Международный союз электросвязи

# МСЭ-Т X.1541

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(09/2017)

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

Обмен информацией о кибербезопасности – Обмен информацией о событии/инциденте/эвристических правилах

## Формат обмена описаниями инцидентов как объектов, версия 2

Рекомендация МСЭ-Т X.1541

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 системы (ИТС) | X.1370–X.1389 |
| Безопасность технологии распределенного реестра | X.1400–X.1429 |
| 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 |

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

# Рекомендация МСЭ-Т X.1541

## Формат обмена описаниями инцидентов как объектов, версия 2


**Резюме**

В Рекомендации МСЭ-Т X.1541 представлено описание информационной модели формата обмена описаниями инцидентов как объектов (IODEF) версии 2 и приведена соответствующая модель данных в форме схемы XML. Формат IODEF определяет представление модели данных для совместного использования информации, которой обычно обмениваются, об инцидентах, связанных с нарушением компьютерной безопасности, или иных типах инцидентов. Для этого перечислены соответствующие пункты IETF RFC 7970 с указанием их характера – нормативного или информативного.



**Хронологическая справка**

| Издание | Рекомендация | Утверждение | Исследовательская комиссия | Уникальный идентификатор* |
|---|---|---|---|---|
| 1.0 | МСЭ-Т X.1541 | 07.09.2012 г. | 17-я | 11.1002/1000/11375 |
| 2.0 | МСЭ-Т X.1541 | 06.09. 2017 г. | 17-я | 11.1002/1000/13264 |


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

## ПРЕДИСЛОВИЕ

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

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

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

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

## ПРИМЕЧАНИЕ

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

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

## ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

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

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

**СОДЕРЖАНИЕ**

**Введение**

В Рекомендации МСЭ-Т X.1500 "Методы обмена информацией о кибербезопасности" приведено руководство по обмену информацией о кибербезопасности, в том числе об инцидентах и индикаторах, как это предусмотрено в настоящей Рекомендации. Формат обмена описаниями инцидентов как объектов (IODEF) – это модель данных для представления информации, которой обычно обмениваются, о компьютерной безопасности. Этот формат определяет представление модели данных XML для передачи информации об инциденте между объектами, на которые возложена эксплуатационная ответственность за осуществление упреждающих действий по защите, действий по ликвидации последствий или наблюдение и предупреждение определенного сообщества. Эта модель данных обеспечивает метод кодирования информации о хост-узлах, сетях и услугах, реализуемых в этих системах; о методе использования и связанных с этим данных; о последствиях инцидента, а также об ограниченных методах документирования потока операций.

Главное назначение IODEF состоит в расширении эксплуатационных возможностей и повышении уровня информированности о ситуации. Коллективное принятие IODEF укрепляет способность урегулирования инцидентов и передачи информации о ситуации с угрозами, благодаря упрощению совместной деятельности и обмену информацией. Структурированный формат IODEF обеспечивает:

- повышение уровня автоматизации при обработке информации об инциденте путем обмена информацией о структуре инцидента, что устраняет необходимость разбора специалистами по безопасности текстовых документов, составленных в произвольной форме;
- снижение объема работы при сопоставлении схожих данных (даже при высокой степени структурированности) из разных источников, что повышаем информированность о ситуации;
- общий формат, на основе которого обеспечивается функциональная совместимость средств обработки и анализа инцидентов, в особенности при поступлении информации от нескольких объектов.

Многочисленные процедурные, доверительные, политические и правовые факторы могут ограничивать или не позволять обмен информацией. IODEF является технической спецификацией и не предназначен для решения этих вопросов. Вместе с тем в эксплуатационных реализациях IODEF и связанных с ним форматах и протоколах при составлении соглашений об обмене информацией следует учитывать этот более широкий контекст.

# Рекомендация МСЭ-Т X.1541

## Формат обмена описаниями инцидентов как объектов, версия 2

### 1 Сфера применения

Формат обмена описаниями инцидентов как объектов (IODEF) определяет представление модели данных для совместного использования информации, которой обычно обмениваются, об инцидентах, связанных с нарушением компьютерной безопасности, или иных типах инцидентов. В настоящей Рекомендации представлено описание информационной модели IODEF и приведена соответствующая модель данных в форме схемы XML.

Любое представление или основа модели данных, позволяющие осуществлять обмен информацией об инцидентах, связанных с нарушением компьютерной безопасности, или иных типах инцидентов должны обеспечивать возможность соблюдения всех применимых национальных и региональных законов, нормативных актов и принципов политики.

Разработчики и пользователи всех Рекомендаций МСЭ-Т, включая настоящую Рекомендацию и ее базовые методы, должны соблюдать все применимые национальные и региональные законы, нормативные акты и принципы политики.

### 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.

[IETF RFC 5070] IETF RFC 7970 (2016), *The Incident Object Description Exchange Format Version 2*. <https://datatracker.ietf.org/doc/rfc7970/>

### 3 Определения

#### 3.1 Термины, определенные в других документах

Отсутствуют.

#### 3.2 Термины, определенные в настоящей Рекомендации

Отсутствуют.

### 4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

| | | |
|---|---|---|
| IANA | Internet Assigned Numbers Authority | Орган присвоения номеров интернета |
| IODEF | Incident Object Description Exchange Format | Формат обмена описаниями инцидентов как объектов |

### 5 Соглашения по терминологии

Следующие термины считаются равнозначными:

– Использование в МСЭ слов "должен" ("shall") и "обязан" ("must"), а также их отрицательных форм, считается равнозначным.

– Использование в МСЭ слова "должен" ("shall") равнозначно использованию в IETF слова "ОБЯЗАН" ("MUST").
– Использование в МСЭ выражения "не должен" ("shall not") равнозначно использованию в IETF термина "НЕ ОБЯЗАН" ("MUST NOT").

ПРИМЕЧАНИЕ. – В IETF слова "должен" ("shall") и "обязан" ("must"), написанные строчными буквами, используются в справочных текстах.

## 6 Формат обмена описаниями инцидентов как объектов

В пункте 6 определен формат обмена описаниями инцидентов как объектов (IODEF) версии 2, с прямым указанием раздела [IETF RFC 7970] путем согласования номеров пунктов с номерами разделов. Таким образом, например, пункт 6.x соответствует разделу x [IETF RFC 7970] и, в том числе, имеет то же название.

### 6.1 Введение

Раздел 1 [IETF RFC 7970] является информативным.

#### 6.1.1 Терминология

Подраздел 1.1 [IETF RFC 7970] является информативным.

#### 6.1.2 Условные обозначения

Подраздел 1.2 [IETF RFC 7970] является информативным.

#### 6.1.3 О модели данных IODEF

Подраздел 1.3 [IETF RFC 7970] является информативным.

#### 6.1.4 Изменения по сравнению с RFC 5070

Подраздел 1.4 [IETF RFC 7970] является информативным.

### 6.2 Типы данных IODEF

Раздел 2 [IETF RFC 7970] является информативным, однако его подразделы, а именно подразделы 2.1−2.15, носят нормативный характер. В них определены нижеследующие типы данных.

– Целые числа (определены в подразделе 2.1 [IETF RFC 7970])
– Действительные числа (определены в подразделе 2.2 [IETF RFC 7970])
– Символы и строки (определены в подразделе 2.3 [IETF RFC 7970])
– Многоязычные строки (определены в подразделе 2.4 [IETF RFC 7970])
– Двоичные строки (определены в подразделе 2.5 [IETF RFC 7970])
  – Байты в Base64 (определены в подразделе 2.5.1 [IETF RFC 7970])
  – Шестнадцатеричные байты (определены в подразделе 2.5.2 [IETF RFC 7970])
– Перечислимые типы (определены в подразделе 2.6 [IETF RFC 7970])
– Строка "дата-время" (определена в подразделе 2.7 [IETF RFC 7970])
– Строка "часовой пояс" (определена в подразделе 2.8 [IETF RFC 7970])
– Список портов (определен в подразделе 2.9 [IETF RFC 7970])
– Почтовый адрес (определен в подразделе 2.10 [IETF RFC 7970])
– Телефонный номер (определен в подразделе 2.11 [IETF RFC 7970])
– Строка электронной почты (определена в подразделе 2.12 [IETF RFC 7970])
– Строки универсального указателя ресурсов (определены в подразделе 2.13 [IETF RFC 7970])
– Идентификаторы и ссылки на идентификаторы (определены в подразделе 2.14 [IETF RFC 7970])
– ПО (определено в подразделе 2.15 [IETF RFC 7970])

  - Класс "Ссылка на ПО" (SoftwareReference) (определен в подразделе 2.15.1 [IETF RFC 7970])
- Расширение (определено в подразделе 2.16 [IETF RFC 7970])

### 6.3 Модель данных IODEF

Раздел 3 [IETF RFC 7970] является информативным, однако его подразделы, а именно подразделы 3.1−3.29, носят нормативный характер. В них определены нижеследующие модели данных.

- Класс "Документ IODEF" (IODEF-Document) (определен в подразделе 3.1 [IETF RFC 7970])
- Класс "Инцидент" (Incident) (определен в подразделе 3.2 [IETF RFC 7970])
- Общие атрибуты – (определены в подразделе 3.3 [IETF RFC 7970])
  - Атрибут ограничения (определен в подразделе 3.3.1 [IETF RFC 7970])
  - Атрибут идентификатора видимого (определен в подразделе 3.3.2 [IETF RFC 7970])
- Класс "Идентификатор инцидента" (IncidentID) (определен в подразделе 3.4 [IETF RFC 7970])
- Класс "Идентификатор варианта" (AlternativeID) (определен в подразделе 3.5 [IETF RFC 7970])
- Класс "Связанная деятельность" (RelatedActivity) (определен в подразделе 3.6 [IETF RFC 7970])
- Класс "Злоумышленник" (ThreatActor) (определен в подразделе 3.7 [IETF RFC 7970])
- Класс "Кампания" (Campaign) (определен в подразделе 3.8 [IETF RFC 7970])
- Класс "Контактная информация" (Contact) (определен в подразделе 3.9 [IETF RFC 7970])
  - Класс "Дескриптор реестра" (RegistryHandle) (определен в подразделе 3.9.1 [IETF RFC 7970])
  - Класс "Почтовый адрес" (PostalAddress) (определен в подразделе 3.9.2 [IETF RFC 7970])
  - Класс "Адрес электронной почты" (Email (подраздел 3.9.3 [IETF RFC 7970])
  - Класс "Телефонный номер" (Telephone) (определен в подразделе 3.9.4 [IETF RFC 7970])
- Класс "Обнаружение" (Discovery) (определен в подразделе 3.10 [IETF RFC 7970])
  - Класс "Шаблон выявления" (DetectionPattern) (определен в подразделе 3.10.1 [IETF RFC 7970])
- Класс "Метод" (Method) (определен в подразделе 3.11 [IETF RFC 7970])
  - Класс "Ссылка" (Reference) (определен в подразделе 3.11.1 [IETF RFC 7970])
- Класс "Оценка" (Assessment) (определен в подразделе 3.12 [IETF RFC 7970])
  - Класс "Воздействие на систему" (SystemImpact) (определен в подразделе 3.12.1 [IETF RFC 7970])
  - Класс "Воздействие на деятельность" (BusinessImpact) (определен в подразделе 3.12.2 [IETF RFC 7970])
  - Класс "Воздействие по времени" (TimeImpact) (определен в подразделе 3.12.3 [IETF RFC 7970])
  - Класс "Финансовое воздействие" (MonetaryImpact) (определен в подразделе 3.12.4 [IETF RFC 7970])
  - Класс "Достоверность" (Confidence) (определен в подразделе 3.12.5 [IETF RFC 7970])
- Класс "Журнал событий" (History) (определен в подразделе 3.13 [IETF RFC 7970])
  - Класс "Запись в журнале" (HistoryItem) (определен в подразделе 3.13.1 [IETF RFC 7970])
- Класс "Данные о событии" (EventData) (определен в подразделе 3.14 [IETF RFC 7970])
  - Соотношение классов Incident и EventData (определено в подразделе 3.14.1 [IETF RFC 7970])
  - Рекурсивное описание EventData (определено в подразделе 3.14.2 [IETF RFC 7970])

- Класс "Ожидание" (Expectation) (определен в подразделе 3.15 [IETF RFC 7970])
- Класс "Поток" (Flow) (определен в подразделе 3.16 [IETF RFC 7970])
- Класс "Система" (System) (определен в подразделе 3.17 [IETF RFC 7970])
- Класс "Узел" (Node) (определен в подразделе 3.18 [IETF RFC 7970])
  - Класс "Адрес" (Address) (определен в подразделе 3.18.1 [IETF RFC 7970])
  - Класс "Роль узла" (NodeRole) (определен в подразделе 3.18.2 [IETF RFC 7970])
  - Класс "Счетчик" (Counter) (определен в подразделе 3.18.3 [IETF RFC 7970])
- Класс "Данные о домене" (DomainData) (определен в подразделе 3.19 [IETF RFC 7970])
  - Класс "Серверы имен" (Nameservers) (определен в подразделе 3.19.1 [IETF RFC 7970])
  - Класс "Контактная информация для домена" (DomainContacts) (определен в подразделе 3.19.2 [IETF RFC 7970])
- Класс "Сервис" (Service) (определен в подразделе 3.20 [IETF RFC 7970])
  - Класс "Имя сервиса" (ServiceName) (определен в подразделе 3.20.1 [IETF RFC 7970])
  - Класс "Прикладной заголовок " (ApplicationHeader) (определен в подразделе 3.20.2 [IETF RFC 7970])
- Класс "Данные электронной почты" (EmailData) (определен в подразделе 3.21 [IETF RFC 7970])
- Класс "Запись" (Record) (определен в подразделе 3.22 [IETF RFC 7970])
  - Класс "Данные записи" (RecordData) (определен в подразделе 3.22.1 [IETF RFC 7970])
  - Класс "Структура записи" (RecordPattern) (определен в подразделе 3.22.2 [IETF RFC 7970])
- Класс "Измененные ключи реестра ОС Windows" (WindowsRegistryKeysModified) (определен в подразделе 3.23 [IETF RFC 7970])
  - Класс "Ключ" (Key) (определен в подразделе 3.23.1 [IETF RFC 7970])
- Класс "Данные сертификата" (CertificateData) (определен в подразделе 3.24 [IETF RFC 7970])
  - Класс "Сертификат" (Certificate) (определен в подразделе 3.24.1 [IETF RFC 7970])
- Класс "Описание файла" (FileData) (определен в подразделе 3.25 [IETF RFC 7970])
  - Класс "Файл" (File) (определен в подразделе 3.25.1 [IETF RFC 7970])
- Класс "Описание хэша" (HashData) (определен в подразделе 3.26 [IETF RFC 7970])
  - Класс "Хэш" (Hash) (определен в подразделе 3.26.1 [IETF RFC 7970])
  - Класс "Нечеткий хэш" (FuzzyHash) (определен в подразделе 3.26.2 [IETF RFC 7970])
- Класс "Данные подписи" (SignatureData) (определен в подразделе 3.27 [IETF RFC 7970])
- Класс "Данные индикатора" (IndicatorData) (определен в подразделе 3.28 [IETF RFC 7970])
- Класс "Индикатор" (Indicator) (определен в подразделе 3.29 [IETF RFC 7970])
  - Класс "Идентификатор индикатора" (IndicatorID) (определен в подразделе 3.29.1 [IETF RFC 7970])
  - Класс "Альтернативные идентификаторы индикатора" (AlternativeIndicatorID) (определен в подразделе 3.29.2 [IETF RFC 7970])
  - Класс "Видимое" (Observable) (определен в подразделе 3.29.3 [IETF RFC 7970])
  - Класс "Выражение индикатора" (IndicatorExpression) (определен в подразделе 3.29.4 [IETF RFC 7970])
  - Класс "Выражения с выражением индикатора" (Expressions with IndicatorExpression) (определен в подразделе 3.29.5 [IETF RFC 7970])
  - Класс "Ссылка на видимое" (ObservableReference) (определен в подразделе 3.29.6 [IETF RFC 7970])

– Класс "Ссылка на индикатор" (IndicatorReference) (определен в подразделе 3.29.7 [IETF RFC 7970])
– Класс "Фаза атаки" (AttackPhase) (определен в подразделе 3.29.8 [IETF RFC 7970])

### 6.4 Соображения, касающиеся обработки

Раздел 4 [IETF RFC 7970] является нормативным, однако некоторые его подразделы носят информативный характер, как показано в нижеследующих пунктах.

#### 6.4.1 Кодирование

Подраздел 4.1 [IETF RFC 7970] является нормативным.

#### 6.4.2 Пространство имен IODEF

Подраздел 4.2 [IETF RFC 7970] является нормативным.

#### 6.4.3 Проверка

Подраздел 4.3 [IETF RFC 7970] является нормативным.

#### 6.4.4 Несовместимость с версией 1

Подраздел 4.4 [IETF RFC 7970] является информативным.

### 6.5 Расширение IODEF

Раздел 5 [IETF RFC 7970] является информативным.

В Рекомендации МСЭ-Т X.1500 "Методы обмена информацией о кибербезопасности" приведено руководство по обмену информацией о кибербезопасности, в том числе об инцидентах и индикаторах, как это предусмотрено в настоящей Рекомендации (МСЭ-Т X.1541). В настоящей Рекомендации (МСЭ-Т X.1541) представлен базовый формат для обмена информацией об инцидентах, однако он охватывает не все случаи использования в соответствии с [b-ITU-T X.1500]. Для охвата необходимых сценариев использования могут быть разработаны расширения.

#### 6.5.1 Расширение количества перечислимых значений атрибутов

Подраздел 5.1 [IETF RFC 7970] и его подразделы являются нормативным.

#### 6.5.2 Расширяющие классы

Подраздел 5.2 [IETF RFC 7970] и его подразделы являются нормативным.

### 6.6 Вопросы интернационализации

Раздел 6 [IETF RFC 7970] является нормативным.

### 6.7 Примеры

Раздел 7 [IETF RFC 7970] и его подразделы, в которых описаны примеры документов IODEF, являются информативными.

### 6.8 Модель данных IODEF (схема XML)

Раздел 8 [IETF RFC 7970] является нормативным.

### 6.9 Соображения, касающиеся безопасности

Раздел 9 [IETF RFC 7970] и его подразделы являются нормативными.

В реализациях, соответствующих МСЭ-Т, базовый формат и протокол передачи сообщений, используемые для обмена экземплярами IODEF, должны обеспечивать надлежащие гарантии конфиденциальности, целостности и аутентичности.

ПРИМЕЧАНИЕ. – В IETF слово "обязан" ("must"), написанное строчными буквами, используются в информативных текстах.

### 6.10 Соображения, касающиеся IANA

Раздел 10 [IETF RFC 7970] и его подразделы являются нормативными.

### 6.11 Справочные документы

#### 6.11.1 Нормативные справочные документы

Подраздел 11.1 [IETF RFC 7970] является информативным.

В настоящей Рекомендации МСЭ-Т подраздел 11.1 [IETF RFC 7970] определен как информативный, поскольку МСЭ-Т не выработал позицию по каким-либо из этих справочных документов в связи с настоящей Рекомендацией. Вместе с тем признается, что IETF определила ряд нормативных справочных документов для [IETF RFC 7970].

#### 6.11.2 Информативные справочные документы

Подраздел 11.2 [IETF RFC 7970] является информативным.

## Библиография

[b-ITU-T X.1500] Рекомендация МСЭ-Т X.1500 (2011 г.), *Методы обмена информацией о кибербезопасности*.

## 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 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, 2018 г.