

Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1245

(12/2010)

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

Безопасность киберпространства – Противодействие
спаму

**Структура противодействия спаму
в мультимедийных IP-приложениях**

Рекомендация МСЭ-Т X.1245

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.379
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	
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 Х.1245

Структура противодействия спаму в мультимедийных IP-приложениях

Резюме

В Рекомендации МСЭ-Т Х.1245 представлена общая структура противодействия мультимедийному IP-спаму. Структура может применяться к мультимедийным IP-приложениям, таким как IP-телефония, мгновенная передача сообщений, мультимедийная конференция и т. д. Структура состоит из 4 функций противодействия спаму, а именно базовой функции противодействия спаму (CASF), функции противодействия спаму на стороне получателя (RASF), функции противодействия спаму на стороне отправителя (CASF) и функций получателя спама (SRF). В настоящей Рекомендации описываются функциональные возможности и интерфейсы каждой функции, служащие для противодействия мультимедийному IP-спаму.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия
1.0	МСЭ-Т Х.1245	17.12.2010 г.	17-я

Ключевые слова

Функции противодействия спаму, мультимедийный IP-спам, спам.

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/>.

© ITU 2011

Все права сохранены. Ни одна из частей данной публикации не может быть воспроизведена с помощью каких бы то ни было средств без предварительного письменного разрешения МСЭ.

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 данной Рекомендации	1
4 Сокращения и акронимы	2
5 Условные обозначения	3
6 Технические методы для противодействия мультимедийному IP-спаму	3
6.1 Метод анализа источника	4
6.2 Метод анализа характеристик	5
6.3 Метод анализа контента	6
7 Структура противодействия мультимедийному IP-спаму	7
7.1 Спамер	7
7.2 Функции SAS	7
7.3 Функции RAS	11
7.4 Функции CAS	13
7.5 Функции SR	17
7.6 Основные точки в структуре	19
Дополнение I – Противодействие спаму при помощи создания трудностей для распространения спама	20
Дополнение II – Аспекты практической безопасности в процессе использованию структуры .	21
II.1 Аспекты безопасности	21
II.2 Практические аспекты	22
Библиография	24

Структура противодействия спаму в мультимедийных IP-приложениях

1 Сфера применения

В настоящей Рекомендации представлена общая структура противодействия мультимедийному IP-спаму. Структура может применяться к мультимедийным IP-приложениям, таким как IP-телефония, мгновенная передача сообщений, мультимедийная конференция и т. д. Структура включает четыре функции противодействия спаму, а именно базовую функцию противодействия спаму (CASf), функцию противодействия спаму на стороне получателя (RASf), функцию противодействия спаму на стороне отправителя (CASf) и функции получателя спама (SRF). В настоящей Рекомендации описываются функциональные возможности и интерфейсы каждой функции, служащие для противодействия мультимедийному IP-спаму. Технические средства для реализации данной структуры не входят в сферу применения настоящей Рекомендации.

Перед введением методов противодействия спаму, описанных в настоящей Рекомендации, следует проверить их соответствие всем законам и нормативным положениям.

2 Справочные документы

Нет.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 спам (spam) [b-ITU-T X.1240]: Значение слова "спам" зависит от того, что понимается под конфиденциальностью в каждой стране, и от того, что представляет собой спам в аспекте национальных технологий, а также с социально-экономической и практической точек зрения. В частности, с развитием технологий значение этого слова изменяется, становясь все шире и открывая все новые возможности для злоупотреблений электронными сообщениями. И хотя согласованного на международном уровне определения спама не существует, 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.

3.1.2 спамер (spammer) [b-ITU-T X.1240]: Организация или лицо, создающее и рассылающее спам.

3.2 Термины, определенные в данной Рекомендации

В настоящей Рекомендации определяются следующие термины:

3.2.1 функция противодействия спаму (anti-spam functions) (ASF): Логические функции для противодействия спаму в мультимедийных IP-приложениях. ASF могут находиться в сетевых элементах, таких как прокси-сервер, сервер приложений и т. д.

3.2.2 черный список (blacklist): Список идентификаций лиц или источников в услугах связи, где идентификации, включенные в список, получают отказ в доступе к конкретным ресурсам связи.

3.2.3 базовая ASF (core ASF) (CASf): Экземпляр ASF, который идентифицирует и блокирует мультимедийный IP-спам. Также имеет возможность управлять правилами противодействия спаму и контролировать RASf и SASf.

3.2.4 мультимедийный IP-спам (IP multimedia spam): Незапрашиваемые сообщения или вызовы в мультимедийных IP-приложениях, которые обычно имеют особые характеристики спама, такие как массовость. В отличие от традиционного спама в электронной почте, мультимедийный IP-спам обозначает спам, передаваемый с помощью методов связи по IP, таких как мгновенная передача сообщений или голосовая связь по IP.

3.2.5 ASF на стороне получателя (recipient-side ASF) (RASf): Экземпляр ASF, который идентифицирует и блокирует мультимедийный IP-спам, доставляемый получателю спама через границу внутренней сети. RASf могут находиться в сетевых элементах, где запросы входящей связи к получателю спама отправляются в качестве последнего скачка.

3.2.6 ASF на стороне отправителя (sender-side ASF) (SASf): Экземпляр ASF, который идентифицирует и блокирует мультимедийный IP-спам, доставляемый от спамера на границу внешней сети. SASf могут находиться в сетевых элементах, где запросы исходящей связи от спамера отправляются в качестве первого скачка.

3.2.7 получатель спама (spam recipient): Объект или лицо, получающее спам.

3.2.8 функция получателя спама (spam recipient functions) (SRF): ASF, роль которой заключается в идентификации и блокировании мультимедийного IP-спама, доставляемого получателю спама. SRF может находиться в домашней сети или терминалах получателя спама.

3.2.9 белый список (whitelist): Список идентификаций лиц или источников в услугах связи, где идентификации, включенные в список, являются известными, доверенными или имеют явно выраженное разрешение.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

ARS	Automated Response System	Система автоматического отклика
ASF	Anti-Spam Functions	Функции противодействия спаму
CA	Certification Authority	Орган сертификации
CAS	Core Anti-Spam	Базовое противодействие спаму
CASF	Core Anti-Spam Functions	Базовые функции противодействия спаму
CRL	Certificate Revocation List	Список отзыва сертификатов
DAC	Discretionary Access Control	Избирательное управление доступом
HBAC	History-based Access Control	Управление доступом на основе истории
IM	Instant Messaging	Мгновенная передача сообщений
IP	Internet Protocol	Протокол Интернет
IPSec	Internet Protocol Security	Безопасность протокола Интернет
L2TP	Layer 2 Tunneling Protocol	Протокол туннелирования уровня 2
MAC	Mandatory Access Control	Обязательное управление доступом
MTA	Mail Transfer Agent	Агент передачи сообщений электронной почты
NDAC	Non-Discretionary Access Control	Неизбирательное управление доступом
OTP	One Time Password	Одноразовый пароль
PBAC	Purpose-based Access Control	Целевое управление доступом
PKI	Public Key Infrastructure	Инфраструктура открытых ключей
RAS	Recipient-side Anti-Spam	Противодействие спаму на стороне получателя
RASf	Recipient-side Anti-Spam Functions	Функции противодействия спаму на стороне получателя
RBAC	Role-based Access Control	Управление доступом на основе ролей
RuBAC	Rule-based Access Control	Управление доступом на основе правил
SAS	Sender-side Anti-Spam	Противодействие спаму на стороне отправителя

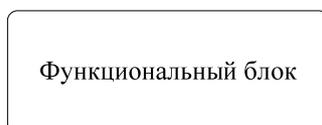
SASF	Sender-side Anti-Spam Fun	Функции противодействия спаму на стороне отправителя
SPF	Sender Policy Framework	Структура правил отправителя
SR	Spam Recipient	Получатель спама
SRF	Spam Recipient Functions	Функции получателя спама
SSL	Secure Socket Layer	Уровень безопасных соединений
TCAC	Temporal Constraints Access Control	Временные ограничения в управлении доступом
TTP	Trusted Third Party	Третья доверенная сторона
TTS	Text To Speech	Преобразование текста в речь
VoIP	Voice over Internet Protocol	Голосовая связь по IP-каналу
VPN	Virtual Private Network	Виртуальная частная сеть

5 Условные обозначения

Функции: В контексте структуры для противодействия мультимедийному IP-спаму, термин "функции" определяется как набор функциональных возможностей. Они представлены следующим символом:



Функциональный блок: В контексте структуры для противодействия мультимедийному IP-спаму, термин "функциональный блок" определяется как группа функциональных возможностей, которые далее не подразделяются на уровне деталей, описанных в данной Рекомендации. Он представлен следующим символом:

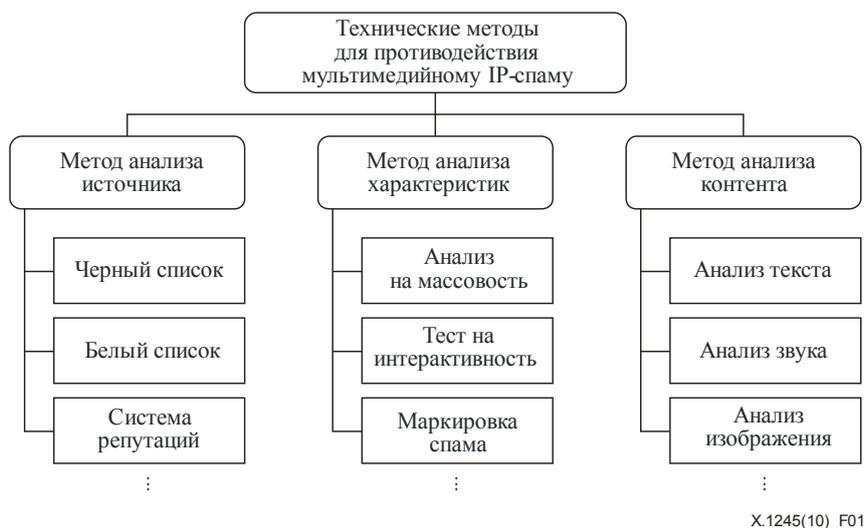


6 Технические методы для противодействия мультимедийному IP-спаму

Мультимедийный IP-спам может быть определен как незапрашиваемые сообщения или вызовы в мультимедийных IP-приложениях. В отличие от традиционного спама в электронной почте, мультимедийный IP-спам обозначает спам, передаваемый с помощью методов электросвязи по сетям IP, таких как голосовая связь по IP-каналу, мгновенная передача сообщений и т. д. Обычно мультимедийный IP-спам имеет особые характеристики, которые могут отличаться от обычных мультимедийных IP-приложений. Эти характеристики могут использоваться для функций противодействия спаму для идентификации и фильтрации спама путем реализации этих функций на соответствующих сетевых IP-элементах. Технические методы для противодействия мультимедийному IP-спаму могут классифицироваться по трем следующим категориям:

- противодействие мультимедийному IP-спаму посредством анализа источника мультимедийных IP-приложений;
- противодействие мультимедийному IP-спаму посредством анализа характеристик мультимедийных IP-приложений;
- противодействие мультимедийному IP-спаму посредством анализа контента мультимедийных IP-приложений.

На рисунке 1 представлены три технических метода противодействия мультимедийному IP-спаму и примеры применения методик противодействия спаму.



X.1245(10)_F01

Рисунок 1 – Технические методы противодействия мультимедийному IP-спаму

Многие методы противодействия спаму, показанные на рисунке 1, применяются для противодействия спаму в электронной почте, но также они могут применяться к мультимедийному IP-спаму. Методы противодействия спаму для противодействия мультимедийному IP-спаму не ограничиваются этими примерами.

Функции противодействия спаму по IP-сети должны взаимодействовать друг с другом, для того чтобы использовать данные методы противодействия спаму. Функции и интерфейсы объектов противодействия спаму, необходимых для реализации методов противодействия спаму описаны в следующих разделах. Для противодействия мультимедийному IP-спаму, возможно, не будет достаточно эффективным использование только одного метода противодействия спаму. В этом случае, для более эффективной фильтрации спама, возможно, в IP-сети должны быть развернуты одновременно больше одного метода противодействия спаму.

6.1 Метод анализа источника

Определить, являются ли спамом IP-приложения, полученные из определенного источника, можно по результатам анализа информации об источнике мультимедийных IP-приложений, такой как информация о репутации или спамовая история источника. В качестве идентификаторов источника могут использоваться IP-адрес, имя домена, телефонный номер и идентификатор пользователя.

Примерами методов противодействия спаму на основе источника являются белый список, черный список, система репутаций и т. д. Они широко используются для противодействия спаму в электронной почте, и также могут применяться для противодействия мультимедийному IP-спаму. Применение данных методов для мультимедийного IP-спама описано в [b-ITU-T X.1244]. Однако методы анализа источника могут иметь некоторые недостатки, которые будут снижать эффективность методов противодействия спаму, например спамеры могут попытаться замаскировать отправителя или смогут создать множество учетных записей услуг. Таким образом, для помощи в противодействии мультимедийному IP-спаму более эффективны следующие методы противодействия спаму на основе источника:

- строгая аутентификация источников мультимедийных IP-приложений;
- эффективное управление правилами идентификации спама и связанной с ними информации.

Во-первых, для эффективной фильтрации спама необходима высокая надежность информации источника мультимедийных IP-приложений, поскольку спамеры, стремясь избежать применения этих методов противодействия спаму, могут попытаться их обойти путем создания большого числа учетных записей услуг или пытаясь замаскировать отправителя, для того чтобы скрыть, что отправитель является спамером. Таким образом, для обеспечения высокой надежности информации источника может быть полезна строгая аутентификация источников мультимедийных IP-приложений.

Как описано выше, информация о фильтрации спама, например белый список, черный список и т. д., а также об источниках мультимедийных IP-приложений используется для идентификации спама. Таким образом, информация о фильтрации спама и критерий идентификации спама необходимы для эффективного управления.

Преимущество данного метода обуславливается тем, что спам можно заблокировать до того, как он будет отправлен получателю. Кроме того, если выполняются изложенные выше условия, возможно эффективно противостоять спаму, прилагая относительно небольшие усилия по сравнению с другими методами противодействия спаму, такими как анализ контента, анализ характеристик и т. д.

6.2 Метод анализа характеристик

6.2.1 Методы противодействия спаму, основанные на анализе характеристик

Мультимедийный IP-спам имеет много особых характеристик, которые могут отличать его от обычных мультимедийных IP-приложений. Например, мультимедийный IP-спам иногда доставляется в массовом порядке и имеет ограниченную интерактивность по сравнению с обычными мультимедийными IP-приложениями. Мультимедийное IP-приложение может рассматриваться как спам и отфильтровываться, если оно имеет одну или несколько таких характеристик. Существуют, но не ограничиваются ими, следующие некоторые характеристики мультимедийного IP-спама:

– Массовый порядок

Мультимедийный IP-спам иногда доставляется в массовом порядке, поскольку спамеры обычно пытаются отправить спам одновременно большому числу получателей спама, для того чтобы минимизировать стоимость рассылки спама. Когда большое количество мультимедийных IP-приложений должно быть доставлено из источника к нескольким получателям за короткое время, это можно рассматривать как потенциальный спам.

– Ограниченная интерактивность

Во многих случаях мультимедийный IP-спам обеспечивает только ограниченную интерактивность, поскольку спамеры имеют тенденцию отправлять спам, используя машины вместо людей, для того чтобы уменьшить стоимость рассылки спама. Например, в спаме мгновенной передачи сообщений или в спаме чата, отправители спама могут не отвечать, поскольку спам в сообщениях посылают машины рассылки спама. Спам в услугах VoIP, форма телемаркетинга, также могут обеспечить ограниченную интерактивность, когда они отправлены с использованием ARS. С учетом этого идентифицировать спам можно по результатам проверки того, обеспечивает ли отправитель мультимедийного IP-приложения интерактивность или нет. Наиболее общие методы противодействия спаму в системе электронной почты, основанные на данном методе, представляют собой тест Тьюринга и серые списки, которые проверяют интерактивность отправителя и МТА, соответственно.

6.2.2 Использование информации протокола для противодействия спаму

Для идентификации спама методом анализа характеристик более эффективно использовать информацию протокола, чем информацию о контенте. Протокольная составляющая мультимедийного IP-приложения может использоваться для идентификации спама посредством анализа источника мультимедийного IP-приложения. Идентификация спама с использованием информации протокола перед доставкой контента мультимедийных IP-приложений получателю требует меньше усилий, что является более эффективным по сравнению с другими методами противодействия спаму, в которых используется информация о контенте. Следующие положения подтверждают данный вывод:

– Предоставление информации о приложении

Протокольная составляющая мультимедийных IP-приложений несет информацию, связанную с предоставлением мультимедийных IP-приложений, например источник, пункт назначения, время доставки, используемый протокол доставки и т. д. Часть этих протокольных составляющих может быть использована для идентификации спама.

– Синхронизация анализа

Информация протокола для инициирования услуги доставляется до того, как доставляется контент мультимедийных IP-приложений. Например, в услуге VoIP процесс сигнализации, во время которого используется информация протокола, выполняется прежде, чем начинается сеанс вызова. Поэтому посредством анализа информации протокола существует возможность идентифицировать спам прежде, чем он будет доставлен получателю.

– Шифрование

Протокольные сообщения обычно доставляются без шифрования, хотя контент мультимедийных IP-приложений может быть зашифрован. Шифрование IP-пакетов делает анализ пакета очень трудным или неподдающимся дешифрованию. Поэтому анализ протокольной составляющей может быть проще по сравнению с анализом информационной составляющей мультимедийных IP-приложений.

– Тип среды передачи

Протокольная составляющая мультимедийных IP-приложений использует только один вид среды передачи; учитывая, что информационная составляющая иногда находится в форме мультимедийной информации, которая является трудной для анализа.

– Путь доставки

Начиная сеанс или обслуживание, протокольные сообщения транзитно проходят через оборудование сети, например сервер приложений для мгновенной передачи сообщений и прокси-серверы для связи через VoIP, которая может получить информацию о предоставлении мультимедийных IP-приложениях из протокольных сообщений. С другой стороны, сообщения с контентом могут быть доставлены от отправителя получателю напрямую, не осуществляя транзитного прохода через оборудование сети. В этом случае может оказаться трудно проанализировать контент мультимедийных IP-приложений.

6.3 Метод анализа контента

В методе анализа контента для идентификации спама используется результат анализа контента мультимедийных IP-приложений. Данный метод широко использовался, для того чтобы противодействовать спаму в электронной почте. Анализ контента мультимедийных IP-приложений может оказаться намного более трудным, чем в случае с электронной почтой, поскольку мультимедийные IP-приложения могут предоставляться в режиме реального времени и/или использовать мультимедийную информацию, в то время как электронная почта обычно основана на текстовой информации и предоставляется не в режиме реального времени. Для эффективного противодействия мультимедийному IP-спаму в методе анализа контента рассматриваются следующие положения:

– Продолжительность времени анализа контента

Контент мультимедийного IP-приложения необходимо проанализировать в течение приемлемого времени, для того чтобы пользователи этого приложения могли использовать его для идентификации спама. Для мультимедийных IP-приложений, предоставляемых в режиме реального времени, может оказаться невозможным выполнить анализ контента прежде, чем начнется доставка приложения.

– Точность анализа контента

Для эффективной идентификации спама точность анализа контента мультимедийных IP-приложений должна соответствовать определенному уровню качества. Будут полезны методы распознавания звука и изображения высокого качества, поскольку анализ контента мультимедийных приложений является очень трудным по сравнению с анализом текста.

– Шифрование контента

Анализ контента мультимедийных IP-приложений может оказаться очень трудным или не поддающимся расшифровке, когда IP-пакеты зашифрованы.

– Путь доставки контента

Контент мультимедийных IP-приложений считается проанализированным, когда он проходит через определенное оборудование сети, такое как сервер приложений или мультимедийный сервер с функцией анализа контента.

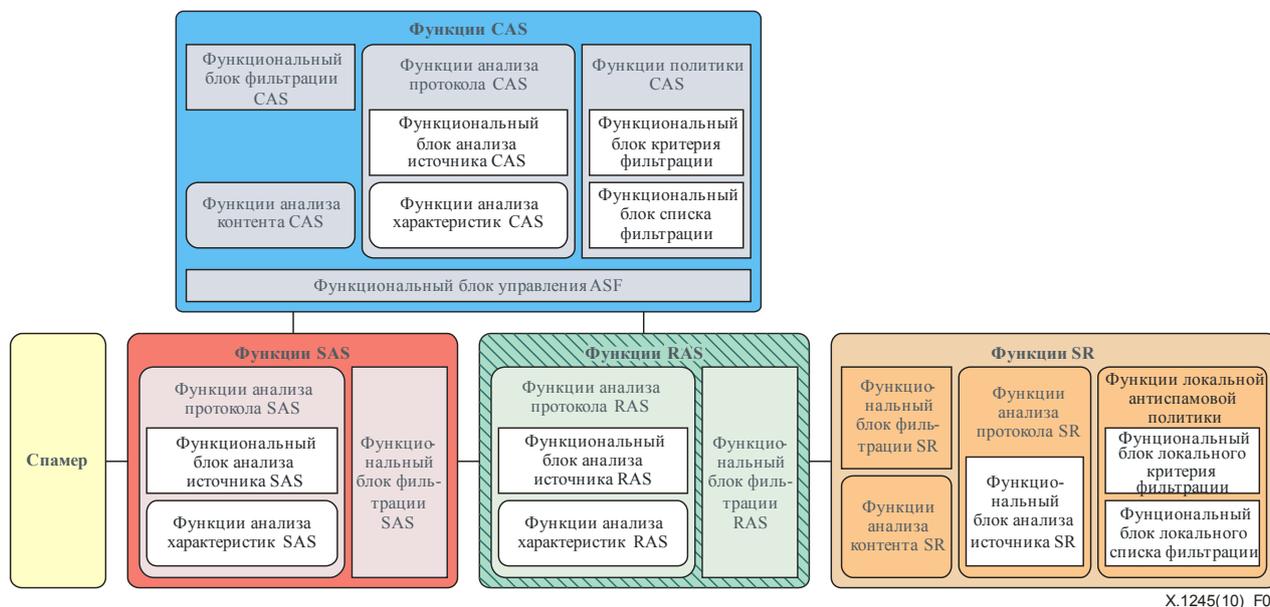
Во многих случаях мультимедийные IP-приложения могут не удовлетворять необходимым критериям. В случае мультимедийных IP-приложений, предоставляемых в режиме реального времени, таких как VoIP, пользователям услуг невозможно обнаружить и отфильтровать спам в пределах приемлемого времени посредством анализа контента, поскольку существует возможность проанализировать контент только после установления сеанса связи между вызывающим и вызываемым абонентами. С другой стороны, вероятно, хватит времени для анализа контента в случае мультимедийных IP-приложений, предоставляемых не в режиме реального времени, таких как записанные голосовые сообщения. Тем не менее метод анализа контента может быть сопряжен с трудностями в получении достаточной информации для идентификации спама в силу недостаточного развития используемых методов распознавания речи и изображения или недостаточного количества

контента. Когда контент мультимедийных IP-приложений, основанных на тексте, таких как услуги IM и услуги передачи текстовых сообщений, анализируется, также может быть трудно определить наличие спама, когда содержание зашифровано или доставлено напрямую между пользователями услуги, не проходя через надлежащее оборудование сети для осуществления анализа контента.

7 Структура противодействия мультимедийному IP-спаму

Для того чтобы противодействовать мультимедийному IP-спаму, объекты IP-сети с функциями противодействия спаму должны взаимодействовать друг с другом. В данном разделе описаны функции и взаимодействия объектов противодействия спаму, необходимых для реализации методов противодействия спаму. Может быть недостаточно эффективным использовать приложение только одного метода противодействия спаму для противодействия мультимедийному IP-спаму. Поэтому, возможно, для более эффективной фильтрации спама, одновременно в IP-сети должны быть реализованы более одного метода противодействия спаму.

В данном разделе описывается структура противодействия мультимедийному IP-спаму. Она была разработана таким образом, что может быть легко расширена различными техническими средствами, для того чтобы противодействовать спаму в различных приложениях и сетях. Структура разработана для защиты пользователей и сетей от мультимедийного IP-спама. Спам может появиться в любом месте, поэтому механизмы обнаружения и фильтрации для различного вида спама должны быть предоставлены по всей сети.



X.1245(10)_F02

Рисунок 2 – Структура противодействия мультимедийному IP-спаму

Как показано на рисунке 2, структура противодействия мультимедийному IP-спаму состоит из пяти элементов. В следующих разделах описываются функции и интерфейсы каждого элемента.

7.1 Спамер

Спамер создает и распространяет спам по сети. Это – создатель спама. Функции противодействия спаму не реализуются в спамере.

7.2 Функции SAS

SASF (функции противодействия спаму на стороне отправителя) представляют группу функций противодействия спаму, роль которых состоит в идентификации и блокировке мультимедийного IP-спама, который исходит от спамера. SASF могут быть реализованы на сетевых элементах, таких как прокси-сервер, где запросы исходящей связи от спамеров отправляются в качестве последнего скачка. SASF взаимодействуют с CASF (базовыми функциями противодействия спаму) для реализации функций противодействия спаму в SASF. Несмотря на то что SASF могут играть менее активную роль, чем другие компоненты в реальной среде связи, они могут более эффективно заблокировать спам на стороне источника прежде, чем он распространится по сети.

SASF состоят из функций анализа протокола SAS и функционального блока фильтрации SAS, предназначенного для управления фильтрацией спама. В следующих разделах описываются различные методы противодействия мультимедийному IP-спаму, которые могут применяться функцией SASF.

7.2.1 Функциональный блок фильтрации SAS

Посредством анализа функций и антиспамовых правил функциональный блок фильтрации SAS определяет, является ли проанализированное мультимедийное IP-приложение спамом или нет. Поэтому он взаимодействует с CASF и другими блоками противодействия спаму или функциональными блоками в SASF.

7.2.2 Функции анализа протокола SAS

Функции анализа протокола SAS анализируют информацию протокола полученных мультимедийных IP-приложений. Они состоят из функционального блока анализа источника SAS и функций анализа характеристик SAS, которые анализируют информацию источника и характеристики полученных мультимедийных IP-приложений, соответственно.

і) Функциональный блок анализа источника SAS

На основании информации источника мультимедийных IP-приложений SASF могут отличить мультимедийный IP-спам от мультимедийных IP-приложений, не являющихся спамом. У SASF есть два аспекта, связанных с источником мультимедийных IP-приложений. Один аспект – это фильтрация источника с помощью антиспамовых правил, предоставленная с помощью CASF, а другой – аутентификация отправителя.

– Антиспамовые правила

SASF могут идентифицировать и отфильтровать спам, используя адрес источника пакета мультимедийных IP-данных. Фильтрация осуществляется не только с адресом источника, но также и с другой информацией протокола, которая доступна для SASF. На рисунке 3 представлены функции противодействия спаму и взаимодействия функций для противодействия мультимедийному IP-спаму посредством анализа источника в SASF.

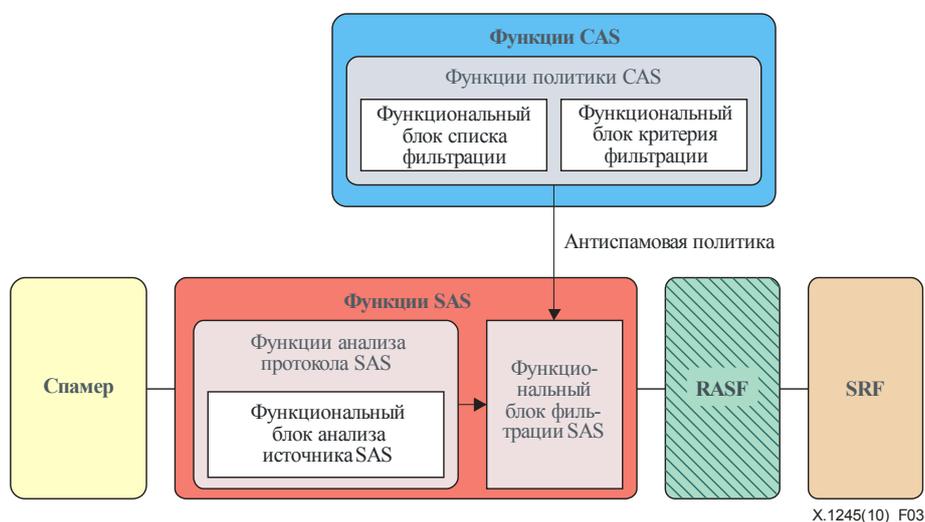


Рисунок 3 – Противодействие мультимедийному IP-спаму посредством анализа источника в SASF

Функциональный блок фильтрации SAS может получить антиспамовые правила от функций политики CAS. Функциональный блок фильтрации SAS отфильтровывает IP-пакет, посланный спамером, когда IP-пакет идентифицирован как спам на основе результата анализа.

– Аутентификация отправителя

SASF имеют информацию аутентификации отправителей, поэтому SASF могут предоставить аутентификацию пользователя для исходящего трафика. Когда требуется, SASF могут препятствовать тому, чтобы неавторизованные объекты использовали мультимедийные IP-приложения.

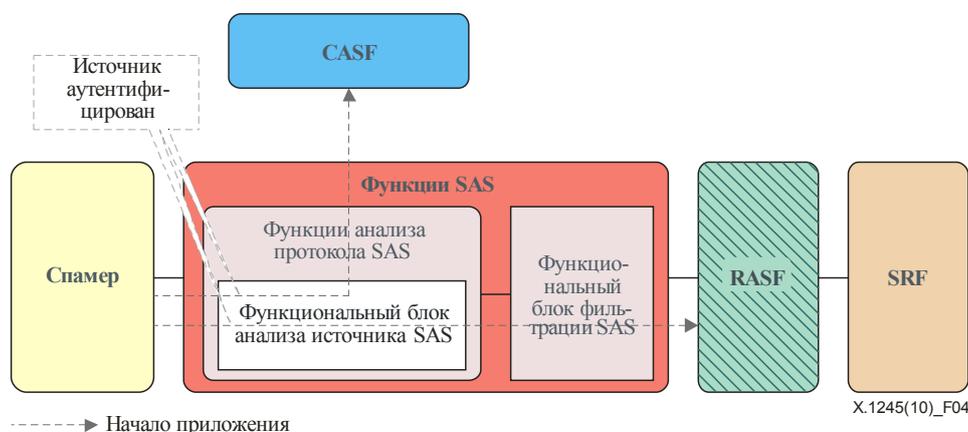


Рисунок 4 – Аутентификация источника, осуществляемая SASF

На рисунке 4 показана схема для аутентификации источника, осуществляемая SASF. В возможности анализа источника SASF входят функциональные возможности аутентификации, которые могут аутентифицировать трафик спамера прежде, чем начнется его отправка к CASF или RASF (функции противодействия спаму на стороне получателя). Если это необходимо, SASF могут сбросить трафик, не прошедший аутентификацию и отправить к другим ASF только аутентифицированный трафик. Сброс неавторизованного трафика может оказаться полезным, для того чтобы препятствовать спамерам, которые пытаются использовать маскировку (спуффинг).

– Процедура фильтрации

Процедура, в которой SASF отфильтровывают мультимедийный IP-спам посредством анализа источника следующая:

- 1) Доставка антиспамовых правил: SASF получают антиспамовые правила от CASF. Антиспамовые правила могут быть доставлены к SASF как уведомление или в виде запроса/ответа.
 - 2) Прием мультимедийных IP-приложений: SASF принимают инициацию мультимедийных IP-приложений.
 - 3) Аутентификация источника: SASF осуществляют аутентификацию источника приложений. Если процесс аутентификации терпит неудачу, SASF отклоняют запрос о начале передачи от спамера.
 - 4) Идентификация и фильтрация спама: SASF принимают решение относительно принятого мультимедийного IP-приложения на основании полученных от CASF антиспамовых правил и источника запроса. SASF могут уменьшить или проигнорировать трафик, который был определен как мультимедийный IP-спам.
- ii) Функции анализа характеристик SAS

SASF могут отличить спам, использующий такие характеристики приложений, как предоставление услуги в массовом порядке. SASF могут задействовать порог, который может использоваться для проверки массового порядка. Функции анализа характеристик SAS могут включать несколько функциональных блоков анализа конкретных характеристик. Функциональные возможности и интерфейс каждого функционального блока являются определенными техническими средствами для противодействия мультимедийному IP-спаму, но они не входят в сферу применения настоящей Рекомендации. В следующих списках представлены некоторые примеры характеристик, которые может отличить SASF, для того чтобы применить метод противодействия спаму.

– Массовый порядок

Функции анализа характеристик SAS имеют возможность проанализировать число запросов услуги из одного источника и проанализировать скорость запроса услуги. Функциональный блок фильтрации SAS идентифицирует мультимедийный IP-спам на основе результата анализа характеристик функций SAS и антиспамовых правил, полученных от функционального блока критерия фильтрации CAS.

– Ограниченная интерактивность

SASF могут иметь возможность проверить на спамере интерактивность услуги, хотя тест на интерактивность для источника мультимедийных IP-приложений обычно может производиться с помощью CASF. Для того чтобы начать предоставление мультимедийных IP-приложений, спамеры имеют тенденцию использовать машину, которая требует относительно меньших затрат, чем людские ресурсы. Поэтому проверка на интерактивность является одним из методов, для того чтобы отличить мультимедийный IP-спам.

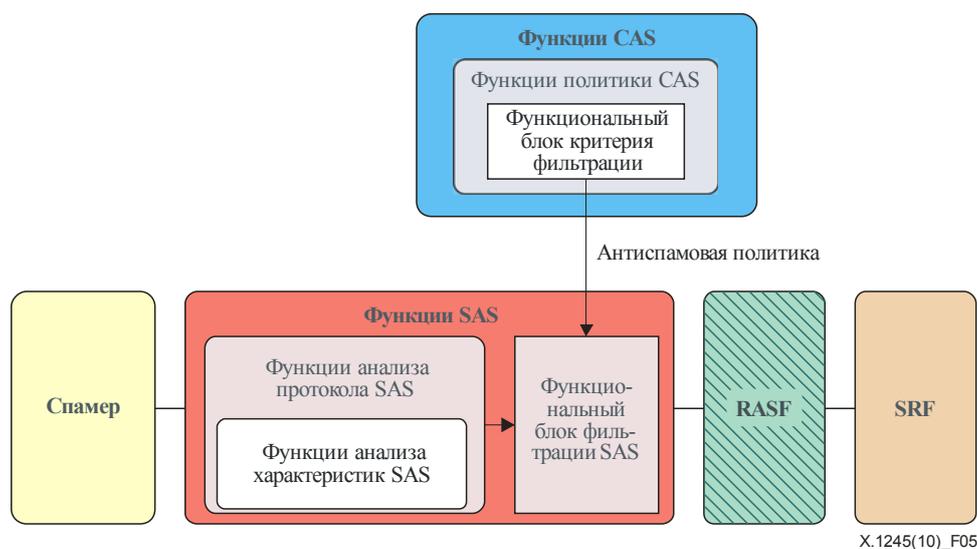


Рисунок 5 – Противодействие мультимедийному IP-спаму посредством анализа характеристик в SASF

Процедура, в которой SASF отфильтровывают мультимедийный IP-спам посредством анализа характеристик, следующая:

- 1) Доставка антиспамовых правил: функциональный блок фильтрации SASF получает от CASF антиспамовые правила, основанные на анализе характеристик. Антиспамовые правила могут быть доставлены к SASF как уведомление или в виде запроса/ответа.
- 2) Прием мультимедийных IP-приложений: SASF принимают инициацию мультимедийных IP-приложений.
- 3) Анализ характеристик: функции анализа характеристик SAS раскрывают связанные со спамом характеристики полученных мультимедийных IP-приложений.
- 4) Обработка результата: результат анализа характеристик отправляется от функций анализа характеристик SAS к функциональному блоку фильтрации SAS.
- 5) Фильтрация спама: функциональный блок фильтрации SAS обрабатывает спам согласно антиспамовым правилам. Если итоговый результат анализа определит спам, то SASF могут уменьшить или проигнорировать трафик, который определен как мультимедийный IP-спам.

Правила управления спамом в отношении мультимедийного IP-спама зависит от поставщиков услуг, пользователей услуг, мультимедийных IP-приложений, национальных нормативных положений и т. д. Таким образом, SASF и RASF должны взаимодействовать с CASF, для того чтобы получить информацию об антиспамовых правилах для противодействия спаму, основанному на характеристиках мультимедийных IP-приложений.

7.3 Функции RAS

RASF являются группой функций, роль которых состоит в том, чтобы идентифицировать и блокировать мультимедийный IP-спам, который должен быть доставлен получателю спама. RASF могут быть реализованы на сетевых элементах, таких как прокси-сервер, где запросы входящей связи к получателям спама отправляются в качестве последнего скачка. RASF взаимодействуют с CASF для осуществления функций противодействия спаму в RASF.

CASF и RASF могут быть реализованы в том же оборудовании сети, которое одновременно обслуживает и спамеров и получателей спама. Однако функции противодействия спаму, которые работают в оборудовании, различаются в соответствии с потоком трафика. Иными словами, функции противодействия спаму оборудования работают как SASF, когда трафик направлен от пользователей мультимедийных IP-приложений, которых обслуживает данное оборудование, и работает как RASF, когда трафик направлен к пользователям мультимедийных IP-приложений, которых обслуживает оборудование.

RASF состоят из функций анализа протокола RAS и функционального блока фильтрации RAS, предназначенного для управления фильтрацией спама.

Несмотря на то что у SASF или RASF существует техническая возможность, для того чтобы проанализировать контент доставленного трафика для противодействия спаму, они не охватываются функциями анализа контента в настоящей Рекомендации, поскольку это может потребовать применения к ним дополнительных ограничений на обработку. Когда мультимедийное IP-приложение по умолчанию через CASF не проходит, RASF могут доставить мультимедийное IP-приложение к CASF и передать CASF запрос проанализировать контент мультимедийного IP-приложения для идентификации спама.

В следующих разделах описываются различные методы по противодействию мультимедийному IP-спаму, которые могут быть приняты с помощью RASF.

7.3.1 Функциональный блок фильтрации RAS

На основе результата анализа и антиспамовых правил функциональный блок фильтрации RAS определяет, является ли проанализированное мультимедийное IP-приложение спамом или нет. Поэтому он взаимодействует с CASF и другими блоками противодействия спаму или функциональными блоками в RASF.

7.3.2 Функции анализа протокола RAS

Функции анализа протокола RAS анализируют информацию протокола полученных мультимедийных IP-приложений. Они состоят из функционального блока анализа источника RAS и функций анализа характеристик RAS, которые анализируют информацию источника и характеристики полученных мультимедийных IP-приложений, соответственно.

i) Функциональный блок анализа источника RAS

На основании информации источника мультимедийных IP-приложений, RASF могут отличить мультимедийный IP-спам от мультимедийных IP-приложений, не являющихся спамом. Для идентификации спама RASF квалифицирует антиспамовые правила относительно источника, предоставленным CASF, такие как черный список, белый список, оценка репутации и т. д. На рисунке 6 представлены функции противодействия спаму и их взаимодействие для противодействия мультимедийному IP-спаму с помощью анализа источника.

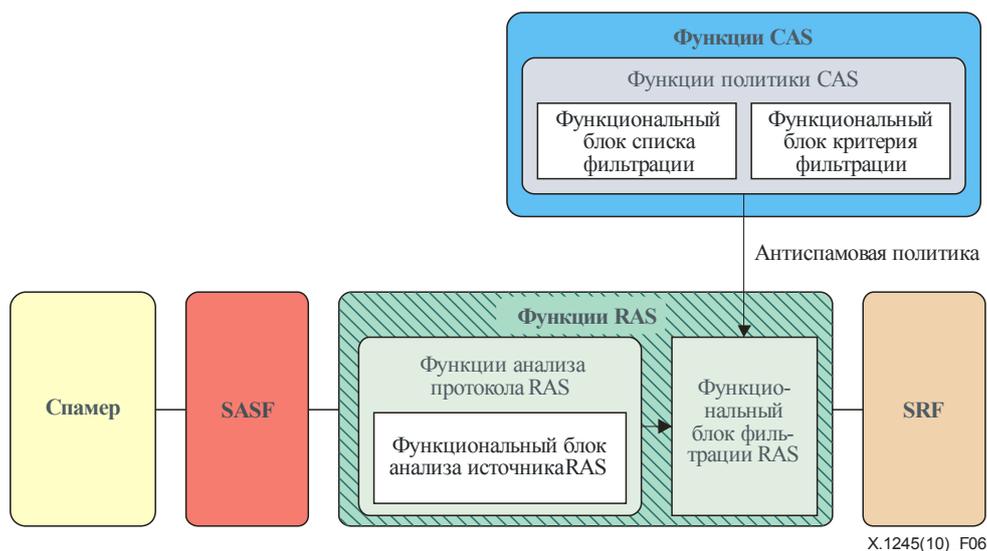


Рисунок 6 – Противодействие мультимедийному IP-спаму посредством анализа источника

На основании информации источника мультимедийного IP-приложения RASF определяет, является ли мультимедийное IP-приложение спамом или нет, а затем рассматривает его согласно результату. Поскольку для эффективности метода противодействия спаму, основанного на источнике, требуется высокая надежность информации источника, предполагается, что мультимедийное IP-приложение, которое RASF принимают от SASF, заслуживают доверия, т. е. проходит аутентификацию. RASF идентифицирует мультимедийный IP-спам согласно критерию фильтрации спама или списку фильтрации спама, предоставленному CASF. CASF поддерживает список фильтрации и критерий фильтрации в целях поддержки RASF, SASF или самой CASF в отношении идентификации спама. Следующие действия описывают процесс идентификации и фильтрации RASF, использующие метод анализа источника:

- 1) Доставка антиспамовых правил от CASF: RASF получают антиспамовые правила от CASF. Антиспамовые правила могут быть доставлены к RASF как уведомление или в виде запроса/ответа.
- 2) Прием мультимедийных IP-приложений: RASF принимают мультимедийное IP-приложение и проверяют источник мультимедийного IP-приложения.
- 3) Идентификация и фильтрация спама: RASF принимают решение относительно принятого мультимедийного IP-приложения на основании информации источника и правил антиспамового управления, полученных на предыдущем этапе. RASF могут уменьшить или проигнорировать трафик, который был определен как мультимедийный IP-спам в соответствии с правилами противодействия спаму поставщика услуги или услуги.

Когда RASF определяют спам на основе белого списка, может использоваться список фильтрации, полученный от CASF. Когда RASF определяют спам на основе оценки репутации, критерием фильтрации может выступать порог оценки репутации, по которому мультимедийное IP-приложение определяется как спам.

ii) **Функции анализа характеристик RAS**

RASF может идентифицировать спам, используя мультимедийное IP-приложение для определения того, имеет ли спам характеристики мультимедийного IP-спама. Функции анализа характеристик RAS могут включать несколько определенных функциональных блоков анализов характеристик. Технические средства для противодействия мультимедийному IP-спаму не входят в сферу применения настоящей Рекомендации.

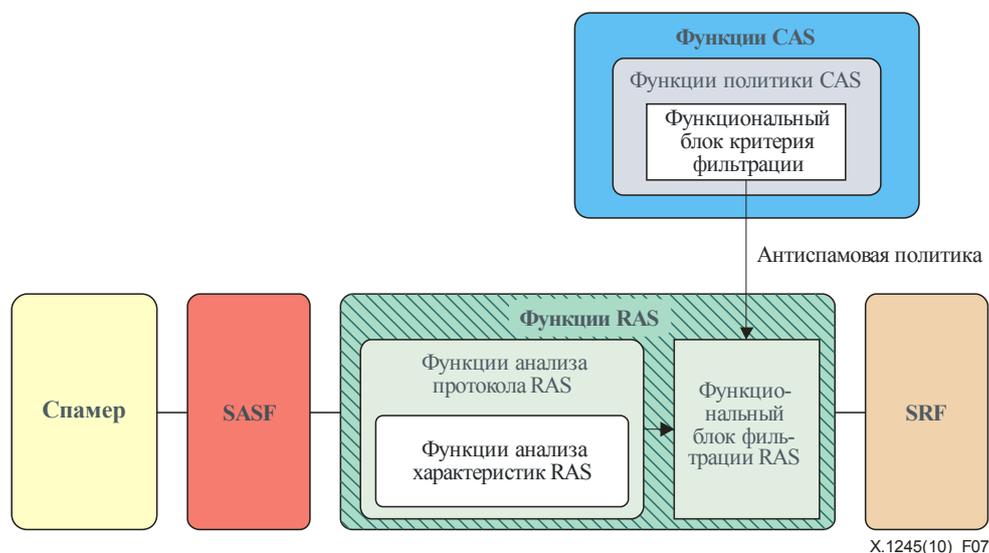


Рисунок 7 – Противодействие мультимедийному IP-спаму посредством анализа характеристик

На рисунке 7 представлены функции противодействия спаму и их взаимодействие для противодействия мультимедийному IP-спаму посредством анализа характеристик в RASF. Процедура, в которой RASF отфильтровывают мультимедийный IP-спам посредством анализа характеристик следующая:

- 1) Доставка антиспамовых правил: функциональный блок фильтрации RASF получает от CASF антиспамовые правила, основанные на анализе характеристик. Антиспамовые правила могут быть доставлены к RASF как уведомление или в виде запроса/ответа.
- 2) Прием мультимедийных IP-приложений: RASF принимают сигнал об иницировании мультимедийных IP-приложений.
- 3) Анализ характеристик: функции анализа характеристик RAS раскрывают связанные со спамом характеристики полученных мультимедийных IP-приложений.
- 4) Функции анализа характеристик RAS предоставляют результат анализа функциональному блоку фильтрации RAS.
- 5) Фильтрация спама: функциональный блок фильтрации RAS обрабатывает спам согласно антиспамовым правилам. Если итоговый результат анализа определит спам, то RASF могут уменьшить или проигнорировать трафик, который определен как мультимедийный IP-спам.

7.4 Функции CAS

У CASF существует возможность управлять правилами противодействия спаму и контролировать RASF и SASF. Также у них есть возможность проанализировать источник или характеристики мультимедийных IP-приложений, для того чтобы идентифицировать и отфильтровать спам, когда существует маршрут IP-пакетов между спамерами и получателями спама для предоставления мультимедийных IP-приложений согласно типу мультимедийных IP-приложений. CASF имеют функции анализа протокола CAS, функции анализа контента CAS, функциональный блок фильтрации CAS, функции антиспамовых правил CAS и функциональный блок управления ASF. В данном разделе описаны функциональные возможности и взаимодействие каждого объекта в CASF, для того чтобы противодействовать мультимедийному IP-спаму.

7.4.1 Функциональный блок фильтрации CAS

На основе результата анализа и антиспамовых правил функциональный блок фильтрации CAS определяет, является ли проанализированное мультимедийное IP-приложение спамом или нет. Поэтому он взаимодействует с другими функциями противодействия спаму или функциональными блоками в CASF.

7.4.2 Функции анализа протокола CAS

Функции анализа протокола CAS анализируют информацию протокола полученных мультимедийных IP-приложений. Они состоят из функционального блока анализа источника CAS и функций анализа характеристик CAS, которые анализируют информацию источника и характеристики полученных мультимедийных IP-приложений, соответственно.

i) Функциональный блок анализа источника CAS

Когда мультимедийное IP-приложение предоставлено под управлением компонента сети, в котором размещена CASF, например регистрация пользователя для получения услуги мгновенной передачи сообщений или услуги VoIP под управлением серверов приложений, CASF может являться возможным функциональным объектом для идентификации спама посредством анализа источника. На рисунке 8 представлены функции противодействия спаму и их взаимодействие для противодействия мультимедийному IP-спаму посредством анализа источника в CASF.

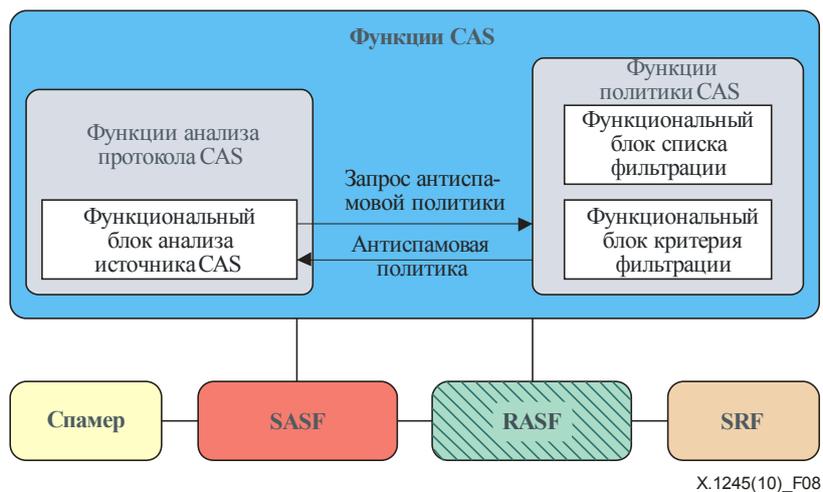


Рисунок 8 – Противодействие мультимедийному IP-спаму посредством анализа источника

Следующие действия описывают возможную процедуру противодействия мультимедийному IP-спаму в CASF на основе информации источника мультимедийного IP-приложения:

- 1) Аутентификация: пользователь желает использовать мультимедийное IP-приложение, например услугу мгновенной передачи сообщений, и поэтому проходит аутентификацию с помощью компоненты сети, такой как сервер приложений, который имеет CASF.
- 2) Прием мультимедийных IP-приложений: пользователь отправляет запрос CASF на доставку IP-сообщения и функциональный блок анализа источника CAS проверяет источник пользователя.
- 3) Получение антиспамовых правил: функциональный блок анализа источника CAS запрашивает антиспамовые правила и получает их от функций правил CAS.
- 4) Идентификация и фильтрация спама: CASF принимает решение, является ли спамом данное мультимедийное IP-приложение, на основании информации источника и антиспамовых правил, полученных на предыдущих этапах. CASF может уменьшить или проигнорировать трафик, который был определен как мультимедийный IP-спам, и далее он обрабатывается согласно антиспамовым правилам поставщика услуг или пользователя услуги, если идентифицирован как спам.

ii) Функции анализа характеристик CAS

CASF могут быть пунктом анализа характеристик для целей противодействия спаму, когда мультимедийного IP-приложения предоставлено под управлением объекта сети CASF. CASF анализируют мультимедийное IP-приложение, для того чтобы определить, имеет ли оно характеристики спама, и использует при этом критерии фильтрации в антиспамовых правилах, для того чтобы определить, спам это или нет. На рисунке 9 показаны полная архитектура и интерфейсы в методе анализа характеристик для противодействия мультимедийному IP-спаму по CASF.

Функции политики CASF имеют функциональный блок критерия фильтрации, который состоит из критериев фильтрации спама, требуемых для идентификации мультимедийного IP-спама и предоставляющих критерии SASF или RASF, для того чтобы поддержать их идентификацию спама. Например, когда функции анализа характеристик CAS пытаются идентифицировать спам, если мультимедийное IP-приложение имеет массовый порядок, функциональный блок критерия фильтрации CASF может предоставить критерий количества, который идентифицирует уровень количества мультимедийного IP-приложения и определяет его как мультимедийный IP-спам.

На рисунке 9 представлены функции противодействия спаму и их взаимодействие для противодействия мультимедийному IP-спаму посредством анализа характеристик в CASF.

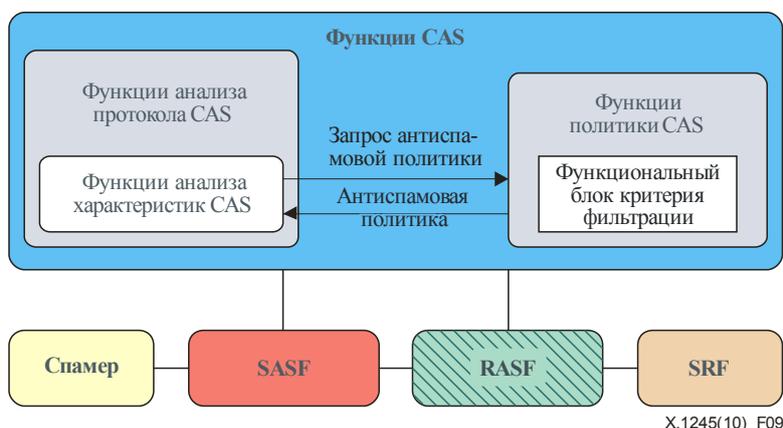


Рисунок 9 – Противодействие мультимедийному IP-спаму посредством анализа характеристик

Следующие действия описывают процедуру анализа характеристик для противодействия мультимедийному IP-спаму с помощью CASF:

- 1) Анализ характеристик спама: если мультимедийное IP-приложение пытается подключиться под управлением объекта сети, принадлежащего CASF, то CASF анализирует, имеет ли оно характеристики спама, например массовость, ограниченную интерактивностью и т. д.
- 2) Получение антиспамовых правил: функции анализа характеристик запрашивают функции политики CAS для антиспамовых правил, связанных с анализом характеристик для фильтрации спама. Антиспамовые правила блокируют отправку запрошенной информации для функций анализа характеристик CAS.
- 3) Идентификация и фильтрация спама: на основании результата анализа характеристик и принятых антиспамовых правил функции CAS принимают решение относительно того, является ли мультимедийное IP-приложение спамом или нет.

7.4.3 Функции анализа контента CAS

CASF имеют функции анализа контента CAS, которые анализируют контент мультимедийного IP-приложения для идентификации спама, когда мультимедийное IP-приложение доставлено получателю через оборудование сети, где прописаны CASF, такие как сервер приложений или мультимедийный сервер.

Любые CASF, SASF или RASF могут быть анализаторами с точки зрения спама, т. к. они осуществляют идентификацию, использующую информацию протокола мультимедийных IP-приложений, например информацию источника или характеристики спама. Однако с точки зрения идентификации спама с использованием анализа контента, CASF, через который проходит контент мультимедийных IP-приложений, является рациональным пунктом для анализа контента, когда для противодействия мультимедийному IP-спаму используются методы противодействия спаму, основанные на контенте.

На рисунке 10 представлены функции противодействия спаму и их взаимодействие для противодействия мультимедийному IP-спаму посредством анализа контента в CASF.

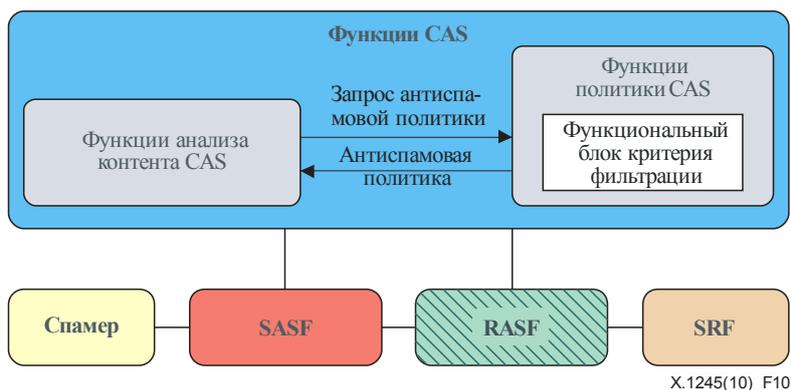


Рисунок 10 – Противодействие мультимедийному IP-спаму посредством анализа контента

Следующие действия описывают процедуру анализа контента для противодействия мультимедийному IP-спаму с помощью CASF:

- 1) Прием мультимедийных IP-приложений: контент мультимедийных IP-приложений доставляется на CASF.
- 2) Анализ контента: функции анализа CAS анализируют контент IP-приложения.
- 3) Получение антиспамовых правил: CASF запрашивает функции правил CAS для получения антиспамовых правил и приема правил от функционального блока критерия фильтрации.
- 4) Идентификация и фильтрация спама: на основании результата анализа функции и антиспамовых правил CASF принимают решение относительно того, является ли мультимедийное IP-приложение спамом или нет.

Как описано в разделе 6, возможности метода анализа контента могут быть ограничены в соответствии с характеристиками мультимедийного IP-приложения, например предоставляется ли мультимедийное IP-приложение в режиме реального времени или нет, является ли оно мультимедийным или нет, зашифрован ли контент мультимедийного IP-приложения или нет.

7.4.4 Функции правил CAS

Функции правил CAS поддерживают антиспамовые правила для противодействия мультимедийному IP-спаму и состоит из функционального блока критериев фильтрации и функционального блока списка фильтрации.

i) Функциональный блок критерия фильтрации

Функциональный блок критерия фильтра поддерживает критерий антиспамовой фильтрации для идентификации мультимедийного IP-спама. Могут существовать различные виды критериев фильтрации в соответствии с используемыми методами противодействия спаму. Например, анализ массового порядка, пороговое количество мультимедийных IP-приложений, которые отправляются в одно и то же время из одного источника, могут оказаться критерием фильтрации. Механизмы создания критериев фильтрации и управления ими не входят в сферу применения настоящей Рекомендации.

ii) Функциональный блок списка фильтрации

Функциональный блок списка фильтрации управляет списком фильтрации для идентификации мультимедийного IP-спама посредством анализа источника. Могут существовать различные виды списков антиспамовой фильтрации в соответствии с используемыми методами противодействия спаму. Например, черный список, белый список и оценка репутации могут использоваться как список фильтрации. Список фильтрации может быть либо общедоступным списком для многих пользователей идентичных услуг, личным списком, которым управляют лично, или сочетанием этих типов. Механизмы создания и управления списком фильтрации не входят в сферу применения настоящей Рекомендации.

7.4.5 Функциональный блок управления ASF

Функциональный блок управления ASF взаимодействует с SASF и RASF, для того чтобы поддержать их для идентификации и фильтрации спама. Он доставляет от CAS антиспамовые правила для RASF и SASF.

7.5 Функции SR

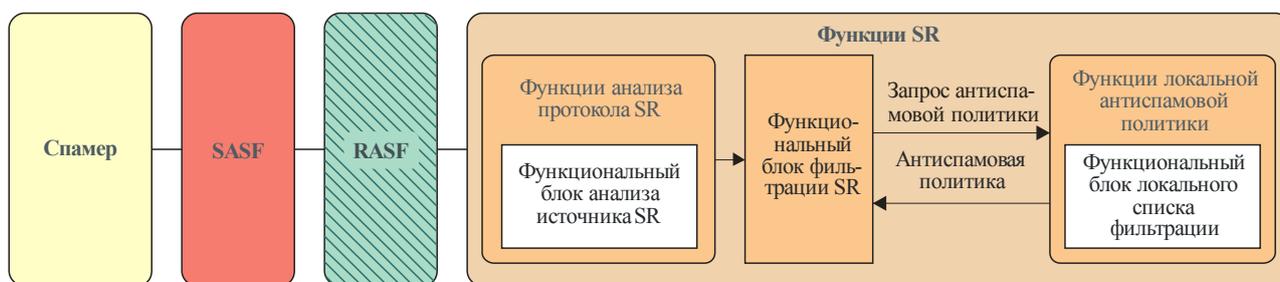
Получатель спама является конечным пунктом для мультимедийного IP-спама. Если нет механизма противодействия спаму, то мультимедийный IP-спам может воздействовать на пользователей и наносить им ущерб.

Получатель спама имеет функции SR (получателя спама), необходимые для того, чтобы защитить себя от мультимедийного IP-спама. Пользователи могут установить антиспамовые правила или получить их от поставщиков услуг, для того чтобы отфильтровать мультимедийный IP-спам. Функции SR состоят из функций анализа протокола SR, функций анализа контента SR, функционального блока фильтрации SR и функций локальных антиспамовых правил. В данном разделе описываются функциональные возможности и взаимодействия каждой функции противодействия спаму, которая может быть принята получателем спама, для того чтобы противодействовать спаму.

7.5.1 Функции анализа протокола SR

Функции анализа протокола SR имеют функциональный блок анализа источника SR, который идентифицирует спам на основе информации отправителя. Несмотря на то что существует возможность отфильтровать спам на CASF, SASF и RASF, в случае непосредственного соединения с мультимедийными IP-приложениями для противодействия мультимедийному IP-спаму могут использоваться функции противодействия спаму и антиспамовые правила SRF.

Получатель спама может определить локальный список фильтрации и локальный критерий или получить список от другой функции противодействия спаму, такой как CASF. Конкретные механизмы для определения антиспамовых правил не входят в сферу настоящей Рекомендации. На рисунке 11 представлены функции противодействия спаму и их взаимодействия для противодействия мультимедийному IP-спаму посредством анализа источника в SRF.



X.1245(10)_F11

Рисунок 11 – Противодействие мультимедийному IP-спаму посредством анализа источника в функциях получателя спама

Следующие действия описывают возможную процедуру противодействия мультимедийному IP-спаму на основе информации источника мультимедийных IP-приложений получателя спама:

- 1) Прием мультимедийных IP-приложений: SRF принимают инициацию мультимедийных IP-приложений и проверяют источник IP-приложений.
- 2) Получение антиспамовых правил: функции анализа протокола SR запрашивают антиспамовые правила и принимают ее от локальных функций антиспамовых правил.
- 3) Идентификация и фильтрация спама: функциональный блок фильтрации SR принимает решение относительно принятого мультимедийного IP-приложения на основе антиспамовых правил и результата анализа источника. Получатель спама может уменьшить или проигнорировать трафик, который был определен как мультимедийный IP-спам.

Функции получателя спама обладают технической возможностью идентификации спама посредством анализа характеристик. Однако функции анализа протокола SR не имеют функционального блока анализа характеристик, так как существует риск зависимости от получателя спама при выполнении сложных функций противодействия спаму, таких как используемые в рамках метода анализа характеристик, поскольку функции анализа протокола SR находятся под управлением весьма изменчивой группы пользователей.

7.5.2 Функции анализа контента SR

Для получателя спама существует возможность противодействовать спаму посредством анализа контента. Получатель спама может поддерживать собственный механизм анализа контента, который является определенным для пользователя или получить механизм от поставщиков услуг. Антиспамовая политика относительно анализа контента находится в локальных функциях антиспамовых правил как часть функционального блока локальных критериев фильтрации. На рисунке 12 представлены функции противодействия спаму и их взаимодействия для противодействия мультимедийному IP-спаму посредством анализа контента в SRF.

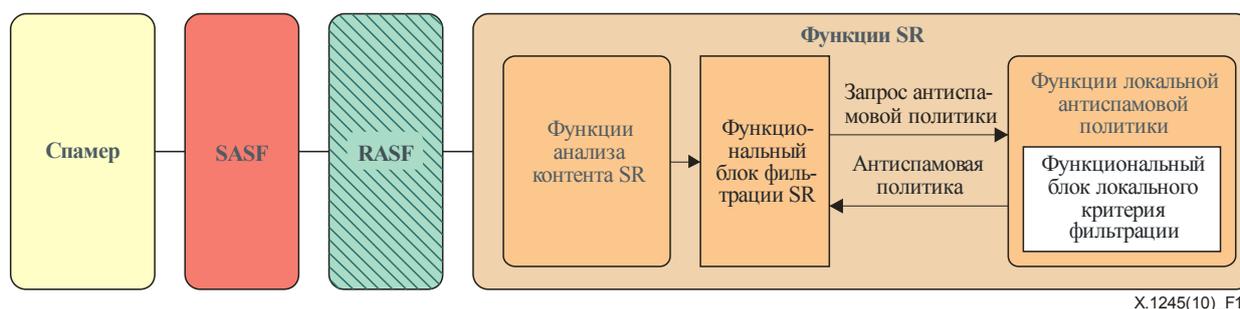


Рисунок 12 – Противодействие мультимедийному IP-спаму посредством анализа контента в функциях получателя спама

Процедура, в которой получатели спама осуществляют фильтрацию мультимедийного IP-спама посредством анализа контента, имеет следующий вид:

- 1) Прием мультимедийных IP-приложений: SRF принимают инициацию мультимедийных IP-приложений. Функции анализа контента SR осуществляют анализ контента для идентификации спама.
- 2) Получение антиспамовых правил: результат анализа контента отправляется к функциональному блоку фильтрации SR. Функциональный блок фильтрации SR запрашивает и принимает антиспамовые правила от локальных функций антиспамовых правил.
- 3) Идентификация и фильтрация спама: функциональный блок фильтрации SR принимает решение относительно принятого мультимедийного IP-приложения на основе антиспамовых правил и результата анализа контента. Получатель спама может уменьшить или проигнорировать трафик, который был определен как мультимедийный IP-спам.

7.5.3 Функциональный блок фильтрации SR

На основе результата анализа и антиспамовых правил, функциональный блок фильтрации SR определяет, является ли проанализированное мультимедийное IP-приложение спамом или нет. Поэтому он взаимодействует с другими функциями или функциональными блоками противодействия спаму в SRF.

7.5.4 Локальные функции антиспамовых правил

Локальные функции антиспамовых правил поддерживают определенные для пользователя антиспамовые правила для противодействия мультимедийному IP-спаму. Функции содержат функциональный блок локального критерия фильтрации и функциональный блок локального списка фильтрации.

- i) Функциональный блок локального критерия фильтрации

Функциональный блок локального критерия фильтрации поддерживают определенный для пользователя критерий антиспамовой фильтрации для идентификации мультимедийного IP-спама. Типы критериев фильтрации зависят от функций противодействия спаму, которые поддерживает SRF.

ii) Функциональный блок локального списка фильтрации

Функциональный блок локального списка фильтрации управляет определяемым пользователем списком фильтрации для идентификации мультимедийного IP-спама посредством анализа источника. Типы списков зависят от функциональных возможностей анализа источника, которые поддерживает SRF.

7.6 Основные точки в структуре

В данном разделе определены основные точки между различными элементами в структуре. На рисунке 13 определены основные точки в структуре.

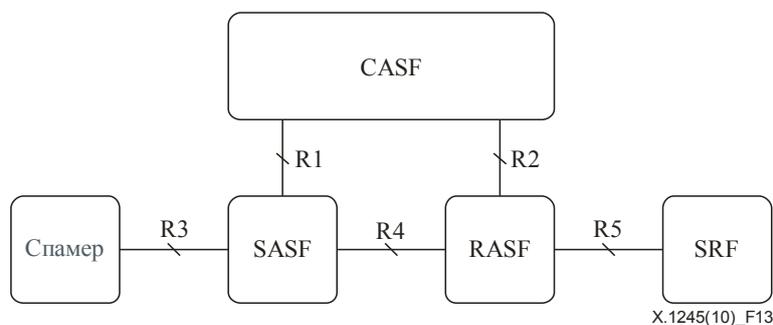


Рисунок 13 – Основные точки в структуре противодействия спаму

7.6.1 Основная точка R1

R1 находится между CASF и SASF, используется для получения правил фильтрации от CASF к SASF. CASF управляют SASF через R1.

7.6.2 Основная точка R2

R2 находится между CASF и RASF, используется для получения правил фильтрации от CASF к RASF. CASF управляют RASF через R2.

7.6.3 Основная точка R3

R3 находится между спамером и SASF, используется в протоколе мультимедийного IP-приложения и/или передаваемом трафике данных.

7.6.4 Основная точка R4

R4 находится между SASF и RASF, используется в протоколе мультимедийного IP-приложения и/или передаваемом трафике данных.

7.6.5 Основная точка R5

R5 находится между RASF и получателем спама, используется в протоколе мультимедийного IP-приложения и/или передаваемом трафике данных.

Дополнение I

Противодействие спаму путем усложнения процесса распространения спама

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Усложнение процесса распространения спама может использоваться в качестве одного из технических методов противодействия мультимедийному IP-спаму. Однако это несколько отличается от других методов, предусматривающих непосредственную идентификацию и фильтрацию спама. Затрудняя распространение спама, возможно косвенно снизить его объем, но этот метод требует усилий, времени и является дорогостоящим. Одним из путей снижения объема мультимедийного IP-спама может стать создание барьеров для спамеров путем увеличения финансовых и трудовых затрат, необходимых для создания и доставки спама. Затраты спамеров на распространение спама определяются величиной сборов за регулирование, включая ожидаемые штрафы за незаконный спам, сборы за использование мультимедийных IP-приложений, выплачиваемые поставщику услуг или поставщику сети, расходы на доставку спама, например тест на интерактивность и т. д. Приведенные далее методы могут применяться в целях усложнения процесса распространения спама:

- Усложнять доступ к IP-адресам: увеличение числа попыток, необходимых для сбора информации о пунктах назначения спама, например IP-адресов и учетных записей прикладных мультимедийных IP-услуг, и усложнение отправки спамерами мультимедийного IP-спама.
- Система платежей: выставление счетов за мультимедийный IP-спам может быть полезно для снижения количества спама. Тем не менее принятие системы платежей за возможный спам, например IP-сообщений в массовом порядке, не является техническим вопросом.
- Предотвращение рассылок в массовом порядке: учитывая, что спам рассылается в массовом порядке во многих случаях, предотвращение рассылок в массовом порядке может помочь снизить количество спама.
- Тест на интерактивность: тест на интерактивность, применяемый к спамерам, может увеличить их затраты на распространение спама. Однако он может иметь побочный эффект, создавая помехи обычным пользователям мультимедийных IP-приложений.

Методы противодействия спаму посредством усложнения процесса распространения спама не ограничиваются приведенными выше примерами.

В тесте на интерактивность CASF может выполнять функции испытателя. В методе предотвращения рассылок в массовом порядке CASF, SASF или RASF могут определять массовость, т. е. определенный уровень количества, и блокировать мультимедийные IP-приложения, характеризующиеся массовостью. Взимание платы за массовые сообщения или контроль над сообщениями со стороны CASF также является возможным методом усложнения процесса распространения спама.

SASF или RASF иногда могут анализировать протокольную информацию, но обычно они не предпринимают дополнительных действий, направленных на усложнение процесса распространения спама, например предотвращение массовой рассылки, управление платежами или тест на интерактивность. Говоря кратко, ожидается, что SASF или RASF предпримут некоторые действия для поддержки CASF в противодействии спаму, а CASF возьмет на себя основные обязанности по усложнению процесса распространения спама.

Дополнение II

Аспекты безопасности и практические аспекты использования структуры

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

II.1 Аспекты безопасности

Далее приведены аспекты безопасности применительно к противодействию мультимедийному IP-спаму.

– Аутентификация

Аутентификация является процессом, в котором объект – получатель спама или CASE – подтверждает свою идентичность, представляя регистрационные данные, которые трудно создать кому-либо, кроме реального пользователя.

Необходимо проводить аутентификацию пользователя для идентификации отправителя сообщения мультимедийных IP-приложений, которое поможет блокировать множество спамерских атак типа спуффинга. Невыполнение надлежащей аутентификации пользователя сделает невозможным отслеживание спамеров, так как спамеры могут подделывать свои IP-адреса при помощи атак спуффинга.

Аутентификацию можно провести разными способами. Некоторые методы аутентификации, например простая аутентификация с помощью пароля, легко реализовать, но в целом они слабы и примитивны. Другие методы аутентификации, например уровень безопасных соединений (SSL), IPSec, протокол безопасной оболочки, Kerberos, которые могут быть более сложными и требовать больше времени для реализации и поддержки, обеспечивают строгую и надежную аутентификацию.

Другие развивающиеся технологии, например методы криптографической подписи, могут быть еще лучшим решением. Однако наиболее широко распространенным и в настоящее время доступным методом аутентификации пользователя по-прежнему остаются классическая структура правил отправителя (SPF) и доменные ключи.

– Управление доступом

Управление доступом является способом внедрения и обязательного применения правил авторизации. Управление доступом выдает пользователю разрешение на осуществление или запрещает ему осуществление действия в отношении получателя спама и ASF, как указывается в политике безопасности.

Управление доступом обычно применяется после проведения аутентификации. В целом управление доступом делится на избирательное управление доступом (DAC) и неизбирательное управление доступом (NDAC). В DAC владелец объекта определяет, кто имеет доступ к объекту или определяет правила. Все правила управления доступом, отличающиеся от DAC, считаются NDAC. В NDAC правилами являются инструкции, которые не определены по усмотрению пользователя. примерами NDAC являются: обязательное управление доступом (MAC), управление доступом на ролевой основе (RBAC), управление доступом на целевой основе (PBAC), управление доступом на основе истории (NBAC), временные ограничения в управлении доступом (TCAC) и управление доступом на основе правил (RuBAC).

– Конфиденциальность

Конфиденциальность относится к механизмам, гарантирующим, что только авторизованный пользователь может получить доступ к безопасной связи. Существует два основных механизма обеспечения конфиденциальности информации, передаваемой электронным способом: шифрование или передача по инфраструктуре безопасности, например через виртуальную частную сеть (VPN) или другой зашифрованный канал связи.

IPSec является протоколом, используемым в большинстве VPN для установления безопасной связи через интернет. IPSec является широко распространенным стандартом для безопасной передачи, и он характеризуется гибкостью и меньшими затратами по сравнению с рядом других методов шифрования. IPSec обеспечивает надежное шифрование, целостность и аутентификацию, он особенно целесообразен для организаций, которым необходимо обеспечивать безопасную передачу данных через интернет.

Протокол туннелирования уровня 2 (L2TP) является протоколом туннелирования, используемым для поддержки VPN. Он инкапсулирует протокол данного уровня сети в протокол передачи из пункта в пункт (PPP) для криптографической защиты фреймов PPP и инкапсулирования данных внутри протокола туннелирования.

– Целостность данных

Целостность означает, что информация не изменена в процессе перемещения между получателем спама и спамером. Без соответствующей защиты спамеры могут изменять или перемешивать контент мультимедийных IP-сообщений.

Используя представление сообщений в краткой форме, созданное криптографической хеш-функцией, системный администратор может обнаруживать несанкционированные изменения в сообщениях. Хеш-функции также можно объединить с другими стандартными криптографическими методами для проверки источника данных. Когда алгоритмы хеширования объединены с алгоритмами шифрования, они создают особое представление сообщений в краткой форме, определяющее источник данных.

Если для поддержки целостности данных применяются цифровые подписи, для управления ключами шифрования может потребоваться инфраструктура с открытым ключом (PKI). PKI отслеживает присвоение и отзыв у пользователей и организаций открытых ключей шифрования.

В качестве альтернативы цифровой подписи и PKI для обеспечения целостности данных может использоваться секретное шифрование. Применение секретного ключа проще тем, что и для шифрования, и для дешифрования используется только один ключ, он должен находиться у как у отправителя, так и у получателя. Системы секретных ключей широко используются, но им присущи сложности, вызванные проблемой безопасного распространения секретных ключей.

– Предотвращение отказа от авторства

Предотвращение отказа от авторства – метод, делающий невозможным отказ отправителя сообщения или инициатора передачи от факта осуществления передачи.

Предотвращение отказа от авторства реализуется посредством обязывающих правовых документов и обязательности следующих механизмов обеспечения безопасности и надежных процессов управления сервером: SSL, жетон OTP запроса-отклика, безопасное хеширование и журналы аудита.

Стандартной практикой реализации предотвращения отказа от авторства является использование преимуществ цифровых подписей, которые могут рассматриваться как одна из лучших альтернатив замены традиционных подписей в обработке электронных данных. Для того чтобы ввести цифровые подписи, должны быть доступны доверенная третья сторона (ТТР) или PKI. ТТР или PKI могут поддерживать как минимум орган сертификации (CA) при выдаче списков цифровых сертификатов и отзыва сертификатов (CRL) для проверки отозванных сертификатов.

II.2 Практические аспекты

Одной из главных задач структуры является обеспечение максимально возможного уменьшения негативного воздействия на коммерческую деятельность. Должно быть очевидным, что выполнение мер по противодействию спаму приведет к положительным результатам для частных и юридических лиц, которые соблюдают требования компании.

Приведенные ниже практические аспекты относятся к действиям по обработке. Они предназначены в качестве руководящих указаний по реализации системы противодействия спаму и для предоставления возможным поставщикам информации высокого уровня:

- обеспечивать высокую точность и хорошую производительность;
- иметь возможность развертывания по периметру интернета;
- осуществлять интеграцию с популярными системами мультимедийных IP-приложений;
- осуществлять запуск на платформе сервера пользователя, по выбору: UNIX, Windows и т. п.;
- обеспечивать фильтрацию как входящего, так и исходящего мультимедийного IP-спама;
- обеспечивать гибкость для соответствия правилам и предпочтениям организации;
- обеспечивать пользователю возможность создания отдельных или специальных фильтров;
- разрешить пользователям управление их собственными папками спама в мультимедийных IP-приложениях и установление простых предпочтений;

- обеспечивать возможность управления функциональными возможностями черных и белых списков;
- обеспечивать возможность фильтрации контента, включая возможность добавления фильтрации контента на стороне сервера с классами административного управления тарифами на уровне пользователя.

Библиография

- [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.*

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия А	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	Качество телефонной передачи, телефонные установки, сети местных линий
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