Международный союз электросвязи

МСЭ-Т X.1581

(09/2012)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

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

Обмен информацией, касающейся кибербезопасности – Гарантированный обмен

Транспортирование сообщений для обеспечения межсетевой защиты в реальном времени

Рекомендация МСЭ-Т X.1581

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	
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	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	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1339
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**

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

Рекомендация МСЭ-Т X.1581

Транспортирование сообщений для обеспечения межсетевой защиты в реальном времени

Резюме

В Рекомендации МСЭ-Т X.1581 определяется протокол транспортирования для обеспечения межсетевой защиты в реальном времени (RID), основанной на передаче сообщений RID по протоколу передачи гипертекста/безопасности транспортного уровня (HTTP/TLS). Это достигается путем перечисления соответствующих пунктов RFC 6546 IETF с указанием их характера – нормативного или информативного.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия
1.0	МСЭ-Т X.1581	07.09.2012 г.	17-я

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 извещение 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

		Стр.
1	Сфера применения	1
2	Справочные документы	1
3	Определения	1
3.1	Термины, определенные в других документах	1
3.2	Термины, определенные в настоящей Рекомендации	1
4	Сокращения и акронимы	1
5	Соглашения по терминологии	2
6	Транспортирование сообщений межсетевой защиты в реальном времени	2
6.1	Введение	2
6.2	Терминология	2
6.3	Передача сообщений RID по HTTP/TLS	2
6.4	Соображения, касающиеся безопасности	2
6.5	Соображения, касающиеся IANA	2
6.6	Выражение признательности	2
6.7	Справочные документы	2
Библиография		3

Введение

В Рекомендации МСЭ-Т X.1500 "Методы обмена информацией о кибербезопасности" содержатся руководящие указания по обмену информацией о кибербезопасности, в том числе по инцидентам и индикаторам, как предусмотрено в настоящей Рекомендации. Формат обмена описаниями инцидентов как объектов (IODEF) определяет общее представление модели данных с использованием расширяемого языка разметки (XML) для обмена информацией об инцидентах в сфере компьютерной безопасности, а межсетевая защита в реальном времени (RID) обеспечивает метод безопасного обмена документами в IODEF, предназначенными для совместной обработки инцидентов безопасности между заинтересованными сторонами. В настоящей Рекомендации определяется протокол транспортирования для обеспечения RID, основанной на обмене сообщениями RID по протоколу передачи гипертекста/безопасности транспортного уровня (HTTP/TLS).

В пункте 6 определяется метод транспортирования сообщений межсетевой защиты в реальном времени (RID).

Рекомендация МСЭ-Т X.1581

Транспортирование сообщений для обеспечения межсетевой защиты в реальном времени

1 Сфера применения

В настоящей Рекомендации определяется протокол транспортирования для обмена сообщениями межсетевой защиты в реальном времени (RID) по протоколу передачи гипертекста/безопасности транспортного уровня (HTTP/TLS).

Реализации, позволяющие осуществлять обмен информацией об инцидентах, должны обеспечивать возможность соответствия всем применимым национальным и региональным законам, нормативным актам и принципам политики.

Пользователи всех Рекомендаций МСЭ-Т, включая настоящую Рекомендацию и ее базовые методы, должны следовать всем применимым национальным и региональным законам, нормативным актам и принципам политики.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылки 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 пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других источников, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

[IETF RFC 6546] IETF RFC 6546 (2012), *Transport of Real-time Inter-network Defense (RID) Messages over HTTP/TLS*.
<https://datatracker.ietf.org/doc/rfc6546/>

3 Определения

3.1 Термины, определенные в других документах

Нет.

3.2 Термины, определенные в настоящей Рекомендации

Нет.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

HTTP	Hypertext Transfer Protocol	Протокол передачи гипертекста
IANA	Internet Assigned Numbers Authority	Орган присвоения номеров интернета
RID	Real-time Inter-network Defense	Межсетевая защита в реальном времени
TLS	Transport Layer Security	Безопасность транспортного уровня
XML	eXtensible Markup Language	Расширяемый язык разметки

5 Соглашения по терминологии

Следующие термины считаются равнозначными:

- Использование в МСЭ слов "должен" ("shall") и "обязан" ("must"), а также их отрицательных эквивалентов, 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 Транспортирование сообщений межсетевой защиты в реальном времени

В пункте 6 определяется транспортирование сообщений межсетевой защиты в реальном времени (RID), как это предусмотрено в [IETF RFC 6546]. В этом пункте содержатся прямые ссылки на [IETF RFC 6546] путем расположения номеров подпунктов и разделов таким образом, чтобы подпункт 6.x соответствовал разделу x [IETF RFC 6546] с таким же названием.

6.1 Введение

Раздел 1 [IETF RFC 6546] является информативным.

6.1.1 Изменения из RFC6046

Раздел 1 [IETF RFC 6546] является информативным.

6.2 Терминология

Раздел 2 [IETF RFC 6546] является нормативным.

6.3 Передача сообщений RID по HTTP/TLS

Раздел 3 [IETF RFC 6546] является нормативным.

6.4 Соображения, касающиеся безопасности

Раздел 4 [IETF RFC 6546] является нормативным.

6.5 Соображения, касающиеся IANA

Раздел 5 [IETF RFC 6546] является нормативным.

6.6 Выражение признательности

Раздел 6 [IETF RFC 6546] является информативным.

6.7 Справочные документы

6.7.1 Нормативные справочные документы

Раздел 7.1 [IETF RFC 6546] является информативным.

В настоящей Рекомендации раздел 7.1 [IETF RFC 6546] 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 6546].

6.7.2 Информативные справочные документы

Раздел 7.2 [IETF RFC 6546] является информативным.

Библиография

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

[b-ITU-T X.1541] Рекомендация МСЭ-Т X.1541, *Формат обмена описаниями инцидентов как объектов*.

[b-ITU-T X.1580] Рекомендация МСЭ-Т X.1580, *Межсетевая защита в реальном времени*.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
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	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	Оконечное оборудование, субъективные и объективные методы оценки
Серия Q	Коммутация и сигнализация
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 и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2012 г.