Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1248

(09/2017)

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

Безопасность киберпространства – Противодействие спаму

Технические требования для противодействия распространению спама при мгновенном обмене сообщениями

Рекомендация МСЭ-Т X.1248

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.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	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.1248

Технические требования для противодействия распространению спама при мгновенном обмене сообщениями

Резюме

В Рекомендации МСЭ-Т X.1248 определены характеристики спама, распространяемого при мгновенном обмене сообщениями (спим), и описаны технические требования для противодействия спаму. С ростом популярности мгновенного обмена сообщениями распространение спима становится все более серьезной проблемой. Характеристики мгновенного обмена сообщениями, такие как функционирование на базе протокола Интернет (IP) и широкое использование, за которое не взимается плата, потенциально способствуют масштабному и не поддающемуся контролю распространению спима. Проблему спима следует решать всесторонне, в противном случае он может оказать негативное воздействие на использование самой услуги мгновенного обмена сообщениями.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1248	06.09.2017 г.	17-я	11.1002/1000/13262

Ключевые слова

Спам, распространяемый при мгновенном обмене сообщениями, спим.

* 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 результате стремительного развития интернета (в частности, мобильного) услуги мгновенного обмена сообщениями превратились из простого средства для ведения бесед в комплексную информационную платформу, в рамках которой интегрированы связь, информация, развлечения, поиск, электронная торговля, деловое сотрудничество и внутрикорпоративное взаимодействие с пользователями. Поскольку услуги мгновенного обмена сообщениями дешевы и просты в использовании, все больше людей начинают пользоваться ими взамен традиционных видов связи, что серьезно сказывается на последних. Сегодня растет число операторов электросвязи, предоставляющих услуги мгновенного обмена сообщениями, но в то же время распространение спама при мгновенном обмене сообщениями наряду с голосовой связью и SMS приняло критические масштабы. Операторы электросвязи во всем мире в разной степени осведомлены о спаме, распространяемом при мгновенном обмене сообщениями, и затронуты этим явлением. Спим приводит не только к напрасной трате сетевых ресурсов, но также к потере времени и снижению производительности труда пользователей. Кроме того, он используется для фишинга и распространения вирусов, червей, шпионских программ и других видов вредоносных программных средств. Наконец, спим может содержать вредную информацию, имеющую оскорбительный для пользователей характер. Таким образом, спим снижает удовлетворенность пользователей услугами мгновенного обмена сообщениями, и это стало важным фактором, препятствующим использованию этих услуг.

Хотя в системах мгновенного обмена сообщениями реализован целый ряд мер противодействия спаму, в них по-прежнему остается множество слабых мест, которыми могут пользоваться распространители спима: неограниченная скорость регистрации, отсутствие подтверждения приема сообщений, незащищенные механизмы передачи данных по сети, отсутствие у пользователей возможности ограничить скорость передачи входящих сообщений, неизбежные уязвимости систем мгновенного обмена сообщениями.

Настоящая Рекомендация устанавливает технические требования к противодействию спиму в контексте функциональности системы обмена ими с целью остановить производство и распространение спима. Например, важное значение имеет требование разработки регистрационного механизма для предотвращения массовой автоматической регистрации, а также предоставления пользователям возможности выбора – получать или блокировать сообщения от авторизованных или неавторизованных абонентов, а также ограничивать скорость отправки сообщений пользователем при превышении порогового значения.

Рекомендация МСЭ-Т X.1248

Технические требования для противодействия распространению спама при мгновенном обмене сообщениями

1 Сфера применения

В настоящей Рекомендации определяются типы и характеристики спама, распространяемого при мгновенном обмене сообщениями (СПИМ). В целях сдерживания выработки и распространения спима Рекомендация устанавливает технические требования к противодействию спиму на клиентской и серверной стороне услуги мгновенного обмена сообщениями. Настоящая Рекомендация главным образом посвящена мерам противодействия спиму на уровне системы мгновенного обмена сообщениями и применима к операторам услуг мгновенного обмена сообщениями.

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 мгновенный обмен сообщениями (instant messaging (IM)) [b-IETF RFC 3428]: Обмен содержанием между несколькими участниками в режиме, близком к реальному времени. Как правило, содержанием являются короткие текстовые сообщения, хотя это и не обязательно.

3.1.2 спам (spam) [b-ITU-T X.1240]: Значение слова "спам" зависит от понимания неприкосновенности частной жизни в каждой стране и от того, что составляет спам с технической, социально-экономической и практической точек зрения. В частности, с развитием технологий содержание спама меняется, становясь все шире и открывая все новые возможности для злоупотреблений электронными средствами связи. Не существует согласованного на международном уровне определения спама, однако этот термин обычно используется для обозначения рассылаемых в массовом порядке по электронной почте или подвижной связи незапрашиваемых сообщений, целью которых является, как правило, продвижение продуктов или услуг коммерческого характера.

3.1.3 спам, распространяемый при мгновенном обмене сообщениями (spam over instant messaging (спим)) [b-ITU-T X.1244]: Спам, целью которого являются пользователей услуги мгновенного обмена сообщениями.

3.1.4 спимер (spimmer) [b-ITU-T X.1244]: Отправитель спама при мгновенном обмене сообщениями.

3.2 Термины, определенные в настоящей Рекомендации

Отсутствуют.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

ID	Identity		Идентификатор
IM	Instant Messaging		Мгновенный обмен сообщениями
IP	Internet Protocol		Протокол Интернет
SMS	Short Message Service		Услуга передачи коротких сообщений
SPIM	Spam over Instant Messaging	Спим	Спам, распространяемый при мгновенном обмене сообщениями

5 Условные обозначения

Отсутствуют.

6 Характеристики и сценарии выработки спима

Спим – это содержимое принятого пользователем мгновенного сообщения, которое воспринимается этим пользователем как нежелательное или мешающее. Таким образом, спим имеет нижеследующие характеристики.

– Обычно передается в реальном времени. Если как отправитель, так и получатель находятся в сети, спим принимается практически сразу после отправки. Если получатель не в сети, он все равно может получить спим сразу после того, как войдет в сеть.

– Часто рассылается массово, т. е. в форме большого количества параллельно рассылаемых сообщений с одинаковым содержимым.

– Неавторизованный отправитель спима получателям в мгновенных сообщениях называется спимером. Вместе с тем может случиться, что учетная запись одного из корреспондентов пользователя будет скомпрометирована и в мгновенных сообщениях с этой учетной записи может рассылаться спим из-за заражения вредоносным кодом или раскрытия учетной записи и пароля другому лицу. Спим, рассылаемый известными корреспондентами, более коварен, особенно когда он содержит ссылки на вредоносные веб-сайты или исполняемые файлы, которые большинство получателей будут склонны открыть, тем самым подвергнув свои системы повышенной опасности заражения вредоносным кодом.

– Установление источника спима в мгновенных сообщениях затруднено, поскольку учетные записи могут создаваться произвольным образом и, как правило, не прослеживаются до реальной личности.

Выработка спима тесно связана с функциональностью системы мгновенного обмена сообщениями (см. Дополнение I) и может происходить по нижеследующим сценариям.

– Спимеры автоматически регистрируют большое число учетных записей с помощью специального программного обеспечения и распространяют спим с этих учетных записей.

– Злоумышленники могут использовать фальшивые учетные записи в системах мгновенного обмена сообщениями и рассылать с них спим.

– Злоумышленник, несанкционированно завладевший учетной записью легитимного пользователя, изменяет пароль пользователя или другие аутентификационные данные, с тем чтобы использовать эту учетную запись (зачастую в течение длительного времени) для рассылки спима.

– Из-за несанкционированного изменения параметров приема у клиента мгновенного обмена сообщениями (IM-клиента) становится возможным прием спима без каких-либо ограничений.

– Мгновенные сообщения несанкционированно изменяются в ходе передачи. В мгновенное сообщение может быть вставлена реклама или вредоносный код, что превращает его в спим.

– Из-за отсутствия механизмов подтверждения спимер имеет возможность без ограничений добавлять корреспондентов и рассылать им спим.

В целях предотвращения рассылки спима необходимо принять комплексные меры противодействия с учетом всех присущих спиму характеристик и сценариев его выработки.

7 Функциональная архитектура противодействия спиму в услуге мгновенного обмена сообщениями

7.1 Общие сведения

Функциональная архитектура противодействия спиму в услуге мгновенного обмена сообщениями показана на рисунке 7-1.

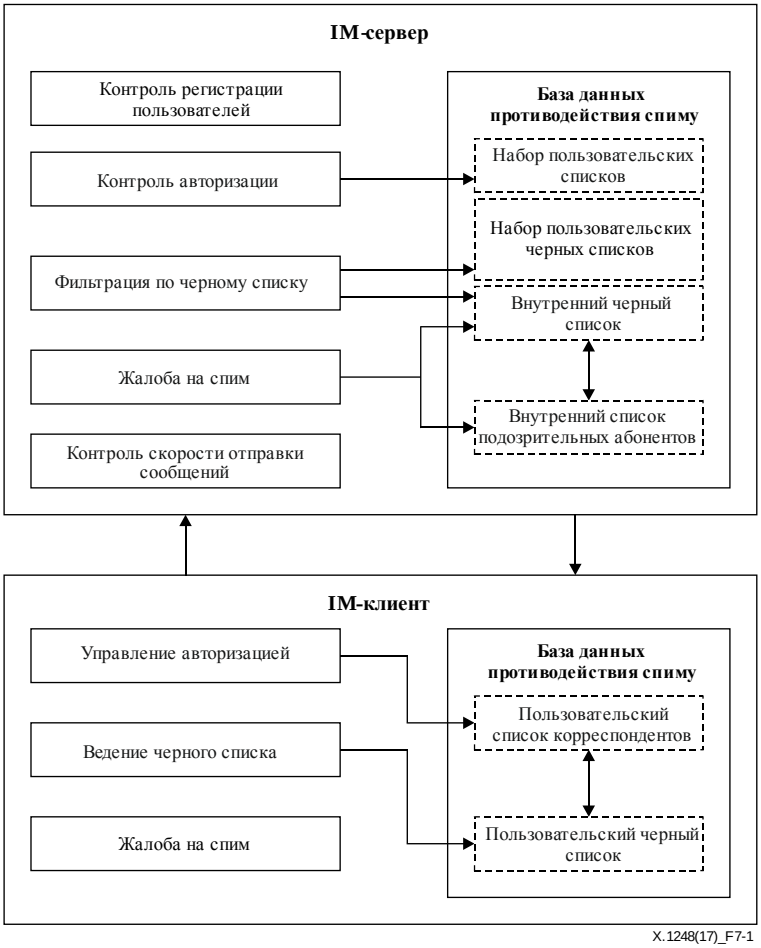

Рисунок 7-1 – Функциональная архитектура противодействия спиму в услуге мгновенного обмена сообщениями

В этой архитектуре предусмотрена функциональность для противодействия спиму, в том числе фильтры по черным спискам, средства контроля регистрации пользователей и средства подачи жалоб на спим. Что еще более важно, она поддерживает фильтрацию на базе ограничения скорости отправки мгновенных сообщений и контроль авторизации отправителя мгновенных сообщений.

В Дополнении I подробнее описана функциональность IM-клиента и IM-сервера, а также роли отправителя, получателя мгновенных сообщений и спимера.

7.2 Функциональность отдельных компонентов

7.2.1 IM-сервер

Функциональность IM-сервера включает в себя следующие шесть элементов:

1) Контроль регистрации пользователей.

   Требуется использовать ручные методы подтверждения (например, кодом, по электронной почте или по SMS) в целях предотвращения автоматической регистрации пользователей. Это не позволит спимерам, имеющим большое число автоматически зарегистрированных учетных записей, рассылать спим в мгновенных сообщениях.

2) Контроль авторизации.

   Требуется переадресовывать запрос пользователя на добавление корреспондента, а также разрешать или не разрешать установление связи с корреспондентом в зависимости от ответа IM-клиента.

3) Фильтрация по черному списку.

Требуется, чтобы IM-сервер фильтровал мгновенные сообщения по внутреннему черному списку и по набору черных списков, созданных пользователями.

4) Подача жалоб на спим.

Требуется принимать от пользователей жалобы на учетные записи, с которых рассылается спим, и принимать решение о внесении этих учетных записей во внутренний список подозрительных абонентов или внутренний черный список. Требуется обеспечить сопряжение с внешними системами обработки жалоб на спим, а также возможность импорта и экспорта встроенного черного списка.

5) Контроль скорости отправки сообщений.

Требуется контролировать количество мгновенных сообщений, отправляемых с одной и той же учетной записи за определенный период времени. Мгновенные сообщения, отправляемые сверх установленного лимита, должны блокироваться.

6) База данных противодействия спиму.

- Набор пользовательских списков корреспондентов: включает в себя список корреспондентов каждого пользователя, обслуживаемого IM-сервером. Требуется, чтобы пользовательский список корреспондентов, хранящийся на IM-сервере, синхронизировался с соответствующим списком IM-клиента.
- Набор пользовательских черных списков: включает в себя черный список каждого пользователя, обслуживаемого IM-сервером. Требуется обеспечить синхронизацию набора черных списков пользователя, хранящегося на сервере, с соответствующим черным списком IM-клиента.
- Внутренний черный список включает в себя учетные записи, указанные в жалобах пользователей и самостоятельно обнаруженные IM-сервером. Например, если пользователь отправляет мгновенные сообщения со скоростью, превышающей заданный порог, идентификатор этого пользователя добавляется во внутренний черный список IM-сервера. Кроме того, внутренний черный список включает учетные записи, данные о которых импортированы из других систем, например с других IM-серверов.
- Внутренний список подозрительных абонентов: требуется формировать список всех подозрительных учетных записей, обслуживаемых IM-сервером. Этот внутренний список может составляться по жалобам пользователей, по данным, импортированным из других систем и т. д.

7.2.2 IM-клиент

Функциональность IM-клиента включает в себя следующие три элемента:

1) Управление авторизацией.

Два важнейших компонента, которые должны присутствовать – это управление видимостью идентификационной информации в услуге мгновенного обмена сообщениями и управление запросами от неавторизованных абонентов. Первый из этих компонентов требует от пользователя решения, должна ли их идентификационная информация (например, идентификатор в услуге мгновенного обмена сообщениями, псевдоним, местоположение) быть видна неавторизованным абонентам. Второй компонент требует, чтобы пользователь мог выбирать подходящую политику обработки запросов от неавторизованных абонентов. Пользователь должен иметь возможность вручную одобрять запросы, требовать точного ответа на вопрос личного свойства или даже блокировать все запросы. Наконец, система должна обеспечивать пользователю возможность указывать доверенных корреспондентов и вести список его корреспондентов в IM-клиенте.

2) Управление черным списком.

Система должна позволять пользователям самостоятельно вести свои черные списки, и все сообщения с учетных записей, фигурирующих в пользовательском черном списке, должны блокироваться. У пользователей должна быть возможность добавлять, удалять свой черный список и даже делиться им с другими.

3) Подача жалоб на спим.

В IM-клиенте должна быть функция представления жалоб на учетные записи, с которых рассылается спим. Такой учетной записью может быть контакт в списке корреспондентов пользователя, участник IM-группы или даже учетная запись неавторизованного абонента, с которой отправлен запрос на авторизацию.

4) База данных противодействия спиму.

- Пользовательский список корреспондентов: требуется хранить список корреспондентов, одобренных пользователем.
- Пользовательский черный список: составляется пользователями и включает в себя учетные записи, сообщения с которых пользователь намерен блокировать.

База данных из IM-клиента автоматически передается на IM-сервер.

8 Рабочие процедуры

8.1 Рабочая процедура контроля скорости отправки сообщений

Лимит скорости отправки, т. е. максимально допустимое число сообщений, разрешенное к отправке с данной учетной записи за определенный временной интервал, должен устанавливаться на IM-сервере.

Данный лимит должен определяться посредством анализа большого количества образцов пользовательских сообщений с использованием таких технологий, как машинное обучение, глубокое обучение и т. п. Он должен устанавливаться для различных сценариев, включая следующие:

– мгновенные сообщения отправляются в адрес группы, членом которой является отправитель;

– мгновенные сообщения отправляются в адрес группы, членом которой отправитель не является;

– мгновенные сообщения отправляются одному или нескольким корреспондентам отправителя;

– мгновенные сообщения отправляются абонентам, не входящим в число корреспондентов отправителя.

Когда IM-сервер получает сообщения, отправленные с заданной учетной записи, он должен осуществлять контроль скорости отправки в соответствии со следующей процедурой, изображенной также в виде алгоритма на рисунке 8-1:

– Подсчитать количество сообщений, отправленных с учетной записи за определенный временной интервал.

– Сравнить количество отправленных сообщений (n) с наименьшим из лимитов, установленных для всех сценариев. Если число n превышает наименьший лимит, сервер мгновенного обмена сообщений определяет, какой сценарий реализуется в этом случае и превышает ли число n лимит для данного конкретного сценария. Если нет, IM-сервер переадресует сообщения получателю.

– Если количество отправленных сообщений (n) превышает лимит для данного сценария, IM-сервер проверяет, не входит ли учетная запись отправителя во внутренний список подозрительных абонентов. Если да, сервер отбрасывает эти сообщения; если нет – IM-сервер переадресует сообщения получателю, но вычисляет превышение лимита (m). Если число m больше некоторого заданного числа (α), IM-сервер добавляет учетную запись отправителя в список подозрительных абонентов.

Процесс контроля скорости отправки сообщений показан на рисунке 8-1.

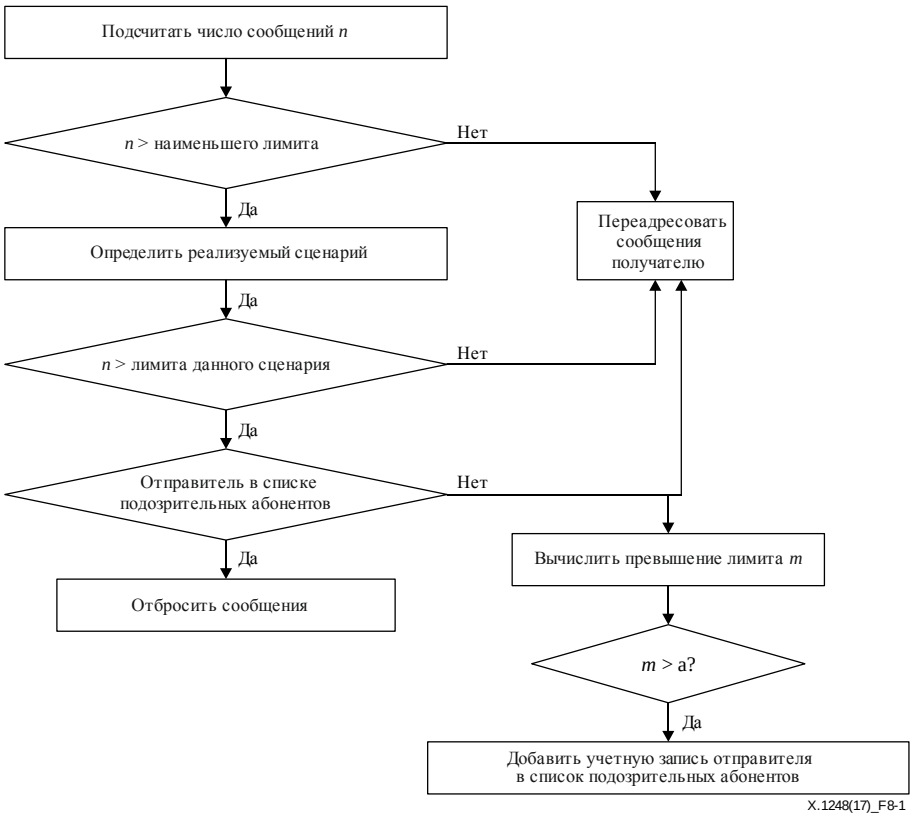

Рисунок 8-1 – Процесс контроля скорости отправки сообщений

8.2 Рабочая процедура ведения черных списков

Системы мгновенного обмена сообщениями относительно независимы друг от друга, поэтому от поставщиков услуг мгновенного обмена сообщениями требуется ведение собственных внутренних черных списков для соответствующих IM-серверов. Кроме того, в интересах пользователей требуется, чтобы в IM-клиентах были предусмотрены пользовательские черные списки.

Процедура взаимодействия со всеми видами черных списков в системе мгновенного обмена сообщениями такова:

– Пользователь редактирует свой пользовательский черный список в IM-клиенте. IM-сервер отслеживает пользовательский черный список в реальном времени и обновляет свой набор пользовательских черных списков, когда пользовательский список меняется.

– IM-сервер отслеживает, сколько раз одна и та же учетная запись была добавлена в пользовательские черные списки. Если это число превышает заданный порог, сервер вносит такую учетную запись в свой внутренний черный список.

– IM-сервер вносит учетную запись, указанную в жалобе пользователя, во внутренний список подозрительных абонентов, если ее нет ни в этом списке, ни в черном списке. IM-сервер подсчитывает, сколько жалоб поступило на одну и ту же учетная запись. Если это число превышает заданный порог, IM-сервер вносит такую учетную запись в свой внутренний черный список.

Процедура фильтрации сообщений по черным спискам такова:

– Когда на IM-сервер поступает сообщение, он проверяет, есть ли учетная запись отправителя во внутреннем черном списке; если да, сервер отбрасывает сообщение.

– Если учетной записи отправителя нет во внутреннем черном списке, сервер далее может проверить, нет ли этой записи в черном списке получателя, и если она там есть, сервер отбрасывает сообщение, а если нет, сервер переадресует сообщение получателю.

8.3 Процедуры управления авторизацией

Рекомендуется обеспечить наличие у IM-клиента функции, позволяющей пользователям выбрать, какие сообщения они хотят получать, а на IM-сервере должна быть обеспечена возможность фильтрации нежелательных сообщений в соответствии с пользовательским определением для предотвращения отправки нежелательных сообщений неавторизованными отправителями (абонентами, не являющимися корреспондентами пользователя, включая членов одной группы, корреспондентами пользователя в других системах мгновенного обмена сообщениями, контактами телефонной книги). Сценарии, по которым происходит авторизация отправителей, включают среди прочего следующие пять шагов:

1) IM-клиент настраивается на прием сообщений только от корреспондентов данного пользователя. Когда на IM-сервер приходит сообщение, отправленное пользователем B пользователю A, сервер проверяет, находится ли пользователь B в списке корреспондентов пользователя A. Если нет, сервер отбрасывает это сообщение.

2) IM-клиент настраивается на прием сообщений из групп, к которым пользователь явно присоединился. Когда на IM-сервер приходит сообщение, отправленное из группы B пользователю A, сервер проверяет, является ли пользователь A членом группы B. Если нет, сервер отбрасывает это сообщение. Кроме того, когда на IM-сервер поступает приглашение пользователю A от члена группы B, сервер должен добавлять пользователя A в группу B только с предварительного разрешения пользователя A.

3) IM-клиент настраивается на прием сообщений от члена группы, дружественной клиенту. Когда на IM-сервер приходит сообщение пользователю A от пользователя B, входящего в группу A, сервер проверяет, находится ли пользователь B в списке корреспондентов пользователя A. Если нет, сервер отбрасывает это сообщение.

4) IM-клиент настраивается на прием сообщений от учетных записей других IM-систем или контактов из телефонной книги только в том случае, если эти учетные записи или контакты были явно внесены пользователем в список корреспондентов. Когда на IM-сервер приходит сообщение, отправленное со связанной учетной записи B пользователю A, сервер проверяет, находится ли учетная запись B в списке корреспондентов пользователя A. Если нет, сервер отбрасывает это сообщение. Кроме того, когда на IM-сервер поступает запрос на добавление корреспондента из учетной записи B в список корреспондентов пользователя A, сервер должен выполнять это действие только с предварительного разрешения пользователя A.

5) IM-клиент настраивается на установление соединений пункта с пунктом только с корреспондентами пользователя. Когда IM-сервер получает запрос от пользователя B на установление соединения пункта с пунктом с пользователем A, сервер проверяет, находится ли пользователь B в списке корреспондентов пользователя A. Если да, сервер переадресует запрос пользователя B пользователю A и содействует пользователям A и B в установлении соединения пункта с пунктом. Если нет, сервер отбрасывает запрос пользователя B.

Взаимоотношения между пользователем A, пользователем B, группой A, группой B и учетной записью B показаны на рисунке 8-2.

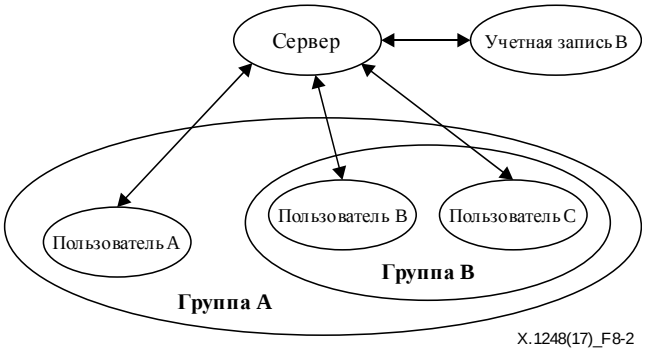

Рисунок 8-2 – Взаимоотношения между пользователями и группами

8.4 Процедуры управления регистрацией пользователей

В целях предотвращения автоматической регистрации учетных записей, в системах мгновенного обмена сообщения должна быть реализована одна мера или более для ручного подтверждения регистрации, например проверка кодом, по электронной почте или по SMS.

Когда пользователь отправляет регистрационную информацию (например, имя пользователя, пароль, номер мобильного телефона, адрес электронной почты) в IM-клиенте или на странице регистрации пользователей системы мгновенного обмена сообщениями, IM-сервер передает пользователю подтверждение регистрации в виде проверочного кода (напрямую или через SMS) или сообщения электронной почты.

После того как пользователь направляет обратно на IM-сервер подтверждение регистрации, IM-сервер проверяет регистрационную информацию, представленную пользователем. Если проверка пройдена, IM-сервер направляет пользователю сообщение об успешной регистрации и сохраняет его регистрационную информацию в базе данных. Если нет, сервер направляет пользователю сообщение о том, что регистрация не выполнена.

Система мгновенного обмена сообщений должна быть сопряжена с SMS-шлюзом или иметь в своем составе почтовый сервер для обретения функции отправки подтверждения регистрации пользователю в виде проверочного кода по SMS или сообщения электронной почты.

8.5 Процедуры приема и обработки жалоб на спим

Должны поддерживаться две процедуры приема жалоб на спим:

1) Прием жалоб через IM-клиента. При таком методе процесс обработки жалоб выглядит следующим образом:

   Пользователи системы мгновенного обмена сообщениями, получив спим, помечают соответствующим образом учетную запись отправителя в IM-клиенте; эта жалоба отправляется на IM-сервер. На IM-сервере должно быть задано пороговое число жалоб. Получив жалобу от пользователя, IM-сервер сначала проверяет, не входит ли указанная пользователем учетная запись во внутренний список подозрительных абонентов или внутренний черный список. Если нет, IM-сервер вносит ее во внутренний список подозрительных абонентов и подсчитывает число жалоб на эту учетную запись. Если это число превышает заданный порог, IM-сервер вносит такую учетную запись во внутренний черный список. Если учетная запись уже фигурирует во внутреннем списке подозрительных абонентов, IM-сервер отслеживает и накапливает жалобы на эту учетную запись. Если их число превышает заданный порог за определенный интервал времени, IM-сервер вносит такую учетную запись во внутренний черный список. Если учетная запись уже фигурирует во внутреннем черном списке, IM-сервер не выполняет никаких дополнительных действий. Сообщения, отправленные с этой учетной записи впоследствии, должны отбрасываться IM-сервером.

2) Прием жалоб через внешние системы обработки жалоб на спим. При таком методе процесс обработки жалоб выглядит следующим образом:

   Пользователи системы мгновенного обмена сообщениями, получив спим, направляют свои жалобы во внешнюю систему обработки жалоб. Внешняя система должна проанализировать жалобу пользователя и решить, следует ли добавить эту учетную запись в черный список. IM-сервер имеет интерфейс к внешней системе обработки жалоб на спим и импортирует или экспортирует черный список через этот интерфейс. Сообщения, отправленные с учетных записей, фигурирующих в черном списке, должны отбрасываться IM-сервером.

8.6 Процедура фильтрации спима

Когда на IM-сервер приходят мгновенные сообщения, он осуществляет фильтрацию спима в них по внутреннему черному списку и набору пользовательских черных списков. Этот процесс описан в п. 8.2.

Если учетной записи отправителя нет ни во внутреннем черном списке, ни в наборе пользовательских черных списков, IM-сервер осуществляет фильтрацию спима путем контроля авторизации, проверяя, есть ли у отправителя разрешение (авторизация) от получателя на отправку ему сообщений. Если нет, сообщение отбрасывается. Сценарий авторизации описан в п. 8.3.

Если авторизация имеется, IM-сервер осуществляет фильтрацию спима посредством контроля скорости отправки сообщений; этот процесс описан в п. 8.1.

Дополнение I

Роли и функции системы мгновенного обмена сообщениями

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Простейшая модель системы мгновенного обмена сообщениями показана на рисунке I.1.

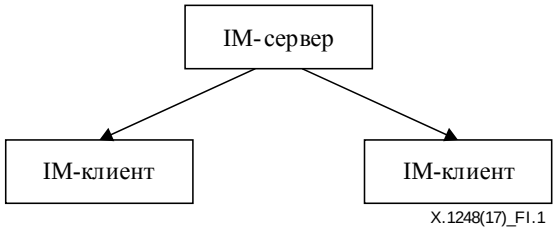

Рисунок I.1 – Простейшая модель системы мгновенного обмена сообщениями

Эта модель включает в себя IM-сервер и множество IM-клиентов. IM-сервер используется для приема и переадресации мгновенных сообщений, отправляемых IM-клиентами. IM-клиент имеет две роли: отправитель и получатель мгновенных сообщений. Отправитель мгновенных сообщений передает их на IM-сервер для доставки, а IM-сервер пытается доставить эти сообщения соответствующим получателям. Если отправитель мгновенных сообщений передает спим, он классифицируется как спимер.

Функции системы мгновенного обмена сообщениями должны реализовываться IM-сервером, соответствующими IM-клиентами и взаимодействием между ними.

Основные функции IM-сервера включают следующее:

– управление пользователями, в частности их регистрация, вход и выход из системы, редактирование учетных записей;

– управление мгновенными сообщениями, в частности их отправка, прием и передача;

– управление корреспондентскими отношениями, в частности поиск корреспондентов и ведение списков корреспондентов;

– управление системой, в частности настройка параметров, обновление, запуск, перезапуск и завершение работы системы.

Основные функции IM-клиента включают следующее:

– управление пользователями, в частности их регистрация, вход и выход из системы;

– управление мгновенными сообщениями, в частности их отправка и прием;

– управление корреспондентскими отношениями, в частности добавление, удаление и поиск корреспондентов;

– управление клиентом, в частности настройка параметров, обновление, запуск, перезапуск и завершение работы клиента.

Библиография

[b-ITU-T X.1231] Рекомендация МСЭ-Т X.1231 (2008 г.), *Технические методы противодействия спаму*.

[b-ITU-T X.1240] Рекомендация МСЭ-Т X.1240 (2008 г.), *Технологии, применяемые при противодействии спаму, рассылаемому по электронной почте*.

[b- ITU-T X.1244] Рекомендация МСЭ-Т X.1244 (2008 г.), *Общие аспекты противодействия спаму в мультимедийных IP-приложениях*.

[b-IETF RFC 2778] IETF RFC 2778 (2000), *A Model for Presence and Instant Messaging*.

[b-IETF RFC 3428] IETF RFC 3428 (2002), *Session Initiation Protocol (SIP) Extension for Instant Messaging*.

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.