Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1367

(09/2020)

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

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

Стандартный формат журналов регистрации ошибок в интернете вещей (IoT) для операций, связанных с инцидентами безопасности

Рекомендация МСЭ-Т X.1367

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

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

Рекомендация МСЭ-Т X.1367

Стандартный формат журналов регистрации ошибок в интернете вещей (IoT) для операций, связанных с инцидентами безопасности

Резюме

Существуют две проблемы, связанные с обработкой инцидентов безопасности, которые обусловлены экосистемой интернета вещей (IoT). Первая заключается в несовместимости протоколов между компьютерными сетями, в которых используется протокол управления передачей/протокол Интернет (TCP/IP), и граничными устройствами IoT. Вторая проблема заключается в несовместимости кодов ошибок производителей граничных устройств.

В Рекомендации МСЭ-Т X.1367 определен стандартизованный формат журнала регистрации ошибок, который может быть помещен в полезную нагрузку протокола, например как системный журнал регистрации [b-IETF RFC 5424], для использования в целях преобразования информации журнала регистрации ошибок, выданной граничным устройством, в стандартный формат журнала регистрации ошибок.

В настоящей Рекомендации определена также таблица стандартизованных кодов ошибок для разрешения второй проблемы. В результате возможно комплексное управление инцидентами безопасности в компьютерных сетях и сетях граничных устройств IoT.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1367	03.09.2020 г.	17-я	11.1002/1000/14263

Ключевые слова

Граничное устройство, код ошибки, формат журнала регистрации ошибок, реагирование на инциденты, Интернет вещей (IoT), операция, связанная с безопасностью.

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

ПРЕДИСЛОВИЕ

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

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

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

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

ПРИМЕЧАНИЕ

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

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

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

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

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

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1367

Стандартный формат журналов регистрации ошибок в интернете вещей (IoT) для операций, связанных с инцидентами безопасности

1 Сфера применения

В настоящей Рекомендации определен стандартизованный формат журнала регистрации ошибок в интернете вещей (IoT), который может быть помещен в полезную нагрузку протокола, такого как системный журнал регистрации [b-IETF RFC 5424], для использования в целях преобразования информации журнала регистрации ошибок, выданной граничным устройством, в стандартизованный формат журнала регистрации ошибок.

В настоящей Рекомендации также приведена таблица стандартизованных кодов ошибок для решения проблемы несовместимости кодов ошибок между разными производителями граничных устройств. В результате становится возможным комплексное управление инцидентами безопасности в компьютерных сетях и сетях граничных устройств IoT.

2 Справочные документы

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 исполнительный механизм (actuator) [b-ITU-T Y.4109]: Устройство, которое инициирует физическое действие после возбуждения входным сигналом.

3.1.2 атака (attack) [b-ISO 13491-1]: Попытка злоумышленника получить или изменить на устройстве конфиденциальную информацию или услугу, которую ему не разрешено получать или изменять.

3.1.3 аутентификация (authentication) [b-ITU-T X.1277]: Аутентификация – это процесс применения пользователем своего аутентификатора FIDO для доказательства полагающейся стороне наличия у него зарегистрированного ключа.

3.1.4 авторизация (authorization) [b-ITU-T X.800]: Предоставление прав, которое включает предоставление доступа на основании прав доступа.

3.1.5 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.

3.1.6 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.

3.1.7 интерфейс человек-машина (human-machine interface (HMI)) [b-ITU-T H.320]: Интерфейс человек-машина между пользователем и терминалом/системой, состоящий из физической части (электроакустический и электрооптический преобразователь, клавиши и т. п.) и логической части, которая имеет дело с функциональными рабочими состояниями.

3.1.8 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.

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

3.1.10 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.

3.1.11 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 сертификация (certification): Независимая аттестация продукции, процессов, систем или физических лиц.

ПРИМЕЧАНИЕ. – На основе определения, данного в [b-ISO/IEC 17000].

3.2.2 командный сервер (command and control (C&C) server): Сервер, который отправляет команды компьютерам (бот-сетям), ставшим ботами в результате заражения вредоносным программным обеспечением, и управляет такими компьютерами.

3.2.3 шифрование (encryption): Криптографическое преобразование данных для получения зашифрованного текста.

ПРИМЕЧАНИЕ. – На основе определения термина "шифрование", данного в [b-ITU-T X.800], где английские термины encipherment и encryption считаются синонимами.

3.2.4 граничное устройство интернета вещей (Internet of things edge device): Оконечное устройство экосистемы IoT, которое осуществляет сбор данных о реальной обстановке с помощью датчиков или оказывает воздействие на реальную обстановку с помощью исполнительных механизмов.

3.2.5 шлюз интернета вещей (Internet of things gateway (IoTGW)): Устройство, которое соединяет сеть граничных устройств IoT с широкодоступными компьютерными сетями, такими как интернет.

3.2.6 микроконтроллер (microcontroller unit (MCU)): Встроенный микропроцессор, содержащий арифметические блоки, блоки памяти и порты ввода/вывода в одной интегральной схеме.

3.2.7 группа реагирования на инциденты безопасности (security incident response team (SIRT)): Команда, которая получает сообщения об инцидентах безопасности, проводит расследование и принимает меры.

3.2.8 центр обеспечения безопасности (security operations centre (SOC)): Подразделение, которое следит за состоянием компьютеров и сетей в организации и реагирует при наличии признаков злонамеренных действий.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

C&C	Command and Control		Командный (сервер)
FW	Firewall		Брандмауэр
HMI	Human/Machine Interface		Интерфейс человек-машина
ID	Identifier		Идентификатор
IDS	Intrusion Detection System		Система обнаружения вторжений
IoT	Internet of Things		Интернет вещей
IoTGW	Internet of Things Gateway		Шлюз интернета вещей
IP	Internet Protocol		Протокол Интернет
JSON	JavaScript Object Notation		Нотация объектов JavaScript
LAN	Local Area Network	ЛС	Локальная сеть

MCU	Microcontroller Unit		Микроконтроллер
PC	Personal Computer	ПК	Персональный компьютер
SIRT	Security Incident Response Team		Группа реагирования на инциденты безопасности
SOC	Security Operation Centre		Центр обеспечения безопасности
TCP	Transmission Control Protocol		Протокол управления передачей

5 Соглашения

Отсутствуют.

6 Общие положения

6.1 Современная обработка ошибок в экосистеме IoT

В контексте обработки ошибок в IoT, если один из компонентов системы IoT, такой как датчик или исполнительный механизм, выходит из строя, выдается код ошибки, который заносится в журнал регистрации ошибок. Если ошибки случаются редко, меры по их исправлению не требуются. Если же ошибка продолжает возникать снова и снова, компонент следует заменить, чтобы решить проблему.

На рисунке 1 показана типичная экосистема IoT, состоящая из таких компонентов IoT, как микроконтроллеры (MCU), связанные с датчиками и исполнительными механизмами, шлюз интернета вещей (IoTGW) и облако.

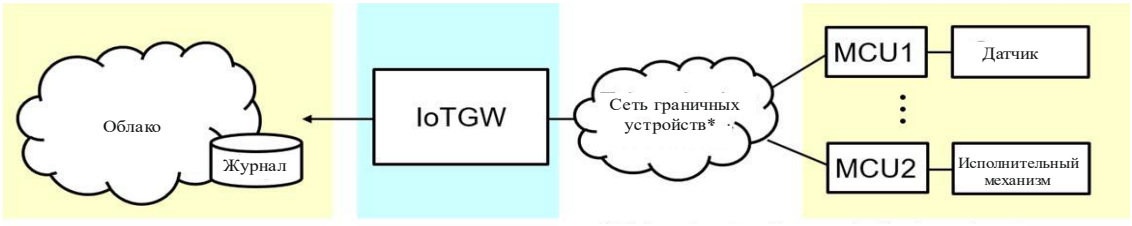


Рисунок 1 − Типичная экосистема IoT

На рисунке 1 связь между IoTGW, MCU1 и MCU2 основана на особом протоколе для этой системы (см. Примечание). MCU1 – датчик и MCU2 – исполнительный механизм являются примерами граничных устройств IoT. В данном случае IoTGW передает запросы MCU, и MCU присылают в ответ информацию из журнала. IoTGW также поддерживает связь с облаком (центральной системой).

ПРИМЕЧАНИЕ. – В качестве особого протокола может выступать протокол больших сетей, такой как oneM2M [b-oneM2M] или ECHONET Lite [b-ISO/IEC 14543-4-3], протокол малых сетей, такой как SPI [b-SPI], I^2C [b-UM10204], Bluetooth [b-IEEE 802.15.1] или ZigBee [b-IEEE 802.15.4], а также специальный протокол, предназначенный только для данной системы IoT.

Поскольку граничные устройства IoT иногда выходят из строя, для надлежащего управления экосистемой IoT в ней необходимо обрабатывать ошибки. Такие системы ведут журналы регистрации ошибок, в которых регистрируются коды ошибок, и инициируют их исправление. Некоторые системы анализируют журналы регистрации ошибок, в которых хранятся коды ошибок, в целях сбора статистической информации для своего совершенствования и даже для обработки инцидентов безопасности. Однако журналы регистрации ошибок разных экосистем IoT трудно унифицировать между собой и с системным журналом [b-IETF RFC 5424].

6.2 Обзор

Для эффективного реагирования на инциденты важно предоставить надлежащие возможности для сбора и анализа информации журналов регистрации ошибок отдельных компонентов экосистемы IoT. Однако в случае экосистемы IoT признаны следующие проблемы.

1) Для сбора информации журналов сетевых устройств существует стандартизированная процедура, включающая процесс обработки инцидентов с использованием системного журнала [b-IETF RFC 5424]. Однако для экосистемы IoT такой процедуры не существует.

2) Информация журналов регистрации ошибок IoT не может храниться в одном компоненте экосистемы IoT, то есть такая информация должна собираться центральной системой (например, облаком) или граничной системой IoT (например, IoTGW) в зависимости от конфигурации экосистемы IoT.

3) Корреляционный анализ информации журналов регистрации ошибок различных компонентов IoT затруднен из-за отсутствия стандартизированного формата журнала регистрации ошибок.

4) Без метода обработки информации журналов регистрации ошибок экосистема IoT не в состоянии эффективно поддерживать свою службу IoT.

В настоящей Рекомендации описана базовая архитектура системы IoT для сбора журналов регистрации ошибок IoT, которые используются в операциях по обработке инцидентов. В ней определяются стандартизированные коды ошибок и формат журнала регистрации ошибок. Преобразовав коды ошибок, принятые у каждого производителя экосистемы IoT, в стандартизированные коды ошибок, можно эффективнее отслеживать состояние разных экосистем IoT. Кроме того, в процессе преобразования кодов ошибок в стандартизированные коды в соответствующих журналах регистрации ошибок также делается запись о ситуации, в которой произошла ошибка. В результате можно обрабатывать инциденты безопасности в нескольких экосистемах IoT (см. пример с несколькими экосистемами IoT в пункте I.4 в Дополнении I).

7 Стандартный формат журнала регистрации ошибок для среды IoT

Из-за ограниченных вычислительных ресурсов граничных устройств IoT реализация ими новых функций обработки журналов регистрации ошибок IoT может оказаться затруднительной. Однако у IoTGW обычно имеется больше вычислительных ресурсов для этого. IoTGW часто обменивается запросами и ответами с облачными системами, и в такие сообщения входит информация журналов регистрации ошибок IoT. Поэтому в настоящей Рекомендации требуется, чтобы IoTGW генерировал стандартизированную информацию журнала регистрации ошибок и передавал ее в облачные системы.

7.1 Базовая структура формата журнала регистрации ошибок

В формате журнала регистрации ошибок IoT, описанном на рисунке 2, используется нотация объектов JavaScript (JSON) с регулярным выражением. Этот формат можно преобразовать для использования в системном журнале или XML (см. Примечание). Описание примеров этого формата приведено в Дополнении I.

ПРИМЕЧАНИЕ. – Длина значения каждого атрибута в настоящей Рекомендации не определена. Отправитель и получатель журнала регистрации ошибок должны заранее согласовать длину значения каждого атрибута.

```
{
    "Timestamp":
        "^([0-9]{4})-(1[0-2]|0[1-9])-(3[01]|0[1-9]|[12][0-9])T
          (2[0-3]|[01][0-9]):([0-5][0-9]):([0-5][0-9])(\.[0-9]{+})Z$",
    "Reporter": {},
    "Protocol": String,
    "Requester": {},
    "Responder": {},
    "Error Code": "/^[0-9A-F]^{+}$/",
    "Error Message": String,
    "Description": String | {},
}
```

Рисунок 2 – Элементы записи об ошибке

В большинстве случаев этот журнал регистрации ошибок ведет IoTGW. Атрибуты, используемые в данном формате, определены в пункте 7.2.

7.2 Базовые атрибуты

Информационными элементами журнала регистрации ошибок служат следующие атрибуты.

a) Timestamp (отметка времени): отметка времени (см. Примечание) требуется для выпуска журнала регистрации ошибок. Например, отметка времени для 13 часов 25 минут и 51 секунды 20 сентября 2018 года должна выглядеть так: "2018-09-20T13:25:51.0Z". [b-ISO 8601-1].

ПРИМЕЧАНИЕ. – Отметка времени является обязательной, даже если в протоколе передачи, содержащем журнал регистрации ошибок, описанный в настоящей Рекомендации, также имеется поле отметки времени, поскольку с момента возникновения проблемы до момента передачи отметка времени, как правило, изменяется.

b) Reporter (отправитель): компонент IoT, который преобразует код ошибки устройства в стандартный код ошибки и передает его в облако. Подробное описание приведено на рисунке 3.

```
"Reporter":{
    "IP Address":
        "(^(?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}
              (?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)$)
         |(^(?:[A-F0-9]{1,4}:){7}[A-F0-9]{1,4}$)"
}
```

Рисунок 3 − Информационные элементы отправителя

1) IP Address（адрес протокола Интернет): уникальный идентификатор (ID) отправителя в сети Ethernet.

c) Protocol （протокол): имя протокола, используемого в IoTGW и граничных устройствах IoT.

d) Requester (запрашивающее устройство) или Responder (отвечающее устройство): компонент IoT, направивший запрос граничному устройству IoT, или компонент IoT, ответивший на запрос. Подробное описание приведено на рисунке 4.

```
"Requester(or Responder)": {
    "Unique ID": string,
    "Transmitted Code": "( [0-9A-F])^{+}}
```

Рисунок 4 − Информационные элементы источника запроса и ответчика

1) Unique ID (уникальный идентификатор) (необязательно): уникальный номер или код каждого устройства, определяемый протоколом сети граничных устройств IoT.

2) Transmitted code (передаваемый код) (необязательно): содержание передаваемых данных. Выражается в шестнадцатеричном формате.

3) Когда происходит ошибка при отсутствии запрашивающего или отвечающего устройства, например когда измерительное устройство периодически передает данные без запросов, содержание принимает вид, как показано на рисунке 5.

```
"Requester(or Responder)": {}
```

Рисунок 5 − Случай отсутствия запрашивающего или отвечающего устройства

e) Error code, error message (код ошибки, сообщение об ошибке) – коды ошибок и сообщения об ошибках приведены в Приложении A.

f) Description (описание) (необязательно) – может выражаться любыми предложениями, фразами и элементами JSON, когда требуется уведомление о состоянии граничных устройств или сетей IoT.

При узкой полосе пропускания канала связи или ограниченном размере постоянной памяти сообщение об ошибке может отсутствовать. Если не нужно записывать никакой дополнительный текст, описание может отсутствовать.

Приложение A

Коды ошибок и сообщения об ошибках

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

Коды ошибок и сообщения об ошибках приведены в таблице A.1.

Таблица A.1 − Коды ошибок и сообщения об ошибках

Код	Сообщение	Описание
	Ошибок нет (0x00-0x0F)	
0x00	Ошибок нет	Ошибок не произошло
	Связь (0x10-0x1F)	
0x10	Отсутствует ответ	Ответ отсутствует, даже если запрос требует какого-то ответа
0x11	Нарушение связи	Некоторые проблемы нарушения связи
0x12	Линия прервана	Линия сетевого интерфейса не работает
0x1E	Расширенные причины	Код префикса для расширенных причин
0x1F	Другие причины, относящиеся к связи	Другие причины, относящиеся к связи
	Безопасность (0x20-0x2F)	
0x20	Ошибка аутентификации	Некоторые проблемы аутентификации
0x21	Ошибка сертификации	Некоторые проблемы сертификации
0x22	Ошибка шифрования	Некоторые проблемы шифрования
0x23	Ошибка авторизации	Некоторые проблемы авторизации
0x2E	Расширенные причины	Код префикса для расширенных причин
0x2F	Другие причины, относящиеся к обеспечению безопасности	Другие причины, связанные с аутентификацией, сертификацией, шифрованием или авторизацией
	Команда (0x30-0x3F)	
0x30	Недопустимая команда	Команда не определена или недействительна
0x31	Недопустимый аргумент	Аргумент вне диапазона или недействителен
0x3E	Расширенные причины	Код префикса для расширенных причин
0x3F	Другие причины, связанные с командами	Другие причины, связанные с командами
	Устройство (0x40-0x4F)	
0x40	Устройство неисправно	Часть устройства полностью вышла из строя
0x41	Отказ устройства	Часть устройства вышла из строя, но ее можно восстановить
0x42	Недостаточно ресурсов	Недостаточно оперативной памяти, постоянной памяти и любых вычислительных ресурсов
0x4E	Расширенные причины	Код префикса для расширенных причин
0x4F	Другие причины, относящиеся к устройству	Другие причины, связанные с устройством
	Зарезервировано для будущего расширения (0x50-0xDF)	
	Зарезервировано для частных применений (0xE0-0xEF)	
	Другие (0xF0-0xFF)	
0xFF	Другие причины	Другие причины, кроме указанных выше

Дополнение I

Примеры использования журналов регистрации ошибок для операций, связанных с инцидентами

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

I.1 Злоумышленник посылает произвольную строку двоичных данных на граничное устройство через шлюз IoTGW

На рисунке I.1 показаны злоумышленник, пославший в MCU1 произвольную строку двоичных данных, и реакция устройства. Заголовок произвольной строки двоичных данных "01000001" указывает на устройство № 0001 и функцию № 0100. Другими словами, злоумышленник пытается взломать функцию № 0100 устройства № 0001. MCU1 не понимает код "3A459187F43CDDE5", поэтому передает на устройство № 0000 (IoTGW) ответ "000003FF" (неизвестная команда).

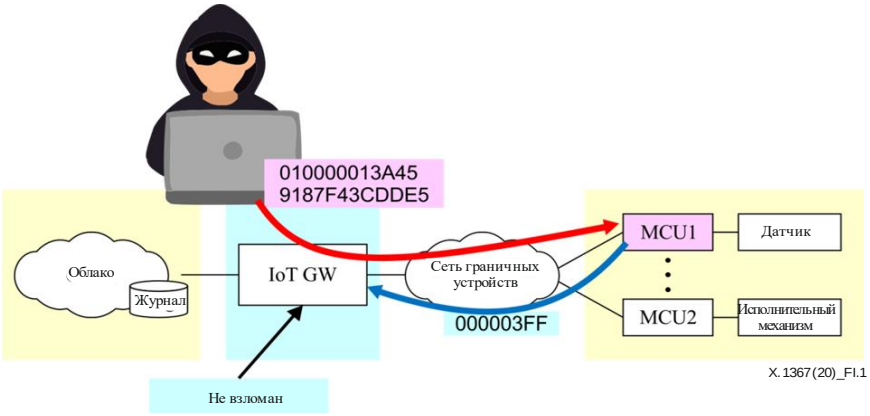


Рисунок I.1 – Злоумышленник посылает в MCU1 произвольную строку двоичных данных

Получив от MCU1 код "000003FF", шлюз IoTGW создает следующий журнал и передает его на сервер журналов в облаке. См. рисунок I.2.

```
{
    "Timestamp":"2018-08-28T09:34:55.0Z",
    "Reporter": { "IP Address": "192.168.2.11"},
    "Protocol": "ABC company protocol",
    "Requester": {
        "Unique ID": "0000",
        "Transmitted Code": "010000013A459187F43CdDE5"
    },
    "Responder": {
        "Unique ID": "0001",
        "Transmitted Code": "000003FF"
    },
    "Error Code": "30",
    "Error Message": "Invalid Command",
}
```

Рисунок I.2 – Журнал регистрации ошибок IoT при неправильном запросе (пример)

I.2 Злоумышленник посылает неверный сертификат на граничное устройство через взломанный шлюз IoTGW

На рисунке I.3 показаны злоумышленник, пославший неверный сертификат в MCU2 через взломанный шлюз IoTGW, и реакция устройства. MCU2 определяет, что сертификат недействителен, поэтому отвечает кодом "00000010000c" (ошибка проверки сертификата) на устройство № 0000 (IoTGW). Однако шлюз IoTGW взломан. Он не передает журнал регистрации ошибок на сервер журналов в облаке. Вместо шлюза IoTGW журнал регистрации ошибок IoT передает система обнаружения вторжений (IDS).

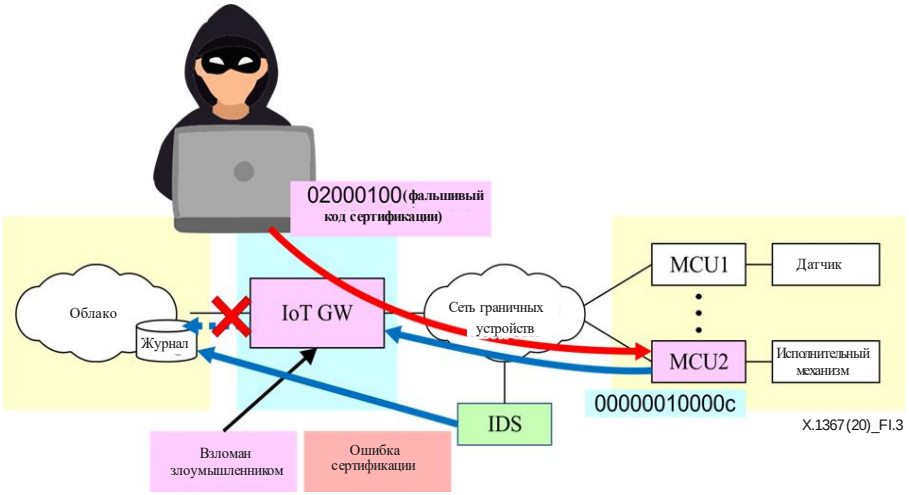


Рисунок I.3 – Злоумышленник посылает фальшивый код сертификации

Злоумышленник посылает в MCU2 фальшивый код сертификации, но MCU2 не может его распознать. Поэтому MCU2 передает сообщение "00000010000c" (ошибка проверки сертификата). Шлюз IoTGW игнорирует ответное сообщение от MCU2, поскольку злоумышленник ранее взломал его. Однако если в системе имеется IDS, она создает журнал регистрации ошибок IoT, показанный на рисунке I.4, вместо шлюза IoTGW. В этом случае отправителем становится IDS.

```
{
    "Timestamp":"2018-08-28T09:34:55.0Z",
    "Reporter": { "IP Address": "192.168.100.249"},
    "Protocol": "EEE Company's protocol",
    "Requester": {
        "Unique Name": "0000",
        "Transmitted Code": "02000100... (Faked certification codes)"
    },
    "Responder": {
        "Unique Name": "0002",
        "Transmitted Code": "000000000010000c"
    },
    "Error Code": "21",
    "Error Message": "Certification Failed",
    "Description": {
        "Status": "This message was sent from IDS not IoTGW"
    },
}
```

Рисунок I.4 – Журнал регистрации ошибок IoT при ошибке проверки сертификата (пример)

I.3 Злоумышленник физически взламывает измерительное устройство, регулярно передающее данные без запроса

На рисунке I.5 показан злоумышленник, который физически вывел из строя измерительное устройство, регулярно передающее данные без запроса. После этого MCU1 не может передать какие-либо данные. В этом случае шлюз IoTGW обнаруживает аномальную ситуацию, связанную с MCU1, и передает журнал регистрации ошибок IoT, показанный на рисунке I.6.

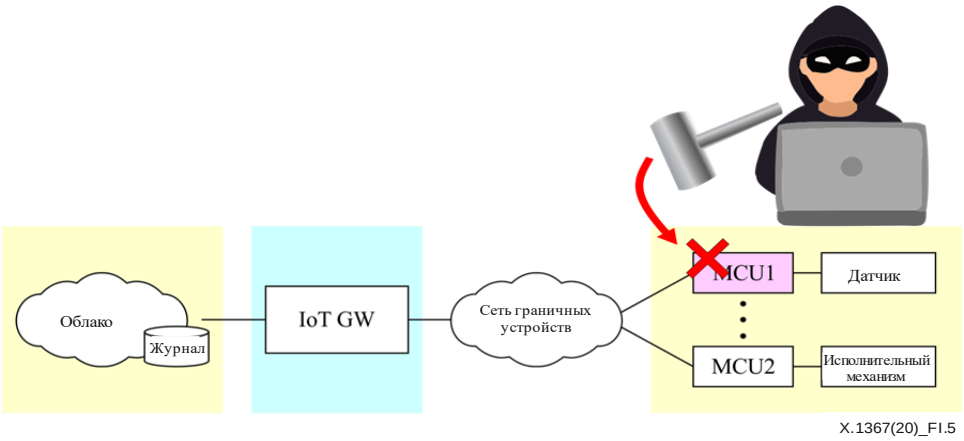


Рисунок I.5 – Злоумышленник физически вывел из строя MCU1

```
{
    "Timestamp":"2018-08-28T09:34:55.0Z",
    "Reporter": { "IP Address": "192.168.10.254"},
    "Protocol": "ZZZ Company's protocol",
    "Requester": {},
    "Responder": {
        "Unique Name": "0002",
        "Transmitted Code": ""
    },
    "Error Code": "11",
    "Error Message": "Communication Failed",
    "Description": {
        "Responder stopped sending data."
    },
}
```

Рисунок I.6 – Журнал регистрации ошибок IoT, переданный при потере связи (пример)

I.4 Как использовать журналы IoT при реагировании на инцидент

На заводе три экосистемы IoT подключены к одной и той же локальной сети (ЛС), как показано на рисунке I.7.

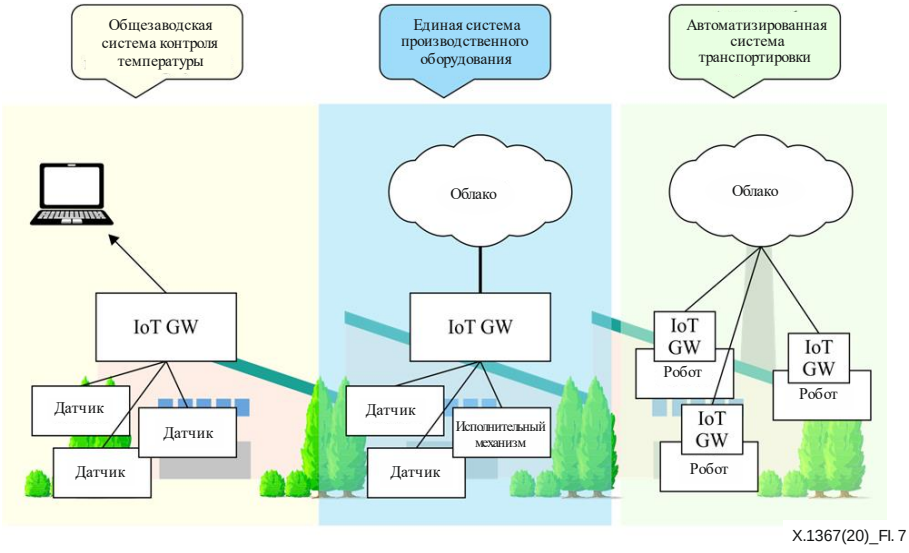
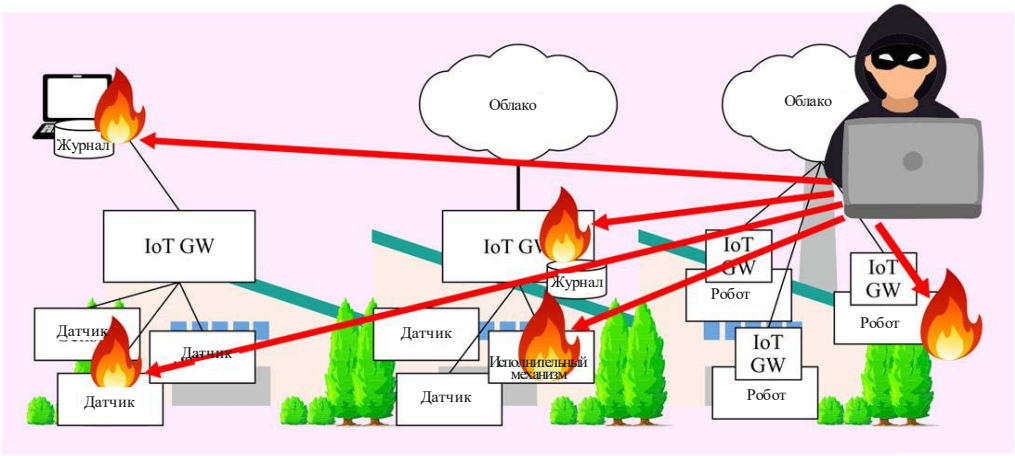


Рисунок I.7 – Несколько экосистем IoT на заводе

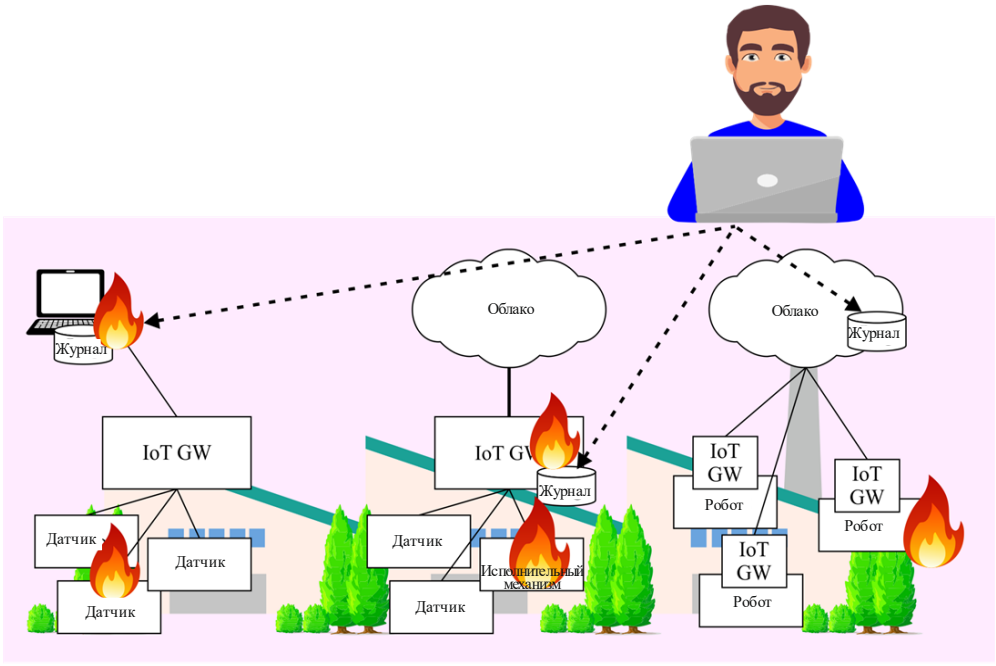
В этом случае злоумышленник легко может атаковать каждое устройство, как показано на рисунке I.8. Если журналы ошибок IoT отсутствуют, группе реагирования на инциденты безопасности (SIRT) сложно отследить злоумышленника, поскольку объединить нестандартные журналы IoT каждой из экосистем IoT не удается.



X.1367(20)_FI.8

Рисунок I.8 – Злоумышленник атакует все экосистемы IoT одновременно

Если же эти экосистемы IoT будут использовать стандартный формат журнала регистрации ошибок IoT, то SIRT легко сможет объединить все журналы ошибок IoT, как показано на рисунке I.9, а также унифицировать системный журнал. Тогда этого злоумышленника можно будет отследить.



X.1367(20)_FI. 9

Рисунок I.9 – Объединение и анализ всех журналов регистрации ошибок IoT

Дополнение II

Предполагаемое реагирование на инцидент безопасности с использованием журнала регистрации ошибок интернета вещей

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Стандартный журнал регистрации ошибок IoT, описанный в настоящей Рекомендации, можно использовать для реагирования на инциденты безопасности в экосистеме IoT. На рисунке II.1 показан процесс обнаружения инцидентов с использованием журнала регистрации ошибок IoT.

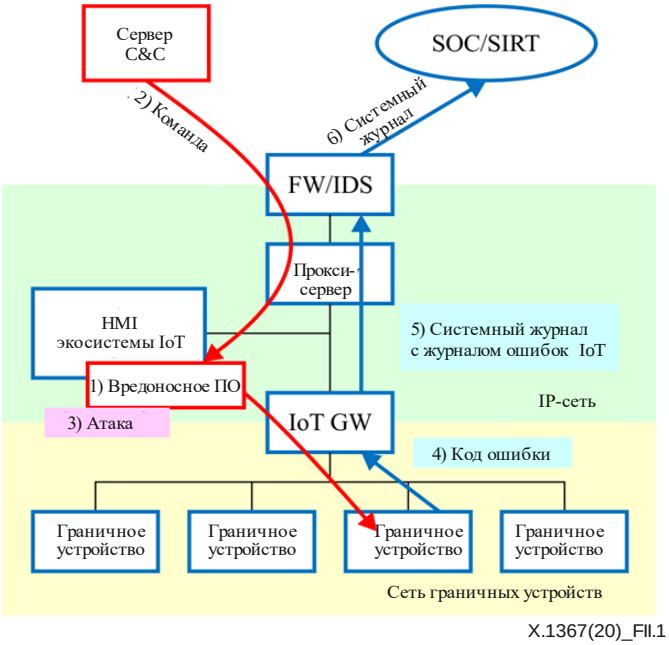


Рисунок II.1 – Обнаружение инцидента с использованием журнала регистрации ошибок IoT

1) Вредоносное ПО каким-то образом заражает интерфейс человек-машина (HMI), например настольный ПК.

2) Вредоносное ПО получает команды от командного сервера (C&C). Межсетевой экран (FW), IDS или прокси-сервер могут вести журнал сеансов связи между вредоносным ПО и сервером C&C.

3) Вредоносное ПО ищет уязвимость граничного устройства IoT. Граничное устройство IoT передает в IoTGW множество кодов ошибок, поскольку вредоносная программа часто пытается отправлять команды с различными параметрами. Для граничного устройства IoT эти параметры почти всегда неверны.

4) Для каждого отправленного кода ошибки IoT шлюз IoTGW передает в FW или IDS журнал регистрации ошибок IoT в указанном в настоящей Рекомендации формате с использованием протокола системного журнала.

5) Прокси-сервер также отправляет журналы сеансов связи с использованием протокола системного журнала в FW или IDS, которые передают все журналы, включая журнал регистрации ошибок IoT, в центр обеспечения безопасности (SOC) или SIRT с использованием протокола системного журнала.

Аналитики в SOC или SIRT могут не отреагировать на один журнал регистрации ошибок IoT, не связанный с другими журналами регистрации ошибок IoT. Однако они могут заметить аномальную ситуацию при постоянном поступлении в SOC или SIRT большого количества журналов регистрации ошибок IoT, поскольку это может быть вызвано тем, что злоумышленник ищет уязвимость в системе IoT.

Настоящая Рекомендация позволяет аналитикам SOC или SIRT обнаруживать атаки на граничные устройства IoT, поскольку SOC или SIRT получает коды ошибок IoT в стандартном формате журнала регистрации ошибок IoT. Затем они проверят другие соответствующие журналы, в том числе журнал обмена данными между вредоносным ПО и сервером C&C, и уведомят оператора завода, чтобы тот изолировал данный настольный ПК от локальной сети или удалил вредоносное ПО из настольного ПК.

Библиография

[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.1277] Recommendation ITU-T X.1277 (2018), *Universal authentication framework.*

[b-ITU-T Y.4000] Рекомендация МСЭ-Т Y.4000/Y.2060 (2012 г.), *Обзор 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.4109] Рекомендация МСЭ-Т Y.4109/Y.2061 (2012 г.), *Требования к поддержке приложений машинно-ориентированной связи в среде сетей последующих поколений.*

[b-ISO 8601-1] ISO 8601-1:2019, *Date and time – Representations for information interchange – Part 1: Basic rules.*

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

[b-ISO/IEC 14543-4-3] ISO/IEC 14543-4-3:2015, *Information technology – Home Electronic Systems (HES) architecture – Part 4-3: Application layer interface to lower communications layers for network enhanced control devices of HES Class 1.*

[b-ISO/IEC 17000] ISO/IEC 17000:2004, *Conformity assessment – Vocabulary and general principles.*

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

[b-IEEE 802.15.1] IEEE 802.15.1-2005, *IEEE Standard for information technology – Local and metropolitan area networks – Specific requirements – Part 15.1a: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPAN).*

[b-IEEE 802.15.4] IEEE 802.15.4-2015, *IEEE Standard for low-rate wireless networks*.

[b-IETF RFC 5424] IETF RFC 5424 (2009), *The syslog protocol*.

[b-oneM2M] oneM2M Partners (2017), Standards for M2M and Internet of things. Доступно [по состоянию на 12.02.2020 г.] по адресу: http://www.onem2m.org/

[b-SPI] Motorola (2001), SPI block guide, V04.01. Доступно [по состоянию на 12.02.2020 г.] по адресу: https://www.nxp.com/files-static/microcontrollers/doc/ref_manual/S12SPIV4.pdf

[b-UM10204] UM10204 (2014), *I^2C-bus specification and user manual*, Rev.6. Доступно [по состоянию на 12.02.2020 г.] по адресу: https://www.nxp.com/docs/en/user-guide/UM10204.pdf

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

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

Отпечатано в Швейцарии
Женева, 2021 г.