.4 контекст (context) [b-ITU-T X.1252]: Среда с определенными граничными условиями, в которой существуют и взаимодействуют объекты.

3.1.5 алгоритм шифрования (cryptographic algorithm) [b-ISO/IEC 19790]: Четко определенная вычислительная процедура, принимающая входные переменные, которые могут включать в себя ключи шифрования, и выдающая выходные данные.

3.1.6 случайное число криптографического качества (cryptographic-quality random-number) [b-ITU-T X.667]: Случайное или псевдослучайное число, генерированное механизмом, обеспечивающим достаточный разброс многократно генерируемых значений, которое должно быть приемлемо для использования в криптографической работе (или используется в такой работе).

3.1.7 криптография (cryptography) [b-ITU-T X.800]: Дисциплина, включающая принципы, средства и методы для преобразования данных, необходимые для того, чтобы скрыть содержащуюся в них информацию, предотвратить их скрытое изменение и/или предотвратить несанкционированное использование.

ПРИМЕЧАНИЕ. – Криптография определяет методы, используемые при шифровании и дешифровании. Атака на криптографический принцип, средство или метод называется криптоанализом.

3.1.8 криптосистема (cryptosystem) [b-ISO 11568-1]: Набор криптографических примитивов, используемых для предоставления услуг информационной безопасности.

3.1.9 устройство (device) [ITU-T Y.4000]: Применительно к интернету вещей означает элемент оборудования, который обладает обязательными возможностями связи и дополнительными возможностями измерения, срабатывания, а также ввода, хранения и обработки данных.

3.1.10 управление определением идентичности (identity management) [b-ITU-T X.1250]: Набор функций и возможностей (например, администрирование, управление и техническое обслуживание, обнаружение, обмен сообщениями, сопоставление и связь, обеспечение реализации политики, аутентификация и утверждение), используемых для:

– гарантирования информации, подтверждающей идентичность (например, идентификаторов, полномочий, атрибутов);

– гарантирования идентичности объекта (например, пользователей/абонентов, групп, устройств пользователей, организаций, поставщиков доступа к сети и поставщиков услуг, сетевых элементов и объектов, а также виртуальных объектов); и

– поддержки коммерческих приложений и приложений безопасности.

3.1.11 интернет вещей (Internet of things (IoT)) [b-ITU-T Y.4000]: 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 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.

3.1.12 обнаружение вторжений (intrusion detection) [b-ISO/IEC 27039]: Формальный процесс выявления вторжений, который обычно характеризуется сбором информации об аномалиях в использовании систем, а также о том, какая уязвимость была использована, в каких именно системах и каким образом, включая то, когда и как это произошло.

3.1.13 система обнаружения вторжений (intrusion detection system) [b-ISO/IEC 27039]: Информационные системы, используемые для выявления попыток вторжения, совершаемых или совершенных вторжений.

3.1.14 предотвращение вторжений (intrusion prevention) [b-ISO/IEC 27033-1]: Формальный процесс активного реагирования с целью предотвратить вторжение.

3.1.15 система предотвращения вторжений (intrusion prevention system) [b-ISO/IEC 27039]: Разновидность систем обнаружения вторжений, специально предназначенных для обеспечения возможности активного реагирования.

3.1.16 управление ключами (key management) [b-ITU-T X.800]: Генерирование, хранение, распределение, удаление, архивирование и применение ключей в соответствии со стратегией безопасности.

3.1.17 облегченное шифрование (lightweight cryptography) [b-ISO/IEC 29192-1]: Алгоритм шифрования, приспособленный для реализации в средах с ограниченными ресурсами.

3.1.18 вредоносное программное обеспечение (malware) [b-ISO/IEC 27033-1]: Вредоносное программное обеспечение, предназначенное специально для повреждения или разрушения системы путем нарушения конфиденциальности, целостности и/или доступности.

ПРИМЕЧАНИЕ. – К примерам вредоносного программного обеспечения относятся вирусы и трояны.

3.1.19 сетевой мониторинг (network monitoring) [b-ISO/IEC 27033-1]: Процесс непрерывного наблюдения и проверки регистрируемых данных об активности и операциях в сети, включая журналы аудита и оповещения и связанный с этим анализ.

3.1.20 информация, позволяющая установить личность (personally identifiable information (PII)) [b-ISO/IEC 29100]: Любая информация, которая a) может быть использована для идентификации субъекта PII, к которому такая информация относится, или b) прямо или косвенно связана либо может быть связана с субъектом PII.

ПРИМЕЧАНИЕ. – Чтобы определить, возможна ли идентификация субъекта PII, следует учесть все способы идентификации этого физического лица, которые, исходя из разумных предположений, может использовать заинтересованное лицо, хранящее данные, или любая другая сторона.

3.1.21 ассоциация безопасности с маскированием (security association with mask (SAM)) [b-ITU-T X.1362]: Набор параметров, зависящий от протокола безопасности. SAM определяет услуги и механизмы, необходимые для защиты трафика путем шифрования с присоединенными данными для маскирования (EAMD). SAM определяется связанным с ней протоколом в зависимости от уровней протокола, например транспортного уровня или уровня протокола Интернет (IP). В этих параметрах могут быть указаны идентификаторы алгоритмов, режимы, идентификаторы уровней, на которых применяется EAMD, и криптографические ключи.

3.1.22 датчик (sensor) [b-ITU-T Y.4105]: Электронное устройство, которое измеряет физическое состояние или химический состав и доставляет электронный сигнал, соответствующий наблюдаемой характеристике.

3.1.23 вещь (thing) [b-ITU-T Y.4000]: Применительно к интернету вещей означает предмет физического мира (физические вещи) или информационного мира (виртуальные вещи), который может быть идентифицирован и интегрирован в сети связи.

3.1.24 угроза (threat) [b-ISO/IEC 27000]: Потенциальная причина нежелательного инцидента, который может нанести ущерб системе или организации.

3.1.25 уязвимость (vulnerability) [b-ISO/IEC 27000]: Слабое место актива или мер контроля, которое может быть использовано одной или несколькими угрозами.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины.

3.2.1 согласование алгоритма шифрования (cryptographic algorithm negotiation): Механизм, посредством которого определяются тип алгоритма и длина ключей шифрования, подлежащие использованию в ходе интегрированного сеанса шифрованной связи, а также наиболее подходящий для обеих сторон алгоритм шифрования.

ПРИМЕЧАНИЕ. – Это определение взято с некоторыми изменениями из [b-ISO/IEC 27033-1]. В настоящей Рекомендации "шлюз безопасности" именуется "шлюзом".

3.2.2 управление внесением исправлений (patch management): Процесс, включающий в себя получение, тестирование и установку множества исправлений в информационные системы.

ПРИМЕЧАНИЕ. – Можно рассмотреть возможность управления уязвимостями.

3.2.3 утечка PII (PII breach): Ситуация, когда обработка информации, позволяющей установить личность, происходит в нарушение одного или нескольких применимых требований защиты PII.

3.2.4 модель предпочтений в отношении конфиденциальности (privacy preference model): Модель, позволяющая веб-сайтам заявлять о предполагаемом способе использования данных, которые они собирают о частных лицах, чтобы те могли лучше контролировать использование своей личной информации.

3.2.5 настройка безопасной конфигурации (secure configuration): Рекомендуемый процесс настройки сетевых устройств, позволяющий снизить уровень присущих этим устройствам уязвимостей и обеспечить предоставление только тех услуг, которые необходимы в рамках назначенной роли.

ПРИМЕЧАНИЕ. – Этот процесс включает следующее: удаление или отключение ненужных программ и учетных записей пользователей; установку надежного пароля вместо заданного по умолчанию; включение брандмауэра и его настройку для блокирования по умолчанию всех соединений, кроме утвержденных; отключение функции автоматического запуска.

3.2.6 шлюз безопасности (security gateway): Точка соединения между сетями, или подгруппами внутри сетей, или программными приложениями различных доменов безопасности, которая предназначена для защиты сети в среде интернета вещей в соответствии с заданной политикой безопасности.

3.2.7 атака по сторонним каналам (side-channel attack): Атака с использованием информации, полученной из физической реализации криптосистемы.

ПРИМЕЧАНИЕ. – Для взлома криптосистем могут использоваться, например, данные о временны́х характеристиках вычислений, энергопотреблении и утечках электромагнитной энергии.

3.2.8 управление уязвимостями (vulnerability management): Процесс, включающий выявление, классификацию, устранение уязвимостей и смягчение их последствий.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

DoS	Denial of Service	Отказ в обслуживании
EAMD	Encryption with Associated Mask Data	Шифрование с присоединенными данными для маскирования
IDS	Intrusion Detection System	Система обнаружения вторжений
IoT	Internet of things	Интернет вещей
IP	Internet Protocol	Протокол Интернет
IPS	Intrusion Prevention System	Система предотвращения вторжений
PII	Personally Identifiable Information	Информация, позволяющая установить личность

5 Условные обозначения

Отсутствуют.

6 Обзор

Интернет вещей (IoT) определяется как глобальная инфраструктура для информационного общества, которая делает возможным предоставление перспективных услуг путем присоединения (физического и виртуального) вещей на основании существующих и развивающихся функционально совместимых информационно-коммуникационных технологий.

Типичная развернутая система IoT состоит из граничных устройств с датчиками в проводной или беспроводной сети, передающих данные через шлюз в общедоступное или частное облако. Особенности топологии такой системы могут существенно различаться в зависимости от конкретного применения; например, в некоторых случаях шлюз может располагаться на устройстве. Устройства на базе такой топологии могут изначально создаваться с поддержкой IoT или же наделяться соответствующими возможностями после их развертывания.

7 Функциональная архитектура и структура

В основу настоящей Рекомендации положена функциональная архитектура IoT, представленная на рисунке 1.

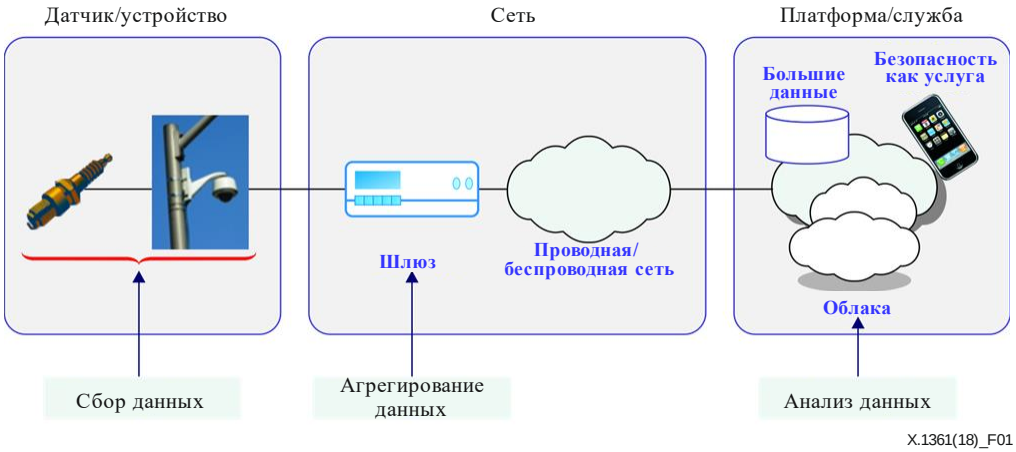

Рисунок 1 – Функциональная архитектура IoT (упрощенная)

Передача данных между конечной точкой IoT (датчиком или устройством) и шлюзом может осуществляться по сетям связи двух типов: сети на базе протокола Интернет (IP-сети) и сети, не являющейся IP-сетью. Предполагается, что связь между шлюзом и компонентом платформы IoT, развернутым в центре обработки данных (ЦОД), должна вестись по IP-протоколу. Поэтому в случае сети, не являющейся IP-сетью, соединение по такой сети должно быть завершено и вновь установлено по IP-сети в шлюзе.

Функциональная архитектура может быть уточнена, как показано на рисунке 2.

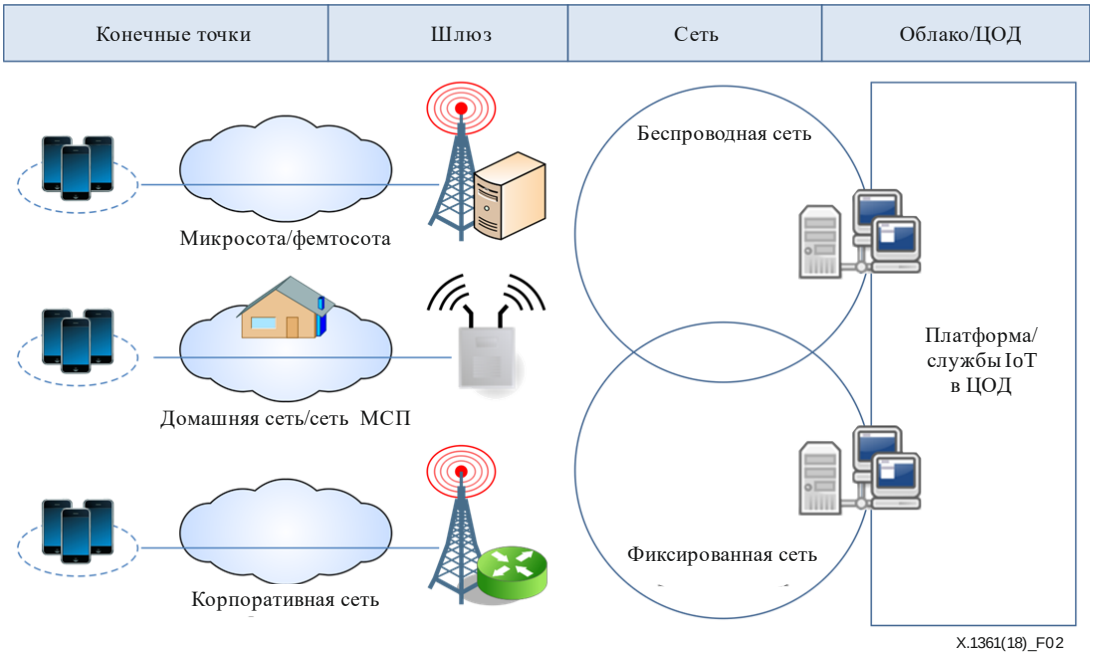

Рисунок 2 – Практическая функциональная архитектура

Например, в интеллектуальной транспортной системе шлюз, показанный на рисунке 2, может играть роль бортового мобильного шлюза, который соединяет внутреннюю сеть автомобиля с внешней открытой сетью.

В состав шлюза должна входить такая возможность, как брандмауэр, чтобы управлять трафиком, конечной точкой для которого является устройство. Некоторые устройства IoT имеют собственные транспортные протоколы, отличные от TCP/IP. Проприетарные протоколы могут использоваться для управления связью между устройствами IoT. Соответственно требуются возможности фильтрации по отраслевым протоколам для выявления вредоносного контента, который может в скрытой форме передаваться по протоколам, отличным от IP.

В шлюзе должна быть реализована функция для фильтрации конкретных данных, конечной точкой для которых служит соответствующее устройство, причем ее реализация должна обеспечивать оптимальное использование ограниченных вычислительных ресурсов.

Шлюз занимает особое положение в функциональной архитектуре. Зачастую он служит первым надежным рубежом защиты в системе IoT, поскольку конечные точки наиболее уязвимы к внесению физических изменений. Учитывая роль, которую играет шлюз в IoT, целесообразно выделить его из сети как самостоятельный актив для обеспечения безопасности. В работе шлюза должны быть учтены ограничения, свойственные узлам с датчиками. Нередко шлюз выполняет определенные функции обеспечения безопасности для конечных точек, которые ограничены в ресурсах, например управление ключами, согласование протокола шифрования, предотвращение вторжений.

Возможности обеспечения безопасности, реализованные в шлюзе, могут существенно различаться в зависимости от таких факторов, как мощность и возможности конечных точек, структура услуги, устройство сети, физическое местоположение и контекст использования.

8 Угрозы безопасности интернета вещей

8.1 Угрозы безопасности датчиков/устройств IoT

Угрозы, специфичные для датчиков/устройств.

– Захват устройства – физическая компрометация устройства или утрата его ключей.

– Атака типа "черная дыра" – атака, при которой скомпрометированное устройство замыкает на себя трафик, образуя "черную дыру" или вводя избирательную переадресацию. Злоумышленник компрометирует подлинное устройство или внедряет в сеть фальшивое устройство, с которого и инициируется такая атака. Скомпрометированное устройство пытается замкнуть на себя весь трафик данных от соседних узлов на основе метрики маршрутизации, используемой в протоколе маршрутизации. Осуществив это, устройство инициирует атаку. Атака типа "черная дыра" – это атака на сетевой уровень, при которой скомпрометированное устройство передает соседям ложную информацию о маршрутизации, чтобы замкнуть на себя сетевой трафик. Беспроводные сети особенно уязвимы для таких атак из-за наличия специальных сетей и модели связи "многие к одному", когда множество узлов передают данные на одну базовую станцию. Исходя из характера информационных потоков в беспроводной сети атаку типа "черная дыра" не обязательно направлять на все узлы – достаточно тех, которые расположены поблизости от базовой станции.

– Атака типа "Сибилла" – атака, при которой несанкционированное устройство незаконно пользуется несколькими идентификаторами. Дополнительный идентификатор такого устройства называют "узел Сибиллы". Эта атака инициируется в связке с другими типами атак, чтобы снизить эффективность механизмов обеспечения отказоустойчивости, таких как распределенное хранение, многотрактовая маршрутизация и поддержание топологии.

– Лавинная атака – разновидность атаки типа "отказ в обслуживании" (DoS), при которой злоумышленник передает на целевое устройство последовательность пакетов приветствия в попытке потребить такой объем ресурсов устройства, который был бы достаточен для того, чтобы оно перестало откликаться на законный трафик.

– Атаки с избирательной переадресацией – атака, при которой скомпрометированный узел случайным образом фильтрует принятые пакеты и переадресовывает некоторые из них на следующий узел. Если узел отфильтровывает (отбрасывает) все принятые пакеты, соответствующая атака называется "черная дыра".

– Атака типа "червоточина" – атака, при которой два несанкционированных/скомпрометированных узла сообщают о наличии между ними очень короткого пути. Туннель – это тракт передачи данных между двумя сетевыми устройствами, создаваемый через существующую сетевую инфраструктуру. Сеть, которая использует туннелирование для передачи данных в другую сеть, получает эти данные из одной сети и передает их копию в другую сеть через туннель, из-за чего работа этой второй сети может нарушаться. В этот момент злоумышленник может легко войти в сеть и неправомерно воспользоваться ею. В связке с атаками типа "черная дыра" и "Сибилла" такая атака может привести к избирательной переадресации или образованию "черной дыры".

– Маскировка под датчик/устройство – атака, при которой злоумышленник успешно выдает себя за подлинный датчик или устройство.

8.2 Угрозы безопасности шлюзов IoT

Угрозы, специфичные для шлюзов.

– Несанкционированный доступ – последствиями несанкционированного доступа к шлюзу могут стать раскрытие конфиденциальной информации, изменение данных, отказ в обслуживании и использование ресурсов в незаконных целях. Например, получив доступ к шлюзу, злоумышленник может просматривать данные, которые теперь передаются без шифрования, и узнавать имена пользователей, пароли и данные безопасной конфигурации.

– Несанкционированный шлюз – даже если все беспроводные шлюзы защищены, злоумышленник может без труда самостоятельно развернуть несанкционированный шлюз. Например, не в меру усердный сотрудник может установить в офисе точку беспроводного доступа без учета требований безопасности. Это позволит реально обойти многие из принятых мер безопасности и даже может создать радиопомехи служебному оборудованию организации и/или предприятия. Несанкционированная точка беспроводного доступа также может быть установлена преднамеренно и скрытно, чтобы обеспечить злоумышленнику легкий локальный или удаленный доступ в сеть. В этой атаке, известной под названием "злой двойник", злоумышленник может заменить имеющуюся точку беспроводного доступа другой, к которой у него есть полный доступ для настройки и мониторинга, или даже развернуть несанкционированную точку беспроводного доступа со схожими настройками, но большей относительной мощностью, чтобы она перебивала сигнал законной точки доступа. После того как законное устройство обманным путем было побуждено подключиться к несанкционированному шлюзу, с него можно собирать конфиденциальную информацию о соединении.

– Атака типа "отказ в обслуживании" – DoS-атака вынуждает устройство – объект атаки существенно замедлить предоставление своих услуг, а в идеальном случае – прекратить их предоставление из-за исчерпания памяти и/или вычислительной мощности устройства. Объект атаки перегружается незаконным трафиком, который передают на него злоумышленники. Особенно уязвимы к DoS-атакам беспроводные сенсорные сети из-за таких своих характеристик, как открытость среды, динамически меняющаяся топология и отсутствие четкой линии защиты. Такие атаки становятся все более обостряющейся проблемой в современных сетях. Многие методы защиты от них, разработанные для фиксированных проводных сетей, неприменимы в сетях подвижной связи.

8.3 Угрозы безопасности сетей

Угрозы, специфичные для сетей.

– Несанкционированный доступ – последствиями несанкционированного доступа к беспроводной сенсорной сети могут стать раскрытие конфиденциальной информации, изменение данных, отказ в обслуживании и использование ресурсов в незаконных целях. Например, получив доступ к сенсорной сети, злоумышленник может просматривать данные, которые теперь передаются без шифрования, и узнавать имена пользователей и пароли.

– Анализ пакетов – в беспроводных сенсорных сетях, где не предусмотрены возможности шифрования, злоумышленникам обычно легко перехватывать передаваемые сообщения. Для такого перехвата требуются антенна, обычные технические средства для работы в беспроводных сетях и анализатор пакетов. Анализатор сетевых пакетов – это средство, которое

переводит сетевую карту в неизбирательный режим. В этом режиме интерфейс принимает и обрабатывает весь трафик, а не только тот, который ему адресован. Анализатор пакетов отображает для своего пользователя все сетевые пакеты и осуществляет декодирование, чтобы облегчить чтение информации. Трафик в виде обычного текста легок для восприятия, и можно задать фильтры для поиска определенных ключевых слов или значений.

– Несанкционированная передача через Bluetooth – эта атака ориентирована на мобильные устройства, поддерживающие технологию Bluetooth, например сотовые телефоны. Злоумышленник инициирует атаку, рассылая пользователям таких устройств незапрашиваемые сообщения. Сами эти сообщения не причиняют вреда устройству, ставшему объектом атаки, но могут побудить пользователя ответить тем или иным образом или добавить контакт в адресную книгу устройства.

– Несанкционированный доступ через Bluetooth – при такой атаке злоумышленник осуществляет несанкционированный доступ к информации на беспроводном устройстве, ставшем объектом атаки, по соединению Bluetooth. Часто в роли атакующих устройств и объектов атаки выступают телефоны, настольные компьютеры, ноутбуки и персональные цифровые ассистенты (PDA). Успешная атака может привести к несанкционированному доступу к личной и конфиденциальной информации, хранящейся на этих устройствах.

8.4 Угрозы безопасности для платформы/служб

В интернете главной задачей на прикладном уровне является сбор и обработка больших объемов пользовательских данных, в том числе их личной информации или конфиденциальной информации о различных транзакциях. Основной мишенью злоумышленника служат данные, которые он стремится похитить, изменить или повредить. Соответственно необходимо обеспечить безопасность данных с использованием механизмов защиты конфиденциальности. К угрозам на прикладном уровне относятся массовая обработка данных, выход "умных" устройств из-под контроля, несанкционированное вмешательство человека и невозможность восстановления работы вышедших из-под контроля устройств после аварийной ситуации.

Угрозы, специфичные для платформы/служб.

– Профилирование – разведывательный сбор информации о платформе/службе.

– Атака типа "отказ в обслуживании" – атака, при которой осуществляют перегрузку платформы/службы большим количеством запросов на обслуживание с целью вынудить ее к отказу в обслуживании законных клиентских запросов.

– Выполнение произвольного кода – атака, представляющая собой попытку запустить вредоносный код на платформе/в службе, чтобы скомпрометировать ее ресурсы, а затем инициировать другие атаки.

– Выполнение вредоносного кода – под вредоносным кодом понимается часть программной системы или сценарий, срабатывание которых должно вызывать нежелательные последствия, например создавать брешь в защите, способствовать утечке информации, позволяющей установить личность (PII), или повреждать систему. Типичными примерами могут служить вирусы, черви и трояны.

– Несанкционированное повышение уровня привилегий – атака, при которой выполнение кода осуществляется с использованием учетной записи привилегированного процесса для повышения уровня привилегий злоумышленника.

– SQL-инъекция – эксплуатация уязвимостей в коде приложения, отвечающем за проверку входных данных и доступ к данным, в целях выполнения произвольных команд, которые несанкционированно вносят или извлекают информацию.

– Сетевой перехват – атака, при которой осуществляется перехват пакетов, передаваемых из сети, и чтение данных из них в попытке найти критичную информацию, такую как пароли, маркеры сеанса или конфиденциальная информация любого вида.

– Несанкционированный доступ – атака, при которой злоумышленник получает доступ к платформе/службе с использованием чужой учетной записи или другим способом. Например, подбор чужого пароля или имени пользователя считается несанкционированным доступом.

– Полный перебор – атака с систематическим перебором всех возможных ключей до тех пор, пока не будет найден правильный ключ.
– Словарная атака для определения имен пользователей/паролей – атака, представляющая собой систематическое преодоление механизмов шифрования или аутентификации путем перебора слов по словарю в поисках пароля.
– Использование заданных по умолчанию имен пользователей и паролей/ненадежных паролей – атака, при которой злоумышленник использует заданные по умолчанию имена пользователей и пароли/ненадежные пароли для получения доступа к платформе/службам.
– Атака на основе логических выводов – атака, при которой используется способность путем логических рассуждений вывести защищенную информацию из доступных на правомерной основе фрагментов информации с более низкой степенью секретности.
– Утечка PII – преднамеренный или непреднамеренный выпуск информации, позволяющей установить личность, в ненадежную среду.

9 Требования безопасности для интернета вещей

В основу настоящей Рекомендации положены требования высокого уровня, описанные в [ITU-T Y.4100] (см. Приложение A).

10 Возможности безопасности для интернета вещей

10.1 Обзор

В настоящей Рекомендации рассматриваются только требования безопасности с учетом надежности и качества обслуживания. Возможности безопасности для IoT расширены по сравнению с описанными в [b-ITU-T Y.4401].

Общие возможности

Архитектура IoT должна включать в себя следующие возможности:

– безопасная связь для поддержки доверенной связи с обеспечением безопасности и защиты конфиденциальности данных;
– безопасное управление ключами для поддержки безопасной связи;
– безопасное управление данными для доверенного управления данными с обеспечением безопасности и защиты их конфиденциальности;
– аутентификация для проверки подлинности устройств;
– авторизация (контроль доступа) для авторизации устройств;
– аудит для обеспечения полностью прозрачного, прослеживаемого и воспроизводимого мониторинга доступа к данным и попыток доступа к приложениям IoT на основе соответствующих нормативно-правовых актов;
– безопасное предоставление услуг для доверенного предоставления услуг с обеспечением безопасности и защиты конфиденциальности;
– интеграция безопасности для интеграции различных стратегий и методов обеспечения безопасности, относящихся к разным функциональным компонентам IoT;
– реализация безопасных протоколов с использованием общедоступных и стандартизированных алгоритмов шифрования;
– реализация безопасных протоколов на основе облегченного шифрования;
– безопасное и устойчивое обновление программного обеспечения, в частности модулей или приложений;
– управление определением идентичности для устройств/датчиков, шлюзов, платформ/служб IoT;
– сканирование на предмет уязвимостей;

– мониторинг доступа к данным и попыток доступа к приложениям IoT на основе полной прозрачности, прослеживаемости и воспроизводимости;
– аппаратная защита (например, на базе модуля доверенной платформы) для предотвращения рисков, связанных с физическим доступом, которые возникают в результате виртуализации сетей и шлюзов;
– многотрактовая маршрутизация для предотвращения атак с избирательной переадресацией;
– защита PII от утечек на протяжении всего жизненного цикла PII;
– настройка безопасной конфигурации;
– использование облегченного шифрования; и
– простое шифрование с присоединенными данными для маскирования (EAMD) [b-ITU-T X.1362] для связи с другими объектами, включая шлюз.

Возможности, связанные с алгоритмами шифрования

Архитектура IoT должна включать в себя следующие возможности:

– генерация случайных чисел криптографического качества для поддержки управления ключами [b-IETF RFC 4086];
– периодическое обновление необходимых ключей шифрования для потокового вещания; и
– использование стандартизированных алгоритмов шифрования.

Возможности, связанные с контекстом

Архитектура IoT должна включать в себя следующие возможности:

– устойчивость к атакам по сторонним каналам;
– поддержка безопасной практики программирования, обеспечивающей тщательную проверку вводимых данных в системах, службах, приложениях баз данных и веб-услугах; и
– плановая оценка рисков для определения рисков, возникающих в различных эксплуатационных контекстах.

10.2 Возможности безопасности для датчиков/устройств

В датчиках/устройствах IoT должны быть предусмотрены следующие возможности:

– управление ключами;
– согласование алгоритмов шифрования;
– шифрование данных, включая в некоторых случаях данные плоскости сигнализации, контроля и управления, для уменьшения проблем безопасности, связанных с конфиденциальностью данных, передаваемых по беспроводным сетям;
– обеспечение целостности данных, передаваемых по беспроводным сетям, с использованием соответствующих схем защиты целостности, которые гарантируют, что пользовательские данные или данные плоскости сигнализации, контроля и управления не были искажены или изменены;
– аутентификация источника данных или проверка подлинности датчиков/устройств IoT, а также администраторов и обслуживающего персонала сенсорных сетей;
– управление внесением исправлений, включая обновление защищенных программных модулей;
– реализация безопасных протоколов на основе облегченного шифрования;
– контроль доступа, гарантирующий, что доступ к элементам сети, хранимой информации, информационным потокам, услугам и приложениям имеют только авторизованные пользователи или устройства;
– обнаружение и/или предотвращение несанкционированного изменения;
– генерация случайных чисел криптографического качества для поддержки управления ключами;
– устойчивость к атакам по сторонним каналам;

– обнаружение вредоносного программного обеспечения и защита от него; и

– защита от утечек PII.

В устройствах IoT должны быть предусмотрены следующие возможности:

– проверка подлинности и целостности программного обеспечения на устройстве с использованием криптографически созданных цифровых подписей [b-ISO/IEC 9796-3];

– брандмауэр, обнаружение вторжений, защита от вторжений или углубленная проверка пакетов для управления трафиком, завершающимся в устройстве; и

– настройка безопасной конфигурации.

10.3 Возможности безопасности для шлюзов

В шлюзах должны быть предусмотрены следующие возможности:

– система обнаружения вторжений (IDS)/система предотвращения вторжений (IPS);

– управление ключами;

– настройка безопасной конфигурации;

– согласование алгоритмов шифрования;

– шифрование данных, включая в некоторых случаях данные плоскости сигнализации, контроля и управления, передаваемые между шлюзом и устройствами или компонентами IoT в центре обработки данных, для уменьшения проблемы безопасности, связанной с конфиденциальностью данных, передаваемых по беспроводным сетям;

– обеспечение целостности данных, передаваемых по беспроводным сетям, с использованием соответствующих схем защиты целостности, которые гарантируют, что пользовательские данные или данные плоскости сигнализации, контроля или управления не были искажены или изменены;

– поддержание готовности к противодействию DoS-атакам различными методами – от безопасной разработки исходных программ, анализа исходного кода и тестирования на уязвимости до использования системы обнаружения или предотвращения вторжений в сети или на хосте;

– аутентификация источника данных или проверка подлинности датчиков/устройств IoT, а также администраторов и обслуживающего персонала сенсорных сетей;

– контроль доступа, гарантирующий, что доступ к элементам сети, хранимой информации, информационным потокам, услугам и приложениям имеют только авторизованные пользователи или устройства; и

– подотчетность устройств IoT, чтобы любое нарушение политики можно было проследить до конкретного устройства.

Шлюз должен поддерживать возможность обновления защищенных программных модулей.

10.4 Возможности безопасности для сетей

Возможности безопасности для сетей выходят за рамки настоящей Рекомендации.

ПРИМЕЧАНИЕ. – Можно использовать возможности безопасности, соответствующие аспектам безопасности, описанным в [b-ITU-T X.805].

10.5 Возможности безопасности для платформ/служб

В платформе/службе должны быть предусмотрены следующие возможности:

– защита регистрационных данных для криптографических операций – набора данных, удостоверяющих идентичность и/или полномочия;

– смена заданных по умолчанию имен пользователей и паролей в ходе первоначальной настройки;

– реализация надежных паролей и детализированной политики контроля доступа;

– блокирование ненужных портов;

– поддержка настройки безопасной конфигурации, например, для удаления ненужных услуг и программного обеспечения;
– защита от заражения вредоносными программами путем использования антивирусного программного обеспечения;
– реализация политики управления внесением исправлений;
– управление уязвимостями;
– обновление защищенных программных модулей и приложений;
– управление ключами для безопасного обмена сообщениями между шлюзом и платформой/службой;
– согласование алгоритмов шифрования для организации безопасного туннеля между шлюзом и платформой/службой в том случае, если необходим безопасный обмен сообщениями между шлюзом и платформой/службой;
– поддержание готовности к противодействию DoS-атакам;
– сетевой мониторинг;
– защита PII при хранении;
– обеспечение безопасности на прикладном уровне для предотвращения угроз и атак на прикладном уровне, описанных в пункте 8.4; и
– обеспечение поддержки для снижения последствий атак на основе логических выводов.

Приложение A

Требования безопасности и защиты конфиденциальности, описанные в Рекомендации МСЭ-T Y.4100/Y.2066

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

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.

В настоящем Приложении приводятся требования безопасности и защиты конфиденциальности высокого уровня, изложенные в Приложении A к [ITU-T Y.4100]. Заключенные в квадратные скобки обозначения в каждом пункте представляют собой ссылку на соответствующие элементы, определенные в Приложении A к [ITU-T Y.4100].

A.1 Безопасность связи

Требуется возможность доверенной 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].

A.2 Безопасность управления данными

Требуется возможность доверенного 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 и обработке данных в среде IoT [SP2].

A.3 Безопасность предоставления услуг

Требуется возможность доверенного 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].

A.4 Интеграция стратегий и методов обеспечения безопасности

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

A.5 Взаимная аутентификация и авторизация

Прежде чем предоставлять устройству (или пользователю IoT) доступ к интернету вещей, требуется провести взаимную аутентификацию и авторизацию устройства (или пользователя IoT) с интернетом вещей в соответствии с заранее установленной политикой безопасности [SP5].

A.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 нормативно-правовым актам. В частности, IoT должен поддерживать аудит безопасности в отношении передачи, хранения и обработки данных, а также доступа к приложениям [SP6].

Дополнение I

Возможности обеспечения безопасности и защиты конфиденциальности, описанные в Рекомендации МСЭ-T Y.4401/Y.2068

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

В настоящем Дополнении приводятся возможности обеспечения безопасности и защиты конфиденциальности высокого уровня, изложенные в [b-ITU-T Y.4401]. Заключенные в квадратные скобки обозначения в каждом пункте представляют собой ссылку на соответствующие элементы, определенные в [b-ITU-T Y.4401].

I.1 Безопасность связи

Безопасность связи – это возможность поддерживать доверенную связь с обеспечением безопасности и защиты конфиденциальности [C-7-1].

I.2 Безопасность управления данными

Безопасность управления данными – это возможность доверенного управления данными с обеспечением безопасности и защиты конфиденциальности [C-7-2].

I.3 Безопасность предоставления услуг

Безопасность предоставления услуг – это возможность доверенного предоставления услуг с обеспечением безопасности и защиты конфиденциальности [C-7-3].

I.4 Интеграция безопасности

Интеграция безопасности – это возможность интеграции различных стратегий и методов обеспечения безопасности, относящихся к разным функциональным компонентам IoT [C-7-4].

I.5 Взаимная аутентификация и авторизация

Взаимная аутентификация и авторизация – это возможность аутентификации и авторизации каждого устройства до предоставления ему доступа в IoT на основе заранее установленной политики безопасности [C-7-5].

I.6 Аудит безопасности

Аудит безопасности – это возможность полностью прозрачного, прослеживаемого и воспроизводимого мониторинга доступа к данным и попыток доступа к приложениям IoT на основе соответствующих нормативно-правовых актов [C-7-6].

ПРИМЕЧАНИЕ. – Эти возможности обеспечения безопасности и защиты конфиденциальности также включают возможность справляться с проблемами в этой сфере при работе в различных доменах безопасности.

Дополнение II

Представление реализации функциональной структуры IoT на базе функциональной архитектуры сетей последующих поколений, описанной в Рекомендации МСЭ-Т Y.4401/Y.2068

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

На рисунке II.1 показано представление реализации функциональной структуры IoT, построенное на базе функциональных объектов, описанных в функциональной архитектуре сетей последующих поколений (СПП) в [b-ITU-T Y.4401], которая связана с функциональной структурой безопасности, изложенной в настоящей Рекомендации. В данной Рекомендации определены возможности, относящиеся к уровню поддержки услуг и уровню устройств, которые изображены на рисунке 7-2 в [b-ITU-T Y.4401].

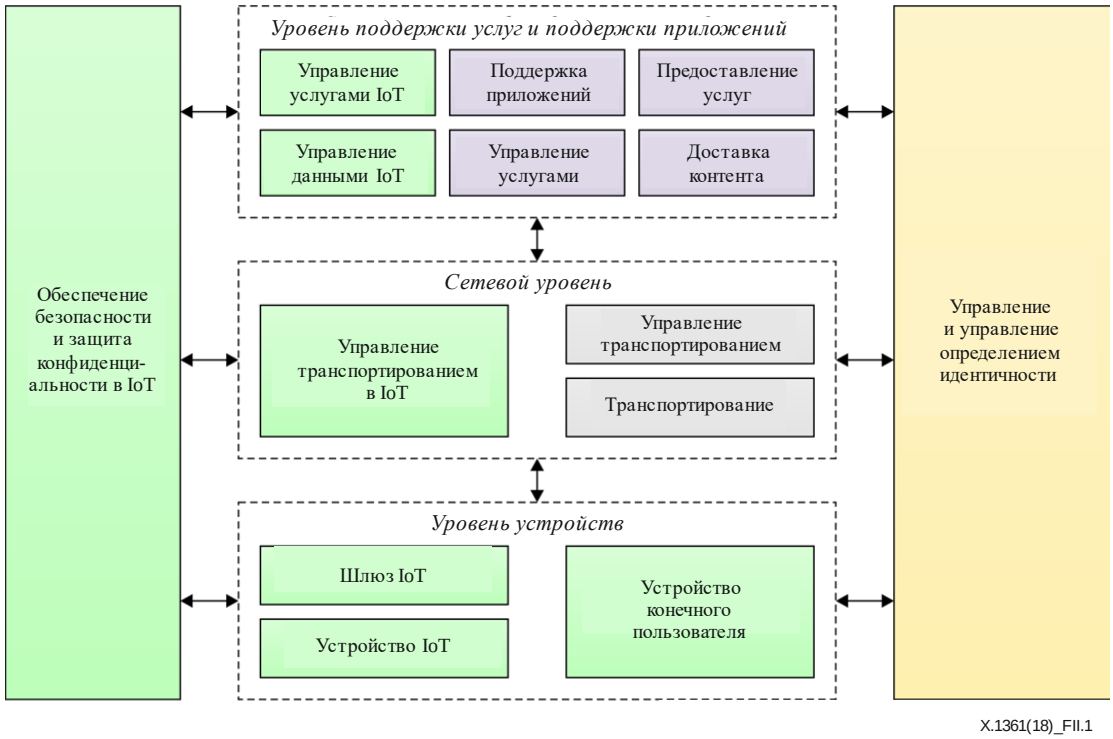

Рисунок II.1 – Представление реализации функциональной структуры IoT, построенное на базе функциональной архитектуры СПП

Библиография

[b-ITU-T X.667] Recommendation ITU-T X.667 (2012), *Information technology – Procedures for the operation of object identifier registration authorities: Generation of universally unique identifiers and their use in object identifiers.*

[b-ITU-T X.800] Рекомендация МСЭ-Т X.800 (1991 г.), Архитектура безопасности для взаимосвязи открытых систем для приложений МККТТ.

[b-ITU-T X.805] Рекомендация МСЭ-Т X.805 (2003 г.), Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами.

[b-IUT-T X.1250] Рекомендация МСЭ-Т X.1250 (2009 г.), Базовые возможности для улучшенного доверия и функциональной совместимости при глобальном управлении определением идентичности.

[b-ITU-T X.1252] Рекомендация МСЭ-Т X.1252 (2010 г.), Базовые термины и определения в области управления определением идентичности.

[b-ITU-T X.1311] Recommendation ITU-T X.1311 (2011) | ISO/IEC 29180:2012, Information technology – Security framework for ubiquitous sensor networks.

[b-ITU-T X.1362] Рекомендация МСЭ-Т X.1362 (2017 г.), Простая процедура шифрования для среды интернета вещей (IoT).

[b-ITU-T Y.4000] Рекомендация МСЭ-Т Y.4000/Y.2060 (2012 г.), Обзор интернета вещей.

[b-ITU-T Y.4050] Рекомендация МСЭ-Т Y.4050/Y.2069 (2012 г.), Термины и определения для интернета вещей.

[b-ITU-T Y.4105] Recommendation ITU-T Y.4105/Y.2221 (2010), *Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment.*

[b-ITU-T Y.4113] Recommendation ITU-T Y.4113 (2016), *Requirements of the network for the Internet of things.*

[b-ITU-T Y.4400] Рекомендация МСЭ-Т Y.4400/Y.2063 (2012 г.), Структура веб-сети вещей.

[b-ITU-T Y.4401] Recommendation ITU-T Y.4401/Y.2068 (2015), *Functional framework and capabilities of the Internet of things.*

[b-IETF RFC 4086] IETF RFC 4086 (2005), *Randomness Requirements for Security.*

[b-ISO 11568-1] ISO 11568-1:2005, *Banking – Key management (retail) – Part 1: Principles.*

[b-ISO 13491-1] ISO 13491-1:2016, *Financial services – Secure cryptographic devices (retail) – Part 1: Concepts, requirements and evaluation methods.*

[b-ISO 19440] ISO 19440:2007, *Enterprise integration – Constructs for enterprise modelling.*

[b-ISO/IEC 9796-3] ISO/IEC 9796-3:2006, *Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms.*

[b-ISO/IEC 19790] ISO/IEC 19790:2012, *Information technology – Security techniques – Security requirements for cryptographic modules.*

[b-ISO/IEC 27000] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary.*

[b-ISO/IEC 27033-1] ISO/IEC 27033-1:2015, *Information technology – Security techniques – Network security – Part 1: Overview and concepts.*

[b-ISO/IEC 27033-6] ISO/IEC 27033-6:2016, *Information technology – Security techniques – Network security – Part 6: Securing wireless IP network access.*

[b-ISO/IEC 27039] ISO/IEC 27039:2015, *Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems (IDPS).*

[b-ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework.*

[b-ISO/IEC 29192-1] ISO/IEC 29192-1:2012, *Information technology – Security techniques – Lightweight cryptography – Part 1: General.*

[b-NIST SP 800-53] NIST Special Publication 800-53 (2013), *Security and Privacy Controls for Federal Information Systems and Organizations*.

[b-ZT] Zhang Li, Tong Xin (2013), *Threat Modeling and Countermeasures Study for the Internet of Things*, Journal of Convergence Information Technology (JCIT), *Vol. 8, No. 5, March.*

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 в 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 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.