Международный союз электросвязи

МСЭ-Т

X.1582

(01/2014)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

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

Обмен информацией, касающейся кибербезопасности – Гарантированный обмен

Протоколы транспортирования, поддерживающие обмен информацией о кибербезопасности

Рекомендация МСЭ-Т X.1582

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**
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.1582

Протоколы транспортирования, поддерживающие обмен информацией о кибербезопасности

Резюме

В Рекомендации МСЭ-Т X.1582 приводится обзор протоколов транспортирования, которые были приняты и адаптированы для использования в рамках обмена информацией о кибербезопасности (CYBEX). В Рекомендации описываются приложения транспортирования, характеристики протоколов транспортирования, а также аспекты безопасности.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1582	24.01.2014 г.	17-я	11.1002/1000/12037

Ключевые слова

Информация о кибербезопасности, протоколы обмена информацией, передача информации.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: http://handle.itu.int/, после которого следует 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 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

Введение

Для обмена информацией о кибербезопасности уже существует и применяется ряд механизмов и протоколов обмена. Вместе с тем многие, если не большинство из них, либо находятся в частном пользовании и не документированы должным образом, либо широко не известны, что затрудняет их использование в глобальном обмене информацией о кибербезопасности. Кроме того, большинство современных приложений обмена применяются среди ограниченных партнеров по обмену, ограниченных по числу или зоне операций в области кибербезопасности.

Для обеспечения более глобального и функционально совместимого обмена информацией о кибербезопасности среди более широкого круга возможных прикладных областей "*Обмен информацией о кибербезопасности*" (CYBEX) содержит обзор семейства спецификаций конкретных протоколов, обеспечивающих придание глобального характера обмену информацией о кибербезопасности в возможно более широком круге прикладных областей и между ними.

Рекомендация МСЭ-Т X.1582

Протоколы транспортирования, поддерживающие обмен информацией о кибербезопасности

1 Сфера применения

В настоящей Рекомендации приводится обзор протоколов передачи и обмена, которые были стандартизированы для и/или в ходе использования в настоящее время в прикладной области передачи информации о кибербезопасности и обмена ею и которые были приняты и адаптированы для использования в рамках Рекомендаций МСЭ-Т серии X.1500.

Настоящая Рекомендация применима в наибольшей степени для проектировщиков и разработчиков, в чью компетенцию входит обеспечение передачи информации о кибербезопасности и обмена ею в локальном, региональном и глобальном масштабах.

2 Справочные материалы

В нижеследующих Рекомендациях МСЭ-Т и других справочных документах содержатся положения, которые, посредством ссылок в настоящем тексте, составляют положения настоящей Рекомендации. На время публикации указанные здесь издания были действительными. Все Рекомендации и другие справочные документы постоянно пересматриваются, поэтому всем пользователям данной Рекомендации настоятельно рекомендуется изучить возможность использования последних изданий перечисленных ниже Рекомендаций и других справочных документов. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется.

Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

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

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 кибербезопасность [ITU-T X.1205]: Набор средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, руководящих принципов, подходов к управлению рисками, действий, профессиональной подготовки, передового опыта, страхования и технологий, которые могут быть использованы для защиты киберсреды, ресурсов организации и пользователя. Ресурсы организации и пользователя включают подсоединенные компьютерные устройства, персонал, инфраструктуру, приложения, услуги, системы электросвязи и всю совокупность переданной и/или сохраненной информации в киберсреде. Цель кибербезопасности заключается в достижении и сохранении свойств безопасности ресурсов организации или пользователя, направленных против соответствующих рисков безопасности в киберсреде. Общие задачи обеспечения безопасности включают доступность, целостность (которая может включать аутентичность и недопущение отказа от авторства) и конфиденциальность.

ПРИМЕЧАНИЕ. – (не является частью [b-ITU-T X.1205]) В ряде национальных и региональных нормативных и законодательных актов может потребоваться реализация механизмов защиты информации, позволяющей установить личность.

3.1.2 протокол обмена [ITU-T X.1500]: Набор технических правил и формат, которые регулируют обмен информацией между двумя или несколькими объектами.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины:

3.2.1 Объект кибербезопасности: любой объект, обладающий информацией о кибербезопасности или стремящийся ее получить.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

BEEP	Blocks Extensible Exchange Protocol	Протокол для расширяемого обмена блоками информации
CAPEC	Common Attack Pattern Enumeration and Classification	Перечень и классификация общеизвестных схем атак
CYBEX	Cybersecurity Information Exchange	Обмен информацией о кибербезопасности
DDoS	Distributed Denial of Service	Распределенный отказ в обслуживании
EVCERT	Extended Validation Certificate	Сертификат с расширенной валидацией
HTTP	Hypertext Transfer Protocol	Протокол передачи гипертекста
HSTS	Hypertext transfer protocol Strict Transport Security	Строгая безопасность передачи информации по протоколу передачи гипертекста
IODEF	Incident Object Description Exchange Format	Формат обмена описаниями инцидентов как объектов
MIME	Multi-purpose Internet Mail Extensions	Многоцелевые расширения почты в интернете
RID	Real-time Inter-network Defense	Межсетевая защита в реальном времени
RSS	Really Simple Syndication	Очень простое приобретение информации
SCTP	Stream Control Transmission Protocol	Протокол передачи для управления потоком
SOAP	Simple Object Access Protocol	Простой протокол доступа к объектам
TCP	Transmission Control Protocol	Протокол управления передачей
TLS	Transport Layer Security	Безопасность транспортного уровня
UDP	User Datagram Protocol	Протокол дейтаграмм пользователя
URI	Uniform Resource Identifier	Универсальный идентификатор ресурса
XML	extensible Markup Language	Расширяемый язык разметки

5 Условные обозначения

Не имеется.

6 Протоколы транспортирования, обеспечивающие обмен информацией о кибербезопасности

6.1 Применение транспортирования

Обмен информацией о кибербезопасности охватывает большое разнообразие сценариев использования, которые могут осуществляться с помощью нескольких протоколов транспортирования, каждый из которых обладает уникальными характеристиками. Для сопоставления их характеристик ниже описываются четыре типовых применения транспортирования.

6.1.1 Распространение информации

Объекты кибербезопасности могут распространять информацию на недискриминационной основе. Это может осуществляться посредством широко доступных протоколов для подачи данных, таких как RSS. В таких целях распространения информации тот же набор информации может предоставляться любой стороне без фильтрации или корректировки данных для конкретной стороны.

6.1.2 Опубликовать-подписаться

Объект кибербезопасности может стать абонентом определенного поставщика информации на двусторонней основе, и этот поставщик информации может поставлять данные, соответствующие потребностям конкретной запрашивающей стороны. При таком сценарии поставщик информации может выступать в качестве посредника между издателем информации (например, поставщиком программного обеспечения) и абонентом. Такие услуги "опубликовать-подписаться" требуют

фильтрации на уровне посредника, что, в свою очередь, делает обязательными перечень и запрос, например, перечень активов или запрос на соответствующую информацию.

6.1.3 Гарантированный обмен информацией

Объекты кибербезопасности с аналогичными возможностями могут обмениваться информацией между собой для расширения охвата или ускорения реагирования на инциденты. Формат обмена описаниями инцидентов как объектов (IODEF) [b-ITU-T X.1541] и межсетевая защита в реальном времени (RID) [b-ITU-T X.1580] представляют собой два таких протокола для сообщения подробной информации. Объекты кибербезопасности определят участвующие в связи конечные точки, и им потребуется аутентификация и гарантия в отношении друг друга. В целях такого гарантированного обмена каждому объекту кибербезопасности может потребоваться инициировать сеанс связи с другими объектами. Это можно осуществить с помощью двунаправленных протоколов транспортирования.

6.1.4 Доказательства обладания информацией

Объекты кибербезопасности могут пожелать осуществлять связь с участвующими сторонами, которые наблюдали конкретное событие или инцидент, не раскрывая подробной информации другим незатронутым соседям. Это может осуществляться с помощью определенного класса криптографического протокола, например с помощью сохраняющего конфиденциальность пересечения множеств [b-Kissner]. По сути по такому криптографическому протоколу происходит обмен доказательствами наличия информации без обмена самой информацией, и тем самым гарантируется конфиденциальность важной информации. Такие криптографические протоколы можно применять поверх двунаправленных протоколов транспортирования.

6.2 Соображения, касающиеся протоколов транспортирования

В зависимости от ролей, придаваемых объектам кибербезопасности, конечные точки связи могут действовать асимметрично или на равных основаниях.

В типичном случае, когда роли обеих конечных точек устанавливаются асимметрично, уместными считаются протоколы типа "запрос-ответ", поскольку сеанс связи всегда инициирует одна из конечных точек. Когда обе конечные точки действуют на равных основаниях, они обе могут инициировать сеанс связи, поэтому уместными считаются двунаправленные протоколы.

6.2.1 Протоколы типа "запрос-ответ"

В протоколах типа "запрос-ответ" клиент является инициатором соединения, а сервер – отвечающей стороной. Здесь направление потока информации не связано с различием между клиентом и сервером; клиенты могут поставлять информацию или потреблять информацию, в зависимости от разделения ролей.

При протоколах типа "запрос-ответ" серверы могут быть не в состоянии своевременно распространять информацию среди клиентов, если клиенты не ведут опрос серверов. Другими словами, клиенты являются инициаторами обмена информацией, а серверы – отвечающей стороной обмена информацией.

Существующие протоколы типа "запрос-ответ" перечислены в таблице 1.

Таблица 1 − Существующие протоколы типа "запрос-ответ" для передачи и обмена

Название протокола	Характеристики	Справочные материалы
Протокол передачи гипертекста (HTTP)	HTTP обеспечивает базовые механизмы получения информации от отвечающей стороны или предоставления ей информации. HTTP может использоваться для обмена информацией любого типа, которая может быть идентифицирована универсальным идентификатором ресурса (URI) и тип которой может быть указан типами многоцелевых расширений почты в интернете (MIME).	[b-IETF RFC 2616]
Простой протокол доступа к объектам (SOAP)	SOAP надстраивается поверх HTTP для содействия связи пар атрибут-значение. Схема расширяемого языка разметки (XML) используется для указания типа атрибут-значение.	[b-SOAP]

6.2.2 Двунаправленные протоколы

При двунаправленных протоколах обе конечные точки могут быть инициаторами обмена информацией. Такие протоколы могут быть асимметричными, т. е. одна конечная точка считается клиентом и должна инициировать соединение. Другой такой протокол может быть симметричным, т. е. обе конечные точки могут по собственному желанию инициировать соединение.

С двунаправленными протоколами своевременный обмен информацией возможен без значительного объема периодических опросов. Преимущества двунаправленных протоколов не ограничиваются случаями симметричного использования, когда несколько объектов кибербезопасности обмениваются информацией между собой; имеются преимущества в плане масштабируемости, когда требуется распространение информации среди большого числа узлов клиентов.

Также возможно создать двунаправленное соединение из пары независимых соединений типа "запрос-ответ". При таком сочетании обе конечные точки должны действовать как клиент и сервер, что может вызвать дополнительные проблемы внедрения программного обеспечения.

Существующие двунаправленные протоколы перечислены в таблице 2.

Таблица 2 − Существующие двунаправленные протоколы для передачи и обмена

Название протокола	Характеристики	Справочные материалы
Протокол для расширяемого обмена блоками информации (BEEP)	BEEP способен работать как с симметричными, так и с асимметричными конечными точками. Обе конечные точки могут быть инициаторами и отвечающими сторонами соединения.	[b-IETF RFC 3080]
WebSocket	Протокол WebSocket надстраивается поверх HTTP, ввиду чего клиенты всегда являются инициаторами соединения. Хотя между клиентом и сервером существует различие, сервер может инициировать взаимодействие протокола через инициированное клиентом соединение.	[b-IETF RFC 6455]

6.3 Соображения, касающиеся безопасности

Среди протоколов транспортирования CYBEX протоколы, поддерживаемые веб-браузерами, до их принятия требуют тщательного анализа безопасности, поскольку некоторые веб-браузеры обеспечивают элементарный уровень разделения между сценариями, осуществляемыми на веб-сайтах, часто с различной степенью надежности. Тогда как действительный объект кибербезопасности может

применять веб-браузеры для обмена информацией, тот же вариант веб-браузера может использоваться для навигации по ненадежным веб-сайтам, на которых может содержаться потенциально вредоносный для конкретной конечной точки CYBEX код. Из числа таких угроз межсайтовая подделка запросов (CSRF) (CAPEC ID 62) и межсайтовый скриптинг (XSS) (CAPEC ID 63) в настоящее время известны как проявления, фактически нарушающие принцип разделения веб-сайтов с различными уровнями надежности.

Контрмеры против таких угроз существуют в виде расширений HTTP, показанных в таблице 3. Поддерживаемые расширения могут варьироваться в зависимости от торговой марки и версии веб-браузера.

Таблица 3 − Существующие расширения HTTP для повышения безопасности

Название	Характеристики	Справочные материалы
Политика безопасности контента (CSP)	CSP может ограничивать источники встроенных объектов, в том числе динамично выполняемых скриптов, до предварительно определенного набора веб-сайтов.	[b-CSP]
Строгая безопасность передачи информации по протоколу HTTP (HSTS)	HSTS может ограничивать последующие взаимодействия протоколов безопасным каналом, таким как безопасность транспортного уровня (TLS), на определенный период времени.	[b- IETF RFC 6797]
HttpOnly	HttpOnly ограничивает доступ программ, выполняемых в веб-браузерах, к данным аутентификации, например cookie-файлы.	[b- IETF RFC 6265]
Origin Cookies	Origin Cookies препятствует другим веб-сайтам в затирании cookie-файлов, установленных первоначальным веб-сервером; изменить изначальные cookie-файлы можно только из точного места происхождения.	[b-Bortz]

Другие протоколы уровня приложений могут подвергаться тем же угрозам. Современные веб-браузеры могут выполнять произвольные программы в рамках дополнительных программных модулей, такие как скрипты Java и Flash, поэтому они могут использоваться для подделки взаимодействия протоколов. Ввиду этого конечным точкам CYBEX следует избегать размещения и использования программного обеспечения из ненадежных источников, в том числе с веб-сайтов. Если применение таких мер к другой конечной точке CYBEX считается невыполнимым ввиду недискриминационной природы конкретного приложения, требуется измерение существующего риска и контроль за ним.

6.4 Аспекты транспортного и сеансового уровней

Учитывая, что конечным точкам CYBEX необходимо защищать неприкосновенность канала связи, рекомендуется использовать TCP или SCTP [b-IETF RFC 4960]. Наряду с этим разработчикам конечных точек CYBEX следует рассмотреть вопрос о защите от отказа в обслуживании различными способами, например с помощью SYN Cookies [b-IETF RFC 4987] и других контрмер против распределенного отказа в обслуживании (DDoS) [b-Mirkovic]. Разработчики могут дополнительно укрепить защищенность канала связи кодами аутентификации сообщения, определенными в варианте аутентификации протокола управления передачей (TCP) [b-IETF RFC 5925] и аутентификации "по кускам" протокола передачи для управления потоком (SCTP) [b-IETF RFC 4895].

Известные угрозы SCTP перечислены в [b-IETF RFC 5062], наряду с контрмерами против них. Не следует использовать UDP, для того чтобы свести к минимуму риск атаки по методу отражения [b-Paxson].

Для обеспечения конфиденциальности связи рекомендуется использовать TLS [b-IETF RFC 5246] [b-IETF RFC 3436]. Если считается необходимым обеспечение идентичности конечной точки, рекомендуется использовать сертификат с расширенной валидацией (EVCERT) [b-EVCERT].

Библиография

[b-ITU-T X.1205] Рекомендация МСЭ-Т X.1205 (2008 г.), *Обзор кибербезопасности.*

[b-ITU-T X.1541] Рекомендация МСЭ-Т X.1541 (2012 г.), *Формат обмена описаниями инцидентов как объектов.*

[b-ITU-T X.1544] Рекомендация МСЭ-Т X.1544 (2013 г.), *Перечень и классификация общеизвестных схем атак*.

[b-ITU-T X.1580] Рекомендация МСЭ-Т X.1580 (2012 г.), *Межсетевая защита в реальном времени*.

[b-Bortz] Andrew Bortz, Adam Barth and Alexei Czeskis, Origin Cookies: Session Integrity for Web Applications, W2SP 2011.

[b-CSP] W3C, Content Security Policy 1.0.
http://www.w3.org/TR/CSP/

[b-EVCERT] CA/Browser Forum, *Guidelines for the Issuance and Management of Extended Validation Certificates*, Ver. 1.3.

[b-IETF RFC 2616] IETF RFC 2616 (1999), *Hypertext Transfer Protocol* – HTTP/1.1.

[b-IETF RFC 3080] IETF RFC 3080 (2001), *The Blocks Extensible Exchange Protocol Core*.

[b-IETF RFC 3436] IETF RFC 3436 (2002), *Transport Layer Security over Stream Control Transmission Protocol*.

[b-IETF RFC 4895] IETF RFC 4895 (2007), *Authenticated Chunks for the Stream Control Transmission Protocol*.

[b-IETF RFC 4960] IETF RFC 4960 (2007), *Stream Control Transmission Protocol*.

[b-IETF RFC 4987] IETF RFC 4987 (2007), *TCP SYN Flooding Attacks and Common Mitigations*.

[b-IETF RFC 5062] IETF RFC 5062 (2007), *Security Attacks Found Against the Stream Control Transmission Protocol (SCTP) and Current Countermeasures*.

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.

[b-IETF RFC 5925] IETF RFC 5925 (2010), *The TCP Authentication Option*.

[b-IETF RFC 6265] IETF RFC 6265 (2011), *HTTP State Management Mechanism*.

[b-IETF RFC 6455] IETF RFC 6455 (2011), *The WebSocket Protocol*.

[b-IETF RFC 6797] IETF RFC 6797 (2012), *HTTP Strict Transport Security*.

[b-Kissner] Lea Kissner and Dawn Song, *Privacy-Preserving Set Operations*, CRYPTO 2005.

[b-Mirkovic] Jelena Mirkovic and Peter Reiher, *A Taxonomy of DDoS Attack and DDoS Defense Mechanisms*, ACM SIGCOMM Computer Communication Review, 34(2), April 2004.

[b-Paxson] Vern Paxson, *An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks*, ACM SIGCOMM Computer Communication Review, 31(3), July 2001.

[b-SOAP] W3C, *Simple Object Access Protocol*.
SOAP Version 1.2 Part 1: Messaging Framework (2007).
SOAP Version 1.2 Part 2: Adjuncts (2007).

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, 2014 г.