Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1369

(01/2022)

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

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

Требования безопасности для платформы услуг IoT

Рекомендация МСЭ-Т X.1369

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 (1)	X.1140–X.1149
Безопасность приложений (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.1350–X.1369**
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1399
Безопасность технологии распределенного реестра (DLT)	X.1400–X.1429
Безопасность приложений (2)	X.1450–X.1459
Безопасность веб-среды (2)	X.1470–X.1489
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
Киберзащита	X.1590–X.1599
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
Защита данных	X.1770–X.1789
БЕЗОПАСНОСТЬ СЕТЕЙ IMT-2020	X.1800–X.1819

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

Рекомендация МСЭ-Т X.1369

Требования безопасности для платформы услуг IoT

Резюме

В Рекомендации МСЭ-Т X.1369 определены требования безопасности для платформы услуг IoT. Проведена оценка угроз и проблем безопасности для платформы бизнес-услуг IoT и описаны меры обеспечения безопасности, которые могут смягчить угрозы и проблемы безопасности.

Хронологическая справка

Издание	Рекомендация	Утверждено	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1369	07.01.2022 г.	17-я	11.1002/1000/14799

Ключевые слова

IoT, платформа услуг, требования безопасности, риски нарушения 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.1369

Требования безопасности для платформы услуг IoT

1 Сфера применения

В настоящей Рекомендации определены требования безопасности для платформы услуг IoT. Проведена оценка угроз и проблем безопасности для платформы услуг IoT и описаны меры обеспечения безопасности, которые могут смягчить угрозы и проблемы безопасности.

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 источники могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ в данной Рекомендации не придает ему как отдельному документу статус Рекомендации.

[ISO/IEC 30141] ISO/IEC 30141 (2018), *Internet of things reference architecture.*

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используется следующий термин, определенный в другом документе.

3.1.1 интернет вещей (Internet of things (IoT)) [b-ITU-T Y.4000]: Глобальная инфраструктура для информационного общества, которая обеспечивает возможность предоставления сложных услуг путем соединения друг с другом объектов (физических и виртуальных) на основе существующих и развивающихся функционально совместимых информационно-коммуникационных технологий.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определен следующий термин.

3.2.1 платформа услуг IoT (IoT service platform): Системная платформа, к которой подключены устройства IoT и на которой выполняются приложения IoT.

С функциональной точки зрения платформа услуг обеспечивает возможности для управления устройствами, управления соединениями, поддержки приложений, проведения бизнес-анализа и т. д. С точки зрения управления данными платформа услуг IoT собирает, хранит и обрабатывает данные (включая личные данные и конфиденциальную информацию пользователей) для приложений IoT и углубленного анализа.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

API	Application Programming Interface	Интерфейс прикладного программирования
CSRF	Cross Site Request Forgery	Подделка межсайтовых запросов
DDoS	Distributed Denial of Service	Распределенный отказ в обслуживании
DoS	Denial of Service	Отказ в обслуживании

IMEI	International Mobile Equipment Identity		Международный идентификатор оборудования подвижной связи
PVLAN	Private VLAN		Частная VLAN
SIM	Subscriber Identity Module		Модуль идентификации абонента
SQL	Structured Query Language		Язык структурированных запросов
SSRF	Server Side Request Forgery		Подделка запросов на стороне сервера
VLAN	Virtual Local Area Network		Виртуальная локальная сеть
VM	Virtual Machine	ВМ	Виртуальная машина
VMM	Virtual Machine Monitor		Монитор виртуальных машин
XSS	Cross Site Script		Межсайтовый сценарий

5 Соглашения

В настоящей Рекомендации ключевые слова "требуется, чтобы" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящей Рекомендации.

6 Обзор

В [ISO/IEC 30141] определена эталонная объектная модель IoT, как показано на рисунке 1. Платформа услуг IoT – ключевой компонент показанной на этом рисунке *подсистемы приложений и услуг*, которая обеспечивает такие возможности, как управление устройствами, управление соединениями, поддержка приложений и анализ услуг. Платформа услуг IoT также обеспечивает сбор, хранение и анализ данных для приложений IoT.

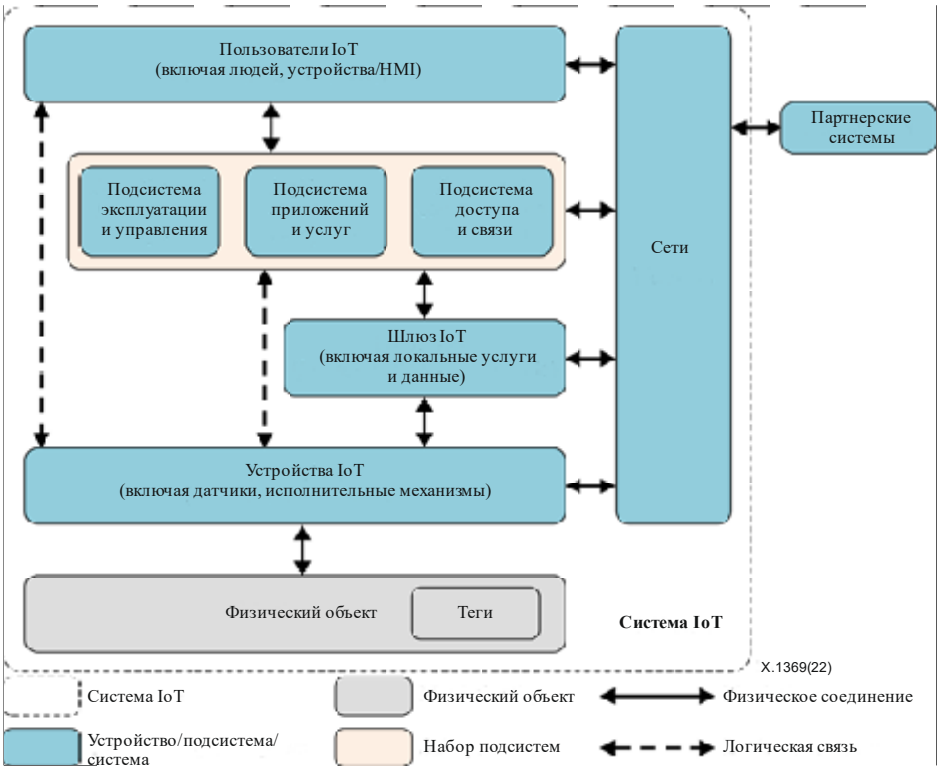

Рисунок 1 – Эталонная объектная модель IoT [ISO/IEC 30141]

В целом платформу услуг IoT можно разделить на четыре части – систему управления устройствами, систему управления подключением, систему поддержки приложений и систему бизнес-анализа.

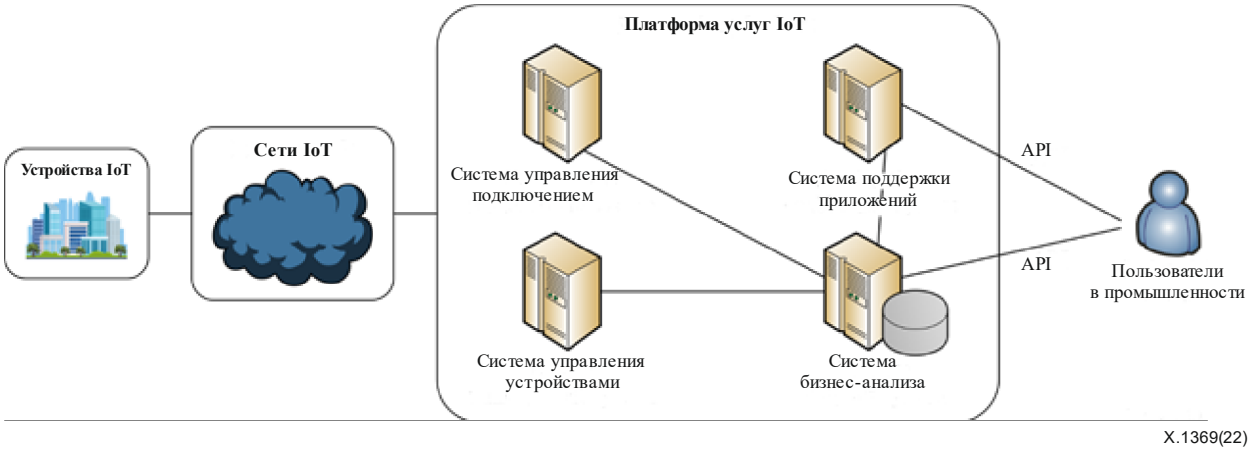

Рисунок 2 – Обзор платформы услуг IoT

- Система управления устройствами

Это система управления устройствами IoT. Она обеспечивает функции удаленного мониторинга, изменения конфигурации, обновления программного обеспечения, модернизации системы, устранения неполадок, управления жизненным циклом и др.

- Система управления подключением

Это централизованная система управления картой модуля идентификации абонента (SIM). Она ориентирована на приложения сотовой сети и обеспечивает функции самообслуживания пользователей, такие как запрос сведений о потреблении данных и состоянии соединения, пополнение счета SIM-карты и управление трафиком.

- Система поддержки приложений

Это платформа типа платформа как услуга, предоставляющая функциональные интерфейсы прикладного программирования (API) для поддержки различных систем обслуживания. С помощью этой системы операторы связи открывают доступ к своим основным услугам электросвязи (передача данных, SMS, телефония, аутентификация, биллинг и т. д.) для различных систем обслуживания, таких как интеллектуальный транспорт, умный город, умный дом и т. д.

- Система бизнес-анализа

Собирает различные данные из системы управления устройствами, системы управления подключением и системы поддержки приложений для анализа и визуального отображения результатов анализа для операторов и потребителей.

Безопасность платформы услуг IoT играет важную роль для всей среды IoT. Любая уязвимость этой платформы или атака на нее могут повлиять на безопасность подключенных устройств, сетей и данных. Платформа услуг IoT уязвима для угроз, включая отказ в обслуживании (DoS), повышение уровня привилегий, несанкционированный доступ, атаки методом перебора, выполнение произвольного кода и т. д., которые могут привести к злонамеренному вторжению, утечке конфиденциальной информации, злонамеренному управлению устройствами и другим серьезным последствиям.

В настоящей Рекомендации анализируются риски нарушения безопасности платформы услуг IoT. Предлагаются меры обеспечения безопасности и методика построения структуры безопасности.

К безопасности платформы услуг IoT относятся безопасность инфраструктуры, безопасность системы, безопасность данных и безопасность приложений от нижнего до верхнего уровня. Имеются четыре уровня безопасности API и эксплуатационной безопасности. В разделах 7–9 подробно описаны риски нарушения безопасности, структура безопасности и требования безопасности с учетом этих шести аспектов.

7 Угрозы безопасности платформы услуг IoT

7.1 Угрозы безопасности приложений

К угрозам безопасности приложений относятся веб-атаки, попытки несанкционированного доступа, повышение уровня привилегий, а также уязвимости услуг.

7.1.1 Веб-атаки

На платформе услуг IoT используются как традиционные веб-технологии, так и технологии связи, большие данные, облачные вычисления и т. п. В результате она наследует основные риски нарушения безопасности всех этих технологий, такие как распределенные атаки типа отказ в обслуживании (DDoS), атаки методом перебора, внедрение кода на языке структурированных запросов (SQL), уязвимости межсайтовых сценариев (XSS), подделка межсайтовых запросов (CSRF), подделка запросов на стороне сервера (SSRF) и т. д.

7.1.2 Несанкционированный доступ и повышение уровня привилегий

Большое количество приложений IoT может быть развернуто на одной централизованной платформе. Это затрудняет эффективную изоляцию разных приложений в целях безопасности и управления доступом, что может привести к несанкционированному доступу, несанкционированной эксплуатации и повышению уровня привилегий. Кроме того, такая платформа подвержена угрозам несанкционированного доступа и повышения уровня привилегий между разными пользователями и устройствами.

7.1.3 Уязвимость услуг

Приложения IoT отличаются сложной логикой обслуживания и большим количеством протоколов приложений, что может привнести ошибки в процессы проектирования и реализации и привести к уязвимостям услуг и нарушению безопасности. В некоторых сценариях приложений IoT через платформу можно управлять терминалами. Взлом платформы приведет к взлому большого количества терминалов и повлияет на промышленное производство и общественную жизнь пользователей.

7.1.4 Предоставление функциональных возможностей

В качестве платформы поддержки приложений платформа IoT предоставляет различные функциональные API для поддержки реализации различных систем обслуживания. Это обеспечивает удобство для различных услуг, однако предоставление функциональных возможностей также может привести к рискам нарушения безопасности платформы. Эти возможности могут оказаться доступными для неавторизованных разработчиков или неправомерно использоваться различными услугами. Более того, предоставление основных возможностей электросвязи (передача данных, SMS, телефония, аутентификация, биллинг и т. д.) может привести к атакам на базовую сеть электросвязи, если она не защищена должным образом.

7.2 Риски нарушения безопасности данных

Конфиденциальность, целостность и доступность данных составляют основу безопасности данных. Однако процесс сбора, передачи, переноса, хранения, обработки и уничтожения данных подвержен множеству рисков.

7.2.1 Утечка данных

Данные приложений IoT обычно собираются терминалами IoT и передаются на платформу, на которой обычно хранятся. Следовательно, если эти данные не защищены должным образом, злоумышленник может получить их с помощью атак, направленных на внедрение SQL, атак по переполнению буфера, повышения уровня привилегий и т. д.

7.2.2 Фальсификация данных

Во время передачи данные могут фальсифицироваться, копироваться или изменяться. Если данные приложений не защищены должным образом, то злоумышленник может подделать их в процессе передачи или хранения. Например, если во время передачи не обеспечивается целостность данных, злоумышленник может скопировать использованную информацию или подделать ее и отправить на платформу IoT.

7.3 Риски нарушения безопасности системы

7.3.1 Взлом учетной записи

Если учетные записи администраторов операционной системы платформы услуг IoT недостаточно защищены или открыт лишний порт системы, то эти учетные записи могут быть взломаны методом перебора, мониторинга и т. п. Безопасности системы также угрожает ненадлежащий контроль доступа.

7.3.2 Злоупотребление привилегиями

Услуги IoT, предоставляемые платформой, работают в среде операционной системы и промежуточного программного обеспечения. Если операционная система или промежуточное ПО вовремя не обновляются, существует риск того, что в устаревшей версии операционной системы или промежуточного ПО имеются уязвимости, которые могут быть использованы хакерами, что приведет к несанкционированному повышению уровня привилегий.

7.4 Риски нарушения безопасности инфраструктуры

Инфраструктура уязвима для угроз нарушения физической безопасности, безопасности сети, безопасности виртуальных машин и безопасности оборудования.

7.4.1 Физические угрозы

На безопасность также влияет физическая среда платформы IoT. Например, она уязвима для природных катастроф, таких как землетрясения, наводнения, штормы и торнадо. Кроме того, угрозу для платформы IoT могут представлять такие объекты, как системы электропитания и охлаждения и даже сами системы безопасности. Более того, следует учитывать человеческий фактор, который может включать умышленное разрушение, кражи и взрывы.

7.4.2 Угрозы для сети

Злоумышленники могут сканировать интернет в поисках точки доступа к платформам IoT. Отсутствие изоляции платформ услуг в сети может привести к появлению возможности доступа к данным разных услуг.

7.4.3 Риски виртуализации

Технология виртуализации серверов значительно упростила построение и повысила операционную гибкость и экономическую эффективность платформы IoT, но она также связана с новыми рисками. Например, ошибки, допущенные при разработке монитора виртуальных машин (VMM), позволяют злоумышленникам вторгаться в виртуальные хосты omtp, а совместное использование сетевой карты с виртуальной машиной того же хоста упрощает распространение проблем безопасности. Существуют и другие риски, такие как скачкообразное переключение виртуальных машин (BM), DoS-атаки и уязвимости платформы дистанционного управления.

7.5 Риски нарушения безопасности интерфейсов

К интерфейсам платформы услуг IoT относятся веб-интерфейс, внешний API и API поставщика, которые подвержены рискам утечки информации, межсайтового скриптинга, слабой аутентификации и слабого контроля доступа.

7.6 Эксплуатационные риски нарушения безопасности

В процессе эксплуатации и технического обслуживания предоставление услуги может быть прервано из-за неправильных эксплуатационных действий технического персонала. Например, сотрудники могут использовать USB-накопитель, зараженный вредоносным ПО, или случайно удалить данные. Также следует учитывать возможность неправильного соединения, использования паролей по умолчанию, злонамеренные атаки и механизм аудита.

8 Архитектура безопасности платформы услуг IoT

Архитектура безопасности платформы услуг IoT предусматривает шесть аспектов требований к защите: безопасность приложений, безопасность интерфейсов, безопасность данных, безопасность системы, безопасность инфраструктуры и безопасность эксплуатации.

Общая архитектура безопасности показана на рисунке 3.

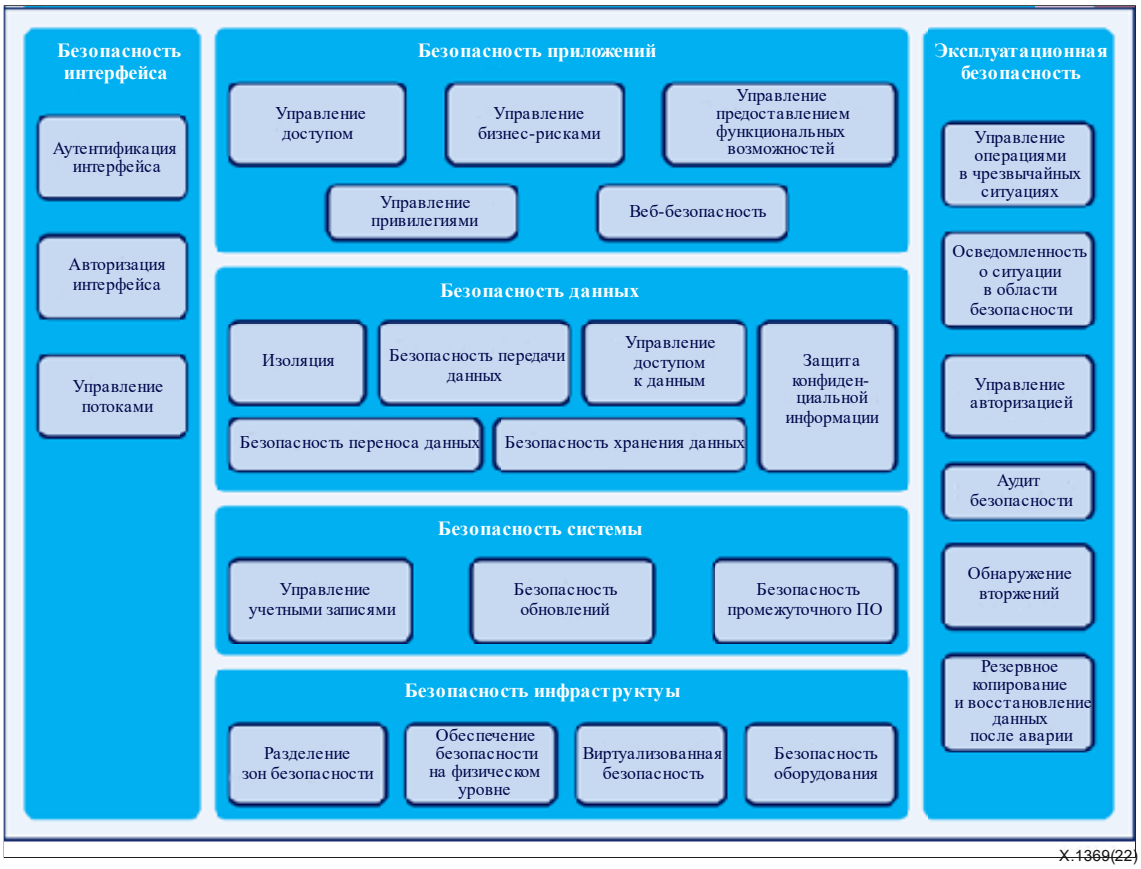

Рисунок 3 – Архитектура безопасности платформы услуг IoT

8.1 Безопасность приложений

К безопасности приложений относятся управление доступом, управление привилегиями, управление бизнес-рисками, веб-безопасность и управление предоставлением функциональных возможностей. Обеспечение этих функций будет способствовать предотвращению угроз повышения уровня привилегий, несанкционированного доступа и т. д.

8.2 Безопасность данных

К безопасности данных относятся изоляция, безопасность передачи данных, управление доступом и безопасность хранения данных. Обеспечение этих функций будет способствовать предотвращению утечки конфиденциальных данных и возникновения других проблем безопасности данных.

8.3 Безопасность системы

К безопасности системы относятся управление учетными записями, безопасность обновлений программного обеспечения и безопасность промежуточного ПО. Обеспечение этих функций будет способствовать предотвращению злонамеренного использования известных уязвимостей.

8.4 Безопасность инфраструктуры

К безопасности инфраструктуры относятся разделение зон безопасности, обеспечение безопасности на физическом уровне, видеонаблюдение и безопасность оборудования. Обеспечение этих функций будет способствовать предотвращению злонамеренного использования известных уязвимостей.

8.5 Безопасность интерфейсов

К безопасности интерфейсов относятся аутентификация интерфейса, авторизация интерфейса и управление потоками. Обеспечение этих функций будет способствовать предотвращению утечки информации, позволяющей установить личность, внедрения SQL и т. д.

8.6 Эксплуатационная безопасность

К эксплуатационной безопасности относятся управление операциями в чрезвычайных ситуациях, осведомленность о ситуации в области безопасности, управление авторизацией, аудит безопасности, обнаружение вторжений, резервное копирование и восстановление данных после аварии. Обеспечение этих функций будет способствовать решению проблем, связанных с эксплуатационной безопасностью.

9 Требования безопасности для платформы услуг IoT

9.1 Безопасность приложений

Платформа услуг должна быть способна предотвращать атаки из интернета на своей границе, в особенности атаки, нацеленные на большие данные, облачные вычисления, веб-приложения и другие технологии. Чтобы гарантировать безопасную и стабильную работу платформы услуг, должна быть обеспечена возможность предотвращения DDoS-атак, взлома, вторжений и вирусов.

9.1.1 Управление доступом

9.1.1.1 Управление доступом пользователей

1. Система идентификации пользователей должна быть построена так, чтобы каждому пользователю присваивалась уникальная идентификационная метка, которая должна оставаться неизменной даже в случае изменения пользователем номера мобильного телефона, адреса электронной почты или другой информации.
2. Следует обеспечить периодическое обнаружение слабых паролей. Кроме того, в процессе передачи пароль должен быть зашифрован. Для услуг с высокими требованиями к уровню безопасности следует рассмотреть возможность использования механизма обязательной периодической замены пароля.
3. Следует строго контролировать использование динамических коротких сообщений. Следует принимать такие меры безопасности, как проверка общей информации, немедленное аннулирование после использования, ограничение количества ошибок при входе в систему, недопущение локальной аутентификации и т. д.
4. В сценарии входа в систему следует использовать механизм графического кода аутентификации. Для предотвращения быстрого машинного распознавания следует рассмотреть возможность использования таких мер по фоновому скремблированию, как добавление фонового шума, небинаризованное изображение, десегментация, зачеркивание, искажение с поворотом шрифта и т. д.
5. Платформа должна иметь возможности для управления рисками и предотвращения конфликтов. Она также должна иметь возможность идентификации санкционированного доступа. Например, возможность взлома должна предотвращаться посредством ограничения количества неудачных попыток входа в систему, IP-адресов, идентификаторов устройства, времени блокировки, режима разблокировки и одновременного доступа.
6. В процессе сброса и восстановления пароля необходимо тщательно проверять личность пользователя, чтобы предотвратить обход аутентификации и подлог идентичности.

9.1.1.2 Управление доступом к приложениям

1. Создайте систему идентификации приложений и присвойте каждому приложению уникальный идентификатор.
2. Должна быть подтверждена действительность приложения, обращающегося к платформе. Доступ к платформе для выполнения последующих обращений к услугам должен быть разрешен только аутентифицированным приложениям.
3. В процессе аутентификации приложения запрещается передавать ключи в виде открытого текста или применять слабый алгоритм преобразования (например, MD5) для ключей.

4. Разным приложениям должны назначаться разные ключи, и должны поддерживаться функции управления ключами для их генерации, распространения, хранения и обновления.

5. Вызов интерфейсов должен быть аутентифицирован, чтобы ограничить объем ресурсов и прав доступа к операциям, которыми можно управлять.

9.1.1.3 Управление доступом к устройствам

1. Должна быть построена система идентификации устройств. Каждому устройству IoT назначается уникальный идентификатор, привязанный к соответствующей информации об оборудовании, такой как название производителя устройства, тип устройства, модель и т. д.

2. Каждому устройству назначается уникальный ключ устройства с помощью схемы предварительного распределения ключей или схемы обмена ключами и т. п. Ключ устройства и идентификатор устройства должны быть связаны между собой. Также должны поддерживаться функции управления ключами для генерации, распространения, хранения и обновления ключей.

3. В момент обращения устройства к платформе производится аутентификация его идентичности. Доступ к сервисной платформе для последующих операций по обслуживанию должны получать только аутентифицированные устройства.

4. В процессе аутентификации приложения запрещается передавать ключи в виде открытого текста или применять слабый алгоритм преобразования (например, MD5) для ключей.

9.1.2 Управление привилегиями

1. Следует поддерживать классификацию пользователей и управление группами. Разным классам и группам пользователей должны предоставляться разные привилегии. Доступ к запрашиваемым данным и возможность выполнять соответствующие операции должны получать только авторизованные пользователи.

2. Приложениям разного класса назначаются разные привилегии. Вызов запрашиваемых возможностей по обслуживанию и выполнение соответствующих операций должны быть разрешены только авторизованным приложениям.

3. Устройствам разного типа или класса назначаются разные привилегии. Доступ к запрашиваемым данным и выполнение соответствующих операций должны быть разрешены только авторизованным устройствам.

9.1.3 Управление бизнес-рисками

9.1.3.1 Управление безопасностью и контроль карт IoT

Коммуникационные функции карт IoT должны быть строго ограничены для разных типов услуг по принципу "минимальность, необходимость и контролируемость". Например, в некоторых сценариях функция передачи голосовых и коротких сообщений должна быть однонаправленной, а при аномальном потоке данных функция передачи данных должна быть ограничена.

9.1.3.2 Управление и контроль безопасности услуг

Должна быть возможность ограничивать общий объем и частоту потока данных, коротких сообщений, голосовых сообщений и т. д., а также возможность отключать услугу, когда объем превышает пороговое значение.

9.1.3.3 Контроль поведения пользователей

Общий объем потока, частота и время сеансов доступа пользователей к платформе должны быть ограничены. Когда пользователи ведут себя аномально, доступ следует немедленно прекратить.

9.1.3.4 Мониторинг аномалий устройств

Следует контролировать поведение устройств. Должен быть предусмотрен механизм сигнализации и обработки событий при обнаружении аномального поведения устройства (например, необычного времени, необычных посещений, необычного местоположения).

9.1.3.5 Мониторинг рисков при обслуживании

Чтобы вовремя обнаруживать отклонения в функционировании услуги, следует анализировать данные терминалов IoT в многомерном формате, например по общему объему и пиковому потоку. Также следует отслеживать ненадлежащее использование услуги во время ее функционирования. Например, отслеживая международный идентификатор аппаратуры подвижной связи (IMEI) устройств, можно обнаружить разделение устройства и карты. В то же время используя большие данные, собранные в ходе эксплуатации терминалов, можно повысить общую способность системы обнаруживать, анализировать и устранять риски нарушения безопасности.

9.1.4 Веб-безопасность

1. Должна быть обеспечена надежная защита от DDoS-атак и должны быть настроены стратегии защиты от DDoS (например, растяжение трафика, очистка сетевого трафика и т. п.) для уровня приложений и сетевого уровня.
2. Платформа должна обеспечивать сканирование веб-уязвимостей, обнаруживая и предотвращая такие проблемы безопасности, как загрузка файлов в сеть, внедрение SQL, XSS-уязвимости, CSRF-уязвимости и SSRF-уязвимости.
3. Платформа должна обеспечивать сканирование уязвимостей хоста и находить уязвимости в информационной системе, включая уязвимости системы безопасности, проблемы настройки системы безопасности, уязвимости системы безопасности приложений и слабые пароли.
4. Платформа должна обладать возможностью ограничивать время подключения к базе данных и доступа к сети в веб-приложениях во избежание ненужного потребления ресурсов.
5. Платформа должна обеспечивать обнаружение вторжений, регистрацию IP-адреса источника, типа атаки, цели атаки и времени попытки вторжения, а также сигнализацию при серьезном вторжении.

9.1.5 Управление предоставлением возможностей

9.1.5.1 Аутентификация идентичности

Система обеспечения возможностей для приложений должна поддерживать аутентификацию идентичности. Когда разработчик запрашивает и применяет некоторые функции API, должна проверяться подлинность разработчика и приложений, и подделка идентичности разработчиков и приложений должна быть исключена.

9.1.5.2 Повышение надежности и защита приложений

Для предотвращения вмешательства и декомпиляции приложений система обеспечения возможностей для приложений должна иметь функцию поддержки повышения надежности и защиты приложений, которые вызывают функции API.

9.1.5.3 Защита безопасности данных

Для предотвращения возможности кражи или подделки информации во время ее хранения, передачи и использования система обеспечения возможностей для приложений должна гарантировать конфиденциальность и целостность секретной информации, связанной с учетными записями и учетными данными пользователей и приложений. Например, конфиденциальная информация, которой обмениваются приложение IoT и платформа, должна быть зашифрована, и следует предусмотреть защиту целостности, гарантирующую, что конфиденциальная информация будет недоступна неавторизованным объектам и процессам и не может быть изменена, повреждена, скопирована и т. д.

9.1.5.4 Аутентификация при активизации возможностей

Система обеспечения возможностей для приложений должна поддерживать аутентификацию и авторизацию при активизации возможностей. Когда приложение активизирует какую-либо возможность, должны быть аутентифицированы частота, общее количество активизаций и типы возможностей, которые могут быть активизированы разработчиком и приложением. Возможности должны активизироваться только после авторизации.

9.1.5.5 Мониторинг активизации возможностей

Система обеспечения возможностей для приложений должна поддерживать мониторинг частоты, времени и общего количества активизаций возможностей. При превышении предела или аномальном поведении выполнение функции должно немедленно прекращаться с одновременной подачей предупредительного сигнала.

9.2 Безопасность данных

Платформа должна защищать данные на протяжении всего их жизненного цикла, включая хранение, передачу, использование и т. д. Должно периодически осуществляться резервное копирование критически важных данных услуги, а также должен быть создан механизм восстановления для обеспечения конфиденциальности, целостности и доступности данных.

9.2.1 Изоляция данных

Различные данные должны обрабатываться и сохраняться в изолированной среде. Платформа должна иметь возможность логически изолировать конфиденциальную информацию и строго контролировать взаимодействие между разными полями.

9.2.2 Безопасность передачи данных

1. Конфиденциальная информация, передаваемая между платформой услуг и устройствами IoT или другими платформами услуг (включая пароль администратора, пароль для входа в операционную систему, пароль для входа в сетевое устройство, а также ответы на страховочные вопросы, связанные с этими паролями), должна быть надежно защищена.
2. Должна быть защищена целостность конфиденциальной информации, передаваемой между платформой услуг, устройствами IoT и другими платформами услуг.

9.2.3 Управление доступом

Платформа должна поддерживать функцию управления доступом, например должны быть установлены разные правила доступа к базам данных разных систем виртуализации, чтобы гарантировать, что пользователи могут работать только в рамках авторизации базы данных соответствующей системы услуг и не могут получить доступ к данным других неавторизованных систем услуг.

9.2.4 Безопасность хранения данных

1. Данные должны быть классифицированы по их значимости, и к ним следует применять разные механизмы в соответствии с уровнем классификации данных. Например, менее важные данные могут храниться в виде открытого текста, тогда как конфиденциальность важных данных должна быть гарантирована.
2. Платформа должна обеспечивать механизм безопасного хранения ключей. Например, чтобы гарантировать невозможность утечки ключей, их следует хранить в шифромашине или на специальном прокси-сервере.
3. Следует защищать целостность данных, а для данных высшей степени конфиденциальности должен быть предусмотрен механизм определения целостности, чтобы вовремя обнаруживать искажение и потерю этих данных. К данным высшей степени конфиденциальности относятся имя пользователя, номер банковского счета и т. д.
4. Платформа должна обеспечивать механизм полного резервного копирования и восстановления данных. В случае потери или уничтожения данных для их восстановления следует использовать механизм резервного копирования, гарантирующий, что при авариях данные не будут потеряны.
5. Платформа должна обеспечивать возможность архивирования всех видов данных и файлов, а также функцию автоматической и периодической очистки временных данных и файлов.
6. Пространство для хранения файлов, каталогов и баз данных в системе должно освобождаться или перераспределяться таким образом, чтобы обеспечить полную очистку и невозможность восстановления.

9.3 Безопасность системы

Система, используемая платформой, должна предусматривать управление учетными записями, безопасность обновлений программного обеспечения и безопасность промежуточного программного обеспечения, что будет способствовать решению проблем злонамеренного использования известных уязвимостей.

9.3.1 Управление учетными записями

1. Система платформы должна автоматически вести журналы системных событий, таких как информация о входах пользователей, эксплуатационная информация и т. д.
2. Система, которая обслуживается удаленно по протоколу HTTP, должна поддерживать протоколы с шифрованием, такие как HTTPS.
3. Для систем с текстовым интерфейсом должна поддерживаться возможность автоматического выхода из учетной записи по времени.
4. Система должна предусматривать возможность управления доступом к ресурсам хоста, например устанавливая ролевую модель надлежащей политики безопасности для управления доступом к ресурсам хоста пользователей разных ролей.

9.3.2 Безопасность обновлений программного обеспечения

1. Должны своевременно обновляться версии операционной системы/исправлений уязвимостей.
2. Должна быть разрешена установка только необходимых компонентов и приложений.
3. Система должна открывать только необходимые порты и закрывать ненужные.

9.3.3 Безопасность промежуточного ПО

1. Должны своевременно обновляться версии/исправления уязвимостей промежуточного программного обеспечения.
2. Во избежание утечки системной информации ненужные интерфейсы промежуточного программного обеспечения должны быть отключены.
3. Во избежание утечки системной информации должен быть защищен флаг промежуточного программного обеспечения (заголовок с названием программного обеспечения/номером версии).

9.4 Безопасность инфраструктуры

Для обеспечения безопасности инфраструктуры должны быть предусмотрены разделение зон безопасности, физическая защита, видеонаблюдение и защита оборудования, что будет способствовать решению проблем, вызванных злонамеренным использованием известных уязвимостей.

9.4.1 Разделение зон безопасности в сети

1. Зоны безопасности должны быть разделены между платформами услуг и интернетом, между платформами услуг и внутренними системами поддержки, а также между разными системами услуг, размещенными на платформе. Границы зон безопасности должны быть установлены между другими зонами и зоной доступа, между зоной доступа и зоной ядра, а также внутри зоны ядра.
2. Разные системы услуг на платформе услуг должны быть разделены на разные виртуальные локальные сети (VLAN), и в разных зонах безопасности должны использоваться разные сегменты VLAN. Для разных систем услуг в каждой зоне безопасности должны использоваться разные VLAN, и по умолчанию все VLAN должны быть изолированы. В рамках одной и той же VLAN должна поддерживаться изоляция ВМ на разных уровнях безопасности одной и той же системы услуг, например разделение суб-VLAN по технологии Private VLAN (PVLAN).
3. Должна быть установлена политика взаимного доступа. Например, следует осуществить стратегическую настройку взаимного доступа для разных зон безопасности в одной системе услуг и взаимного доступа между разными системами услуг.

4. Должна поддерживаться функция изоляции зон безопасности. Например, сеть платформы можно разделить на зону управления, зону услуг, зону интерфейса и т. д. Устройства с разными функциями должны быть распределены по разным зонам безопасности. На границах зон безопасности должны быть реализованы функции обнаружения вторжений и управления доступом.

9.4.2 Безопасность на физическом уровне

1. Физическая среда должна соответствовать требованиям безопасности, относящимся к расположению, источникам электроснабжения, пожарной безопасности, водонепроницаемости, антистатической поддержки, регулирования температуры и влажности.

9.4.3 Безопасность виртуальных объектов

1. Во избежание распространенных проблем безопасности при виртуализации платформа должна обеспечивать защиту гипервизора, изоляцию ВМ, повышение надежности облачной хост-системы, контроль безопасности ВМ, защиту от вредоносных программ, контроль приложений и другие функции.

9.4.4 Безопасность оборудования

1. Физические объекты должны соответствовать требованиям базовой конфигурации системы обеспечения безопасности и требованиям испытаний. Для повышения безопасности объектов следует внедрить доверенные вычисления.

9.5 Безопасность интерфейсов

К безопасности интерфейсов относятся аутентификация интерфейса, авторизация интерфейса и управление потоками. Обеспечение этих функций будет способствовать решению проблем утечки информации, позволяющей установить личность, внедрения SQL и т. д.

9.5.1 Аутентификация интерфейса

1. Для предотвращения несанкционированного использования и доступа платформа должна обеспечивать возможность проверки легитимности систем услуг.
2. Платформа услуг должна иметь функцию ведения полного журнала эксплуатации задействованных ресурсов.

9.5.2 Авторизация интерфейса

1. Платформа услуг должна обеспечивать функцию авторизации в соответствии с диапазоном IP-адресов источников. Помимо предъявления статического пароля вызываемая платформа услуг также должна авторизовать диапазон IP-адресов.
2. Для предотвращения доступа незаконных пользователей у интерфейсов, запрашивающих права доступа пользователя, должен быть механизм доступа на основе черного/белого списка.

9.5.3 Управление потоками

1. Платформа должна иметь возможность управлять скоростью потоков путем установления политики управления потоками, а значение конфигурации в этой политике должно изменяться в соответствии с настройкой рабочих характеристик сервера API. Когда количество одновременных запросов превышает установленный предел, запросы сверх этого предела отклоняются, и возвращается ответ с сообщением об ошибке.

9.6 Эксплуатационная безопасность

К эксплуатационной безопасности относятся управление операциями в чрезвычайных ситуациях, осведомленность о ситуации в области безопасности, управление авторизацией, аудит безопасности, обнаружение вторжений, резервное копирование и восстановление после аварии. Обеспечение этих функций будет способствовать решению проблем, связанных с эксплуатационной безопасностью.

9.6.1 Управление операциями в чрезвычайных ситуациях

1. Платформа должна иметь механизм реагирования на чрезвычайные ситуации, такие как инциденты кибербезопасности, инциденты безопасности на рабочем месте и т. д.
2. Следует проводить регулярные противоаварийные учения и создать систему регулярных учений по планам действий в чрезвычайных ситуациях.

9.6.2 Осведомленность о ситуации в области безопасности

1. Рекомендуется создать систему осведомленности о ситуации в области безопасности для реализации функций мониторинга, оценки, раннего предупреждения, визуализации и централизованного реагирования на ситуации в области безопасности платформы, с тем чтобы улучшить контроль угроз безопасности сети, повысить уровень осведомленности о ситуации, усовершенствовать реагирование на чрезвычайные ситуации, отслеживание и другие функции, а также повысить эксплуатационную безопасность и эффективность технического обслуживания.

9.6.3 Управление авторизацией

1. Платформа должна выполнять необходимую аутентификацию и авторизацию при различных операциях на платформе. Только доверенный системный персонал может выполнять операции, требующие высокоуровневых привилегий.
2. Платформа должна устанавливать ролевые модели и контролировать доступ пользователей к ресурсам хоста в соответствии с политикой безопасности.

9.6.4 Проверка безопасности

1. Все действия администраторов должны регистрироваться и оформляться в журнале.
2. Необходимо гарантировать, что при почти полном исчерпании пространства хранения данных журнал проверок не будет потерян.
3. Необходимо создавать резервные копии журналов проверок.
4. Журналы проверок должны быть защищены от несанкционированного доступа, изменения и уничтожения.
5. Журналы проверок следует экспортировать и удалять.
6. Доступ к журналам должен быть защищенным, чтобы гарантировать конфиденциальность и целостность процесса передачи.
7. Должны быть обеспечены функции мониторинга в режиме реального времени и периодического контроля аномального поведения платформы, такого как аномальное соединение, аномальный доступ и аномальное приложение, на основе анализа трафика, проверки журналов событий, песочницы и т. д. В случае обнаружения аномального поведения должны подаваться своевременные предупредительные сигналы и производиться разъединение.

9.6.5 Обнаружение вторжения

1. Чтобы своевременно обнаруживать вторжение, платформа должна использовать оборудование для обнаружения вторжения.

9.6.6 Резервное копирование и восстановление после аварии

1. В случае пожара, землетрясения и других бедствий платформа должна быть способна своевременно переключиться на удаленную резервную систему резервного копирования, чтобы продолжать работу.
2. Платформа должна поддерживать аварийное восстановление конфиденциальных данных (таких как данные услуг, данные денежных расчетов, данные конфигурации системы, записи об операциях администратора и техобслуживании, сведения о пользователях и т. д.), чтобы гарантировать, что в случае злонамеренного уничтожения критически важных данных система сможет вовремя восстановиться.

Библиография

[b-ITU-T X.1361] Рекомендация МСЭ-Т X.1361 (2018 г.), *Структура безопасности интернета вещей на основе модели с использованием шлюза.*

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

[b-ITU-T X.1601] Рекомендация МСЭ-Т X.1601 (2015 г.), *Основы безопасности облачных вычислений.*

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

[b-ITU-T Y.4100] Рекомендация МСЭ-Т Y.4100/Y.2066 (2014 г.), *Общие требования к интернету вещей.*

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, 2022 г.