Международный союз электросвязи

МСЭ-Т

X.1247

(03/2016)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

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

Безопасность киберпространства – Противодействие спаму

Техническая основа противодействия спаму при передаче сообщений на мобильные устройства

Рекомендация МСЭ-Т X.1247

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	**X.1230–X.1249**
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1339
Рекомендации, связанные с PKI	X.1340–X.1349
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.1247

Техническая основа противодействия спаму при передаче сообщений на мобильные устройства

Резюме

Одновременно с быстрым развитием услуг по передаче сообщений на мобильные устройства, происходит стремительный рост передачи спама на мобильные устройства. К сожалению, не существует какой-либо одной меры, обеспечивающей идеальное средство борьбы со спамом при передаче сообщений на мобильные устройства. Вследствие этого необходимо создать практическую основу для противодействия спаму при передаче сообщений на мобильные устройства. В Рекомендации МСЭ-Т X.1247 представлен обзор процессов, направленных на борьбу со спамом при передаче сообщений на мобильные устройства, и предлагается техническая основа противодействия такому спаму. В рамках данной основы определены функции объектов и процедуры обработки. Кроме того, в данной Рекомендации представлены механизмы совместного использования информации в целях борьбы со спамом при передаче сообщений на мобильные устройства в рамках антиспамовых доменов и между ними.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1247	23.03.2016 г.	17-я	11.1002/1000/12600

Ключевые слова

Антиспам, спам при передаче сообщений на мобильные устройства, техническая основа.

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

ПРЕДИСЛОВИЕ

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

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

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

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

ПРИМЕЧАНИЕ

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

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

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

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

На момент утверждения настоящей Рекомендации МСЭ не получил 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

Передача сообщений на мобильные устройства, включая службу передачи коротких сообщений и службу мультимедийных сообщений, развивается быстрыми темпами благодаря своей низкой стоимости, значительной гибкости и простоте использования. Однако спам при передаче сообщений на мобильные устройства нарушает повседневную жизнь потребителей и имеет многочисленные отрицательные последствия.

Сложно эффективно смягчать последствия спама при передаче сообщений на мобильные устройства, используя только одно решение. Применяя сочетание нескольких антиспамовых технологий к передаче сообщений на мобильные устройства, вред, вызываемый спамом в передаваемых на мобильные устройства сообщениях, может быть значительно снижен. Кроме того, учитывая, что спам при передаче сообщений на мобильные устройства широко распространен по всему миру, сотрудничество большого числа антиспамовых доменов может обеспечить более низкие затраты и более высокую эффективность. Следовательно, необходимо создать открытую основу, обеспечивающую использование различных решений и поддерживающую механизмы сотрудничества. Эта основа совместима с большинством антиспамовых технологий и не ограничивается конкретными техническими деталями. Выполняемые на этой основе процедуры должны требовать явно выраженного согласия конечного пользователя мобильного устройства и должны соответствовать национальным нормативам и законам.

Рекомендация МСЭ-Т X.1247

Техническая основа противодействия спаму при передаче сообщений на мобильные устройства

1 Сфера применения

В настоящей Рекомендации представлена техническая основа борьбы со спамом при передаче сообщений на мобильные устройства. В рамках данной основы определены функции объектов и процедуры обработки. Выполняемые на этой основе процедуры должны требовать явно выраженного согласия конечного пользователя мобильного устройства и должны соответствовать национальным нормативам и законам. Кроме того, в настоящей Рекомендации представлены механизмы совместного использования информации в целях борьбы со спамом при передаче сообщений на мобильные устройства в рамках антиспамовых доменов и между ними.

Настоящая Рекомендация применима в отношении службы коротких сообщений (SMS) и службы мультимедийных сообщений (MMS).

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 спам SMS (SMS spam) [b-ITU-T X.1242]: Спам, переданный через SMS.

3.1.2 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 техническом, социально-экономическом и практическом аспекте в национальном контексте. В частности, значение этого слова изменяется и расширяется с развитием технологий, открывающих 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 на мобильные устройства незапрашиваемых сообщений, целью которых является, как правило, маркетинг коммерческих продуктов или услуг.

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

3.2 Термины, определенные в данной Рекомендации

В настоящей Рекомендации определяются следующие термины:

3.2.1 антиспамовый домен (anti-spam domain): Независимая система, которая объединяет функцию антиспамового управления, функцию антиспамового мониторинга, функцию антиспамовой обработки и клиента передачи сообщений на мобильные устройства.

ПРИМЕЧАНИЕ. – Функции в антиспамовом домене определяются единым управлением оператора.

3.2.2 объект антиспамовой фильтрации (anti-spam filtering entity): Оборудование или система, которая применяет меры борьбы со спамом для фильтрации сообщений, отправленных на мобильные устройства, согласно правилам фильтрации. Объект может блокировать спам, помечать сообщения как подозрительные или отправлять сообщения получателю.

3.2.3 функции антиспамового управления (anti-spam management functions): Группа функций, которые применяются для административного управления антиспамовым доменом и контроля за ним, включая взаимодействие с другими антиспамовыми доменами в целях совместного использования информации о спаме, создания новых правил фильтрации на основе анализа спама и доставки их функциям антиспамовой обработки.

3.2.4 функции антиспамового мониторинга (anti-spam monitoring functions): Группа функций, которые применяются для мониторинга и анализа результатов фильтрации в домене антиспамовой обработки, включая проверку подозрительного спама, собранного ловушками, анализ данных спама, ведение статистики спама и выработку результатов анализа спама.

3.2.5 функции антиспамовой обработки (anti-spam processing functions): Группа функций, которые используются при обработке сообщений, отправленных на мобильные устройства, с применением правил и стратегий фильтрации. Эта группа обрабатывает сообщения путем блокирования спама, отправки со специальной отметкой или отправки сообщений получателю.

3.2.6 ложноотрицательный (false negative): Спам в отправленном на мобильное устройство сообщении был ошибочно обработан системой фильтрации как не являющийся спамом.

3.2.7 ложноположительный (false positive): Сообщение было ошибочно определено системой фильтрации как спам.

3.2.8 правила фильтрации (filtering rules): Набор правил алгоритмов противодействия, которые используются объектом антиспамовой фильтрации, такие как черные списки/белые списки, порог степени сходства и статистический порог. Правила фильтрации могут включать также правила фильтрации, определенные пользователем.

3.2.9 клиент передачи сообщений на мобильные устройства (mobile messaging client): Абонент службы отправки сообщений на мобильные устройства.

3.2.10 спам при передаче сообщений на мобильные устройства (mobile messaging spam): Незапрашиваемые электронные сообщения, которые поступают через службы передачи сообщений на мобильные устройства, как правило состоящие из спама службы передачи коротких сообщений (SMS) и спама службы передачи мультимедийных сообщений (MMS).

3.2.11 спам мультимедийных сообщений (multimedia message spam) (MMS): Спам, переданный через MMS.

3.2.12 служба отчетов (reporting service): Служба, которая обеспечивает сбор и накопление отчетов о спаме абонента при наличии разрешения пользователя, а также в соответствии с нормативами и национальными законами.

3.2.13 отчет по результатам анализа спама (spam analysis report): Результат анализа представляет эффективность системы фильтрации. Этот результат должен включать коэффициент ложноотрицательных/ложноположительных результатов фильтрации, характеристики спама в сообщениях, тенденции в изменении спама и другие аналитические данные.

3.2.14 статистика спама (spam statistics): Накопленные данные о спаме представляют масштаб спама при определенных ограничительных условиях, таких как интервал времени в антиспамовом домене. Статистика должна включать объем спама в сообщениях в рамках доменов входящих или выходящих сообщений, с указанием долей разных типов спама, списка спамеров и другие статистические данные о спаме.

3.2.15 подозрительный спам (suspicious spam): Неопределенное отправленное на мобильное устройство сообщение, в отношении которого существует подозрение, что это – спам.

3.2.16 отчет пользователя (user report): Жалоба от абонента, получающего на мобильное устройство сообщения, являющиеся спамом. В общем, отчет может включать время получения, международный номер абонента подвижной связи в цифровой сети с интеграцией служб/коммутируемой телефонной сети общего пользования (ЦСИС/КТСОП) (MSISDN) отправителя и получателя и т. д. Такой отчет включает информацию о сообщении, неверно помеченном как отправленный на мобильное устройство спам или не помеченном как отправленный на мобильное устройство спам, когда оно должно быть помечено как таковое, то есть о ложноположительных и ложноотрицательных результатах.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы

AO	Application Originated		Ориентированный на приложение
AMgmt	Anti-spam Mobile messaging Management Function		Функция антиспамового управления при передаче сообщений на мобильные устройства
Amon	Anti-spam Mobile Messaging Monitoring Function		Функция антиспамового мониторинга при передаче сообщений на мобильные устройства
APr	Anti-spam Mobile Messaging Processing Function		Функция антиспамовой обработки при передаче сообщений на мобильные устройства
GGSN	Gateway GPRS Supporting Node		Узел шлюза, поддерживающий GPRS
GPRS	General Packet Radio Service		Служба пакетной радиосвязи общего пользования
HPLMN	Home Public Land Mobile Network		Домашняя сухопутная подвижная сеть общего пользования
HTTP	HyperText Transfer Protocol		Протокол передачи гипертекста
ISDN	Integrated Services Digital Network	ЦСИС	Цифровая сеть с интеграцией служб
MAP	Mobile Application Part		Прикладная подсистема подвижной связи
MMS	Multimedia Message Service		Служба мультимедийных сообщений
MMSC	Multimedia Message Service Centre		Центр службы мультимедийных сообщений
MNO	Mobile Network Operator		Оператор сети подвижной связи
MO	Mobile Oriented		Ориентированный на мобильные устройства
MSC	Mobile Switching Centre		Центр коммутации подвижной связи
MSISDN	Mobile Subscriber International ISDN/PSTN Number		Международный номер абонента подвижной связи в ЦСИС/КТСОП
MT	Mobile Terminated		Завершенный в сети подвижной связи
PSTN	Public Switched Telephone Network	КТСОП	Коммутируемая телефонная сеть общего пользования
SMPP	Short Message Peer-to-Peer		Одноранговые короткие сообщения
SMS	Short Message Service		Служба коротких сообщений
SMSC	Short Message Service Centre		Центр службы коротких сообщений
UICC	Universal Integrated Circuit Card		Универсальная карта с интегральной схемой
VPLMN	Visited Public Land Mobile Network		Посещаемая сухопутная подвижная сеть общего пользования
WAP	Wireless Application Protocol		Протокол беспроводных приложений

5 Условные обозначения

Отсутствуют.

6 Обзор противодействия спаму при передаче сообщений на мобильные устройства

Как показано на рисунке 6-1, спам службы коротких сообщений (SMS) может создаваться, в основном, двумя путями. Первый путь – спамеры используют инструменты спама для массовой рассылки сообщений с помощью обычных коротких сообщений из пункта в пункт с большим числом собранных и дублированных универсальных карт с интегральной схемой (UICC). Другой путь – спамеры используют услуги массовой рассылки сообщений, предоставляемые поставщиками услуг, пользуясь интерфейсами шлюзов передачи коротких сообщений операторов. Учитывая, что операторы не имеют эффективного механизма технического и административного надзора над интерфейсом шлюза передачи коротких сообщений, этот шлюз может легко использоваться спамерами.

В зависимости от направления отправки сообщения существуют две процедуры, с помощью которых спамеры создают спамовые SMS, а именно процедура, ориентированная на мобильные устройства (MO)/ориентированная на приложение (AO), и процедура, ориентированная на завершение в сети подвижной связи (MT). При применении процедуры MO спам, созданный с помощью инструментов спама, направляется в центр службы коротких сообщений (SMSC) через соответствующие объекты сети отправителя. При применении процедуры AO короткие сообщения, введенные в спам из шлюза коротких сообщений оператора, направляются в SMSC. Далее, SMSC запрашивает центр коммутации подвижной связи (MSC), обслуживающий получателей, после чего направляет сообщения в этот центр. В конечном счете, короткое сообщение направляется получателю через посещаемую сеть MSC, который вызывает процедуру MT.

По разрешению абонента и в соответствии с административными нормативами операторы сетей подвижной связи (MNO) имеют право смягчать последствия рассылки спама, используя для этого объекты фильтрации. Процесс противодействия спаму должен неукоснительно отвечать применимым законодательным положениям во избежание нарушения конфиденциальности абонента.

Широко принято использование объектов антиспамовой фильтрации в процедуре MO/AO, в процедуре MT или в процедурах обоих типов. Для фильтрации спама в рамках процедуры MO объекты антиспамовой фильтрации собирают короткие сообщения от SMSC. Для обеспечения эффективной фильтрации спама в сети получателей необходимо также взаимодействие между MSC и объектом антиспамовой фильтрации.

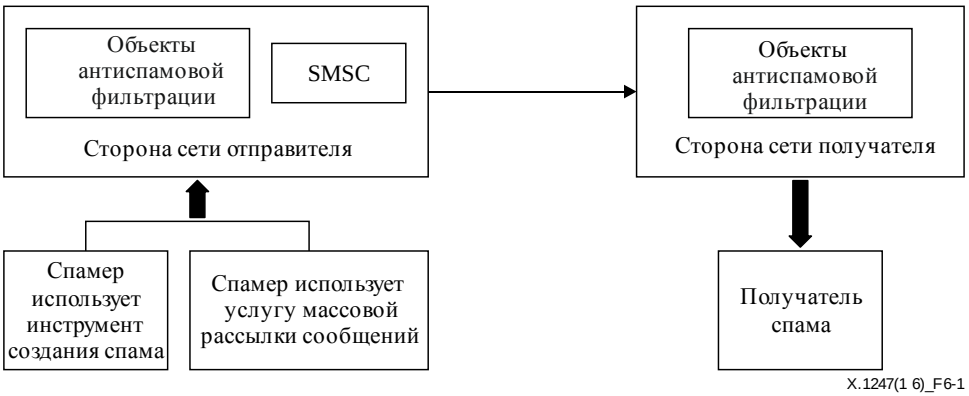

Рисунок 6-1 – Спам в виде SMS сети подвижной связи

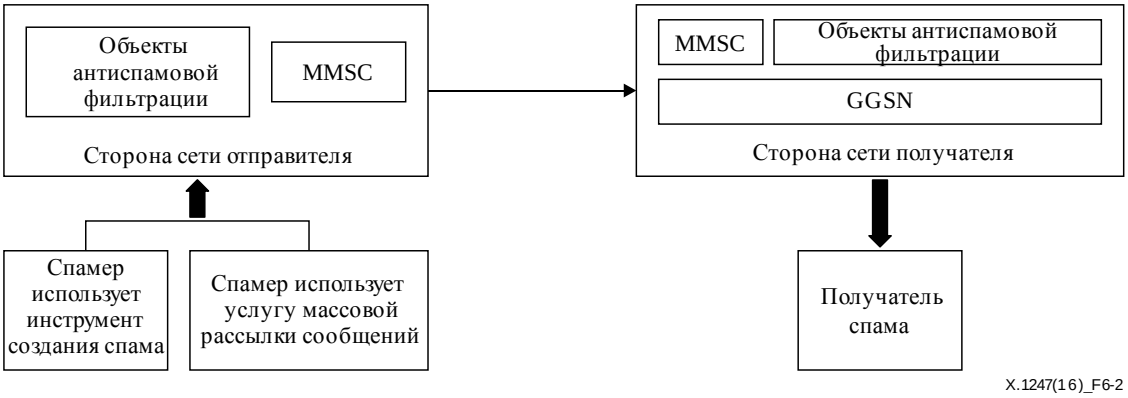

Рисунок 6-2 – Спам в виде MMS в сети подвижной связи

Как показано на рисунке 6-2, процедура отправки сообщений службы мультимедийных сообщений (MMS) аналогична процедуре, используемой в SMS, за исключением того, что MSC заменяется узлом шлюза, поддерживающим GPRS (GGSN), а SMSC заменяется центром службы мультимедийных сообщений (MMSC). Сообщение MMS будет направляться в MMSC сети получателя, после чего SMSC отправит сообщение SMS получателю. Получатель далее загрузит сообщение MMS из MMSC. По этой причине объекты антиспамовой фильтрации MMS могут быть развернуты рядом с MMSC, то есть не имеет значения, развернуты объекты фильтрации на стороне отправителя или на стороне получателя.

7 Структура функций противодействия спаму при передаче сообщений на мобильные устройства

Структура функций противодействия спаму при передаче сообщений на мобильные устройства объединяет функцию антиспамового управления при передаче сообщений на мобильные устройства (AMgmt), функцию антиспамового мониторинга при передаче сообщений на мобильные устройства (AMon), функцию антиспамовой обработки при передаче сообщений на мобильные устройства (APr) и клиентов передачи сообщений на мобильные устройства. Эти функции определяют антиспамовый домен при передаче сообщений на мобильные устройства.

Рекомендуется обеспечить связь с другими антиспамовыми доменами при передаче сообщений на мобильные устройства; они могут осуществлять между собой координацию в соответствии с правилами и стратегиями, определенными соответствующими соглашениями.

Эти функции могут взаимодействовать одна с другой, используя существующие протоколы обмена сообщениями, и их характеристики описаны ниже.

7.1 Общая структура

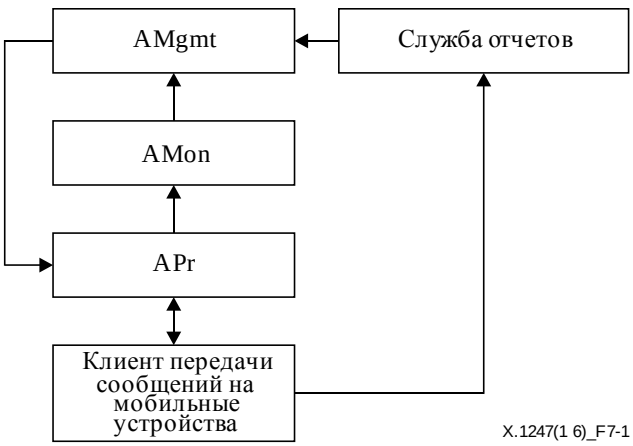

Рисунок 7-1 – Общая структура

AMgmt получает статистические данные о спаме от AMon и обновляет правила фильтрации в своем домене. AMgmt далее совместно использует информацию о спаме со службой отчетов и другими AMgmt.

AMon принимает от APr подозрительные на спам сообщения, отправленные на мобильные устройства, которые собираются ловушками или аналогичными платформами и проверяются, чтобы определить, являются ли они спамом. После накопления и анализа данных о спаме AMon передает также функции AMgmt данные анализа спама и статистические данные о спаме.

APr применяет правила к отправленным на мобильные устройства сообщениям, затем выбирает один из вариантов: отправить, отправить, пометив как спам, или блокировать эти сообщения в соответствии с различными стратегиями и результатами фильтрации и по разрешению пользователя. APr принимает правила фильтрации от AMgmt, а также информацию от пользователей – клиентов передачи сообщений на мобильные устройства. Для накопления подозрительного спама рекомендуется развертывать ряд платформ, таких как ловушки, в Apr.

Клиент передачи сообщений на мобильные устройства вносит вклад в процесс противодействия спаму при рассылке сообщений на мобильные устройства, обеспечивая обратную связь и сообщая APr, что принятое на мобильное устройство сообщение, помеченное как спам, является неверным, и направляя отчет о спаме службе отчетов.

Служба отчетов выполняет сбор и накопление отчетов о спаме абонентов по разрешению пользователя и в соответствии с нормативами и национальными законами. Это позволяет обеспечить совместное использование отчетов пользователей антиспамовыми доменами. Служба отчетов может функционировать под управлением обычного регуляторного аппарата, корпорации безопасности или MNO и т. д. Междоменные соглашения обеспечивают для доменов противодействия спаму при передаче сообщений на мобильные устройства возможность совместного использования специализированной информации о спаме.

7.2 Эталонная модель

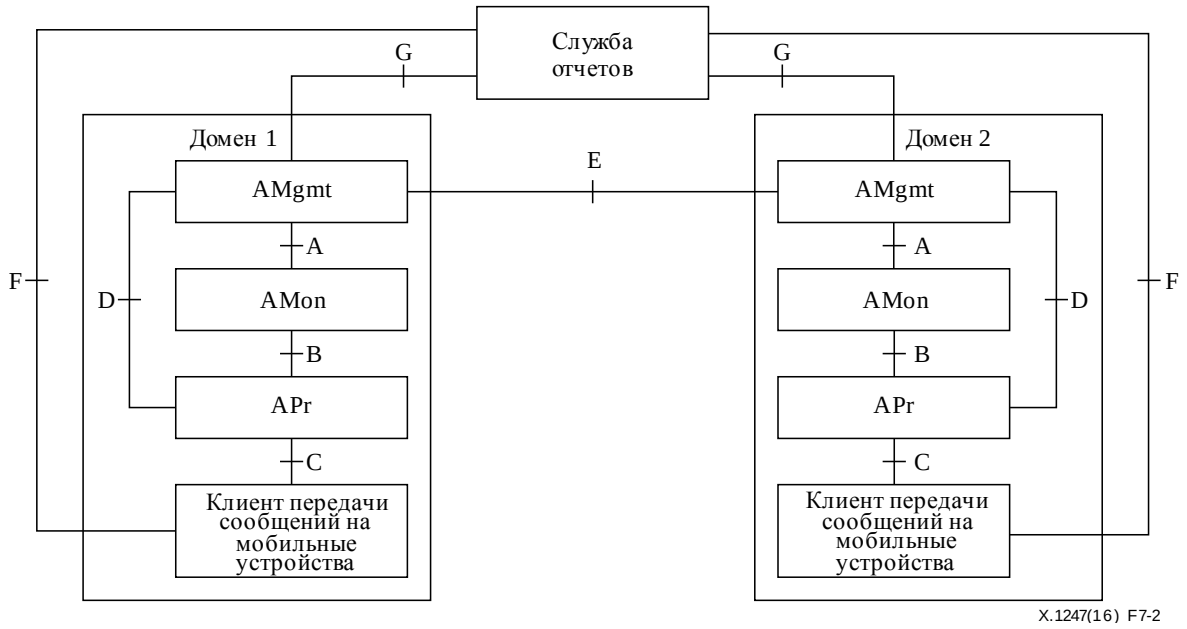

Рисунок 7-2 – Эталонная модель

Интерфейс A – это логический интерфейс между AMgmt и AMon. Интерфейс A используется для передачи аналитических отчетов о спаме и статистических данных о спаме.

Интерфейс B – это логический интерфейс между AMon и APr. Интерфейс B используется для передачи подозрительного спама, захваченного ловушкой, и откликов пользователей о том, что принятое на мобильное устройство сообщение, помеченное как спам, является неверным, которые поступают от клиента передачи сообщений на мобильные устройства.

Интерфейс C – это логический интерфейс между APr и клиентом передачи сообщений на мобильные устройства. Интерфейс C используется клиентом передачи сообщений на мобильные устройства для информирования APr о том, что полученное сообщение было ошибочно помечено MNO как спам. Вместе с тем интерфейс C используется также для отправки сообщений от APr клиенту передачи сообщений на мобильные устройства. В зависимости от разных типов клиента передачи сообщений на мобильные устройства в интерфейсе C должны поддерживаться различные протоколы, такие как прикладная подсистема подвижной связи и протокол беспроводных приложений (MAP/WAP), протокол передачи гипертекста (HTTP) и одноранговые короткие сообщения (SMPP).

Интерфейс D – это логический интерфейс между AMgmt и APr. Интерфейс D используется для передачи правил фильтрации.

Интерфейс E – это логический интерфейс между функциями AMgmt и другими доменами. Интерфейс E используется для обмена данными о спаме между разными доменами противодействия спаму при передаче сообщений на мобильные устройства.

Интерфейс F – это логический интерфейс между клиентом передачи сообщений на мобильные устройства и службой отчетов. Интерфейс F используется клиентом передачи сообщений на мобильные устройства для отправки отчета пользователя службе отчетов при явно выраженном согласии пользователя. В интерфейсе F должны поддерживаться различные протоколы, такие как прикладная подсистема подвижной связи и протокол беспроводных приложений (MAP/WAP), протокол передачи гипертекста (HTTP) и одноранговые короткие сообщения (SMPP).

Интерфейс G – это логический интерфейс между AMgmt и службой отчетов. Интерфейс G служит для передачи информации отчетов о спаме от службы отчетов к функции AMgmt.

В этой эталонной модели интерфейсы A–D являются внутридоменными интерфейсами, а интерфейсы E–G являются междоменными интерфейсами.

7.3 Функции компонентов

7.3.1 Клиенты передачи сообщений на мобильные устройства

Функции клиента передачи сообщений на мобильные устройства включают:

- обеспечение механизмов, помогающих пользователям отправлять отчеты пользователей службе отчетов;
- обеспечение механизмов, помогающих пользователям информировать APr о полученных сообщениях, ошибочно помеченных как спам;
- фильтрация сообщений на основе конкретных правил фильтрации с использованием приложений безопасности.

7.3.2 APr

Функции APr включают:

- применение правил противодействия спаму, полученные от AMgmt, и выбор одного из вариантов: отправить; отправить, пометив как спам; или блокировать сообщения в соответствии с различными стратегиями и результатами фильтрации;
- получение откликов пользователей от клиента передачи сообщений на мобильные устройства, который сообщает, что полученное сообщение, помеченное как спам, таковым не является;
- сбор подозрительного спама с помощью ловушки или других аналогичных платформ;
- доставка функции AMon откликов пользователей, а также подозрительного спама, собранного ловушкой.

7.3.3 AMon

Функции AMon включают:

- накопление подозрительного спама, собираемого ловушкой и поступающего от Apr, и информации отчетов пользователей от службы отчетов;
- проверка подозрительного спама, поступившего от Apr;

- анализ накопленных данных о спаме для изучения характеристик нового спама;
- сообщение статистических данных о спаме и данных анализа спама функции AMgmt.

7.3.4 AMgmt

Функции AMgmt включают:

- получение статистических данных о спаме и аналитического отчета о спаме от Amon;
- анализ данных, сообщенных функциями Amon, для выработки правил фильтрации;
- отправка правил фильтрации функциям APr, эти правила фильтрации будут применяться в отношении клиента передачи сообщений на мобильные устройства;
- взаимодействие с другими функциями AMgmt для обмена данными о спаме и их совместного использования, таких как объем спама, ресурс и характеристики спама, новый список спамеров и т. д.;
- получение информации отчетов пользователей от службы отчетов, включая данные об основных нарушителях, статистику тенденции спама. Информация отчетов пользователей может быть специализированной и включать некоторые обработанные данные из отчетов пользователей в соответствии с соглашением со службой отчетов и в сфере, разрешенной нормативами и национальными законами;
- обеспечение возможности установления абонентом определяемых пользователем правил фильтрации и отправка правил функции APr после проверки их действительности.

7.3.5 Служба отчетов

Функции службы отчетов включают:

- сбор отчетов пользователей и верификация на предмет того, являются ли они спамом;
- хранение и анализ спама для генерирования характеристик спама, используя вместо контента отпечатки пальцев во избежание нарушения конфиденциальности;
- предоставление данных отчетов пользователей, с тем чтобы обеспечить MNO возможность понимать масштаб спама, который находится в пределах их сетей, поступает в них или покидает их, от других операторов, которые запрашивают функции MNO использовать такое наглядное представление, для того чтобы направлять меры принудительного характера только против рассылки спама, не затрагивая пользователей и контент.

8 Технологии противодействия спаму при передаче сообщений на мобильные устройства

Представленные в настоящем разделе технологии относятся к описанной выше структуре противодействия спаму, а также приведен их пример. Все эти меры следует применять с осторожностью, с тем чтобы обеспечить соответствие применимым нормам, национальным законам, а также не нарушать данное пользователем разрешение. Это направлено на недопущение нарушения конфиденциальности абонента.

8.1 Механизмы обратной связи с пользователем

Механизмы обратной связи с пользователем дают абонентам возможность сообщать системе фильтрации свое мнение о результате фильтрации спама. Рекомендуется реализовать службу отчетов и обратную связь с пользователями, с тем чтоб повышать качество результатов фильтрации MNO.

Служба отчетов – это система для сбора отчетов пользователей о получении спамовых сообщений, и она может быть создана правительствами, операторами и т. д. Служба отчетов может быть горячей линией, веб-сайтом или центром отчетов о спамовых коротких сообщениях; таким образом MNO может собирать спамовые короткие сообщения и корректировать правила фильтрации. В целом, регистрация жалоб на получение спамовых коротких сообщений должна включать хэш спамового сообщения, время получения, а также MSISDN отправителей и т. д. В соответствии с различными стратегиями и только с согласия пользователя MNO может не только блокировать спам, но также предлагать получателям доступ к карантину, то есть такие сообщения могут быть отправлены с пометкой или быть записаны на специальном веб-сайте. Это позволяет получателям видеть этот "потенциальный спам", который был помечен как подозрительный спам, и дает им возможность

осуществить обратную связь, если они считают решение, принятое по конкретному сообщению, неверным или "ложноположительным". Не все отклики пользователей надежны сами по себе. Получатели могут ошибаться или исходить из альтернативных причин для указания полученного сообщения в качестве спама. Прежде чем использовать информацию о распознавании спама для создания отпечатков пальцев или правил фильтрации, ее необходимо проверить вручную. Может быть введена система определения рейтинга доверия к направляющим отчеты для автоматического определения корректной обратной связи на фоне ошибочной и злоумышленной.

8.2 Ловушка

Ловушка телефонных номеров – это учетная запись, которая создается в качестве "западни" для целей обнаружения и отклонения неразрешенного использования сообщений, отправленных на мобильные устройства, а также противодействия такому использованию. В этом как правило участвует учетная запись, которая используется или создается для того, чтобы быть обнаруженной спамерами, включая неактивные и несуществующие телефонные номера. Таким образом, любое сообщение, отличающееся от того, что ожидается, может обрабатываться как подозрительный спам и может быть подходящим для анализа контента. Часто может происходить переназначение телефонных номеров, а также при наборе телефонных номеров часто допускаются ошибки, поэтому ловушки телефонных номеров будут получать большое число случайных и не являющихся спамом сообщений. Для того чтобы отфильтровать такие нежелательные данные, до анализа подозрительного спама в целях извлечения его характеристик, необходимо провести верификацию этого подозрительного спама.

Обратная связь с пользователями характеризуется задержками, – до того как получатели сообщат о нежелательных сообщениях, может пройти от нескольких минут до нескольких дней. Западни-ловушки, напротив, могут сразу обнаруживать нежелательные сообщения по мере их доставки.

8.3 Методы определения, используемые MNO

Наряду с обратной связью с пользователями и ловушкой MNO может принять ряд иных мер для определения спама до отсылки его получателям. В зависимости от различных стратегий такие сообщения будут блокироваться или отправляться со специальной отметкой как подозрительные. Эти методы определения могут зависеть от характеристик спама или порядка отправки.

- Черный список/белый список международных номеров абонента подвижной связи в цифровой сети с интеграцией служб/коммутируемой телефонной сети общего пользования (ЦСИС/КТСОП) (MSISDN) отправителя

  MSISDN – это основная информация для различения сообщений, поступивших от абонента или от спамера. В черных списках/белых списках используется MSISDN отправителя для приостановки/принятия сообщений. Операторы подвижной связи могут блокировать широко известных или опознанных спамеров, а абоненты могут определять свои собственные белые списки/черные списки для блокирования или принятия сообщений от конкретных отправителей.

- Распознание неопределенности

  Для обхода фильтрации спама спамеры используют вводящие в заблуждение средства. Например, в текст сообщений произвольно включаются некоторые особые символы, такие как "*","^" и т. д. Буквы заменяются аналогичными символами, например слово "porn" может быть изменено на "p0rn". Может производиться увеличение или вращение изображений. Распознание неопределенности должно узнавать такие уловки и, если имеется разрешение, отфильтровывать их.

- Частота отправки

  В целях быстрого распространения спама спамеры могут в короткое время рассылать сообщения большой части получателей. Спамеры отправляют свои сообщения со значительно большей скоростью по сравнению со скоростью обычного отправителя, поэтому интервал между двумя сообщениями значительно короче. В случае если частота отправки пользователем сообщений превышает заранее установленное пороговое значение, этот пользователь будет определен как весьма подозрительный в том, что он является спамером.

- Коэффициент результативности рассылки сообщений

  Спам в виде сообщений отправляется неизвестным получателям, по этой причине спамер выбирает получателей произвольным образом. Вследствие этого, как правило, попадается ряд несуществующих вызываемых номеров. Коэффициент результативности рассылки сообщений в случае спама заметно ниже по сравнению с обычной отправкой сообщений на мобильные устройства.

- Запись вызовов отправителя

  Запись вызовов пользователя может помочь оператору при анализе шаблона посылки. Такая запись должна содержать, как минимум, номер телефона отправителя, номер телефона получателя и время отправки. Если сообщение отправлено многим абонентам и характеризуется очень низким коэффициентом отзывов или ответных сообщений, отправитель может быть заподозрен как спамер. Спамеры редко используют другие предоставляемые оператором услуги (например, голосовые вызовы), не являющиеся услугой отправки сообщений.

8.4 Дополнительное улучшение

- Определяемая пользователем конфигурация правил

  Механизм определяемой пользователем конфигурации правил позволяет получателям определять и информировать систему фильтрации о том, сообщения какого типа получатель не хотел бы получать. Фильтрация сообщений в соответствии с определенными пользователем правилами может выполняться MNO или с помощью программного обеспечения, установленного получателями.

- Маршрутизация обратно к домашней сухопутной подвижной сети общего пользования получателя (HPLMN)

  Операторы могут применять различные процессы противодействия спаму для клиентов, находящихся в роуминге за пределами HPLMN. Процесс маршрутизации сообщений обратно к HPLMN является необязательным, поэтому находящиеся в роуминге получатели могут получить сообщение, не прошедшее фильтрацию от спама. Вследствие этого сообщения, отправленные находящимся в роуминге клиентам, должны пройти обратную маршрутизацию до объектов антиспамовой фильтрации в HPLMN, не рассчитывая на посещаемую сеть. До прибытия в посещаемую сухопутную подвижную сеть общего пользования (VPLMN) HPLMN получателя необходимо получить и отфильтровать сообщения, применяя соответствующие меры противодействия спаму.

9 Отношения между антиспамовыми доменами

Эффективность мер противодействия спаму в одном антиспамовой домене ограничена и в техническом и в экономическом аспектах. Необходимо присоединение и взаимодействие MNO, важны также механизмы сотрудничества между их антиспамовыми доменами. Механизмы взаимодействия могут способствовать повышению эффективности и действенности функционирования их систем противодействия спаму.

Между антиспамовыми доменами существуют отношения двух типов – доверительные отношения и недоверительные отношения (рисунок 9-1). Отношения по умолчанию между антиспамовыми доменами должны быть недоверительными, в каковом случае все сообщения от недоверенных одноранговых объектов будут проходить фильтрацию. В рамках соглашений о сотрудничестве могут быть установлены доверительные отношения между одноранговыми антиспамовыми доменами; в случае таких отношений операторы могут не выполнять фильтрацию сообщений от доверенных одноранговых объектов, основываясь на своих стратегиях и правилах фильтрации.

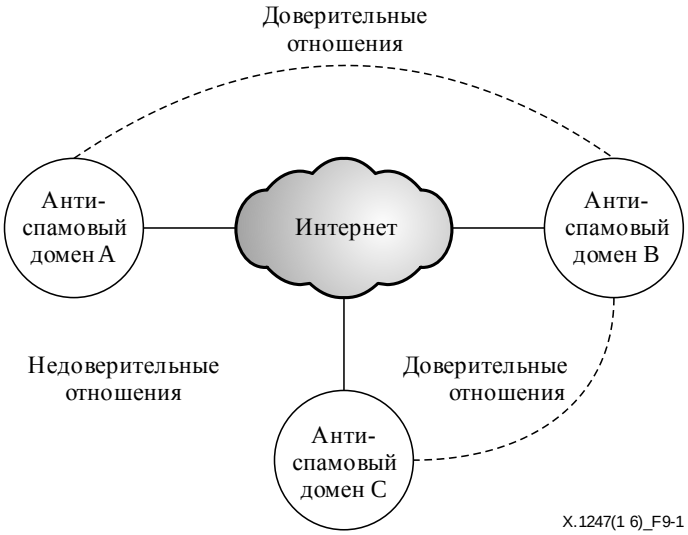

Рисунок 9-1 – Доверительные отношения и недоверительные отношения

Доверительные отношения являются нетранзитивными. Например, если домен A доверяет домену B, а домен B доверяет домену C, то домен A может не доверять домену C, если они напрямую не согласовали и не установили доверительные отношения. Доверительные отношения являются двунаправленными, то есть доверенные одноранговые объекты применяют один к другому одинаковые режимы.

После установления доверительных отношений рекомендуются следующие механизмы координации.

- Совместное использование данных о спаме

  Определенные данные о спаме используются совместно через соединение AMgmt. Совместно используемая информация может содержать черные списки, ключевые слова, отчеты о поступивших жалобах, а также новые характеристики спама. Назначение этой информации будет обсуждаться в процессе установления доверительных отношений. Совместное использование данных о спаме потребует явно выраженного согласия конечного пользователя мобильного устройства и должно соответствовать национальным нормативам и законам.

- Аутентификация источника сообщений

  Сообщение от доверенного однорангового объекта будет рассматриваться как аутентичное, только если источник сообщения аутентифицирован.

- Пропуск фильтрации

  Сообщения от доверенного домена могут отправляться непосредственно получателю, с тем чтобы избежать дублирования обработки сообщений.

- Отчет о жалобах пользователя и обратная связь о подозрительном спаме

  Если получены отчеты о спаме и подозрительный спам в сообщениях от доверенных одноранговых объектов, эти сообщения должны быть отправлены доверенным одноранговым объектам для улучшения их правил фильтрации в соответствии с применимыми нормативами и национальными законами.

Для соответствия различным механизмам координации функции APr и AMon при обработке сообщений, отправленных на мобильные устройства, должны выполнять разные процедуры. Apr принимает решение, применять ли к сообщению фильтрацию. В соответствии с соглашением AMon направляет/блокирует сообщение или отправляет отклик в рамках обратной связи с одноранговыми объектами. На рисунках 9-2 и 9-3 представлены рабочие потоки APr и AMon.

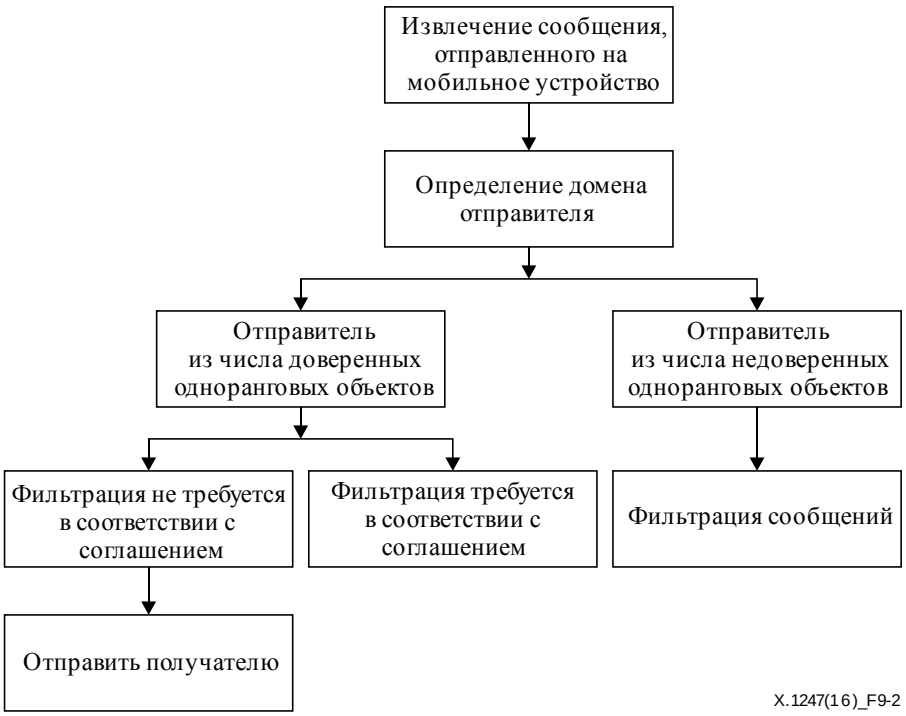

Рисунок 9-2 – Потоки обработки сообщений, отправленных на мобильные устройства, в APr

Рисунок 9-3 – Потоки обработки сообщений, отправленных на мобильные устройства, в AMon

10 Антиспамовая обработка сообщений, отправленных на мобильные устройства

В процесс противодействия спаму в сообщениях, отправленных на мобильные устройства, следует ввести адаптивный механизм для учета постоянно появляющегося нового спама и его новых разновидностей. В целом, процесс противодействия спаму можно рассматривать как состоящий из восьми процедур, показанных на рисунке 10-1. Эти процедуры образуют адаптивную систему, которая вносит вклад в оптимизацию работы системы.

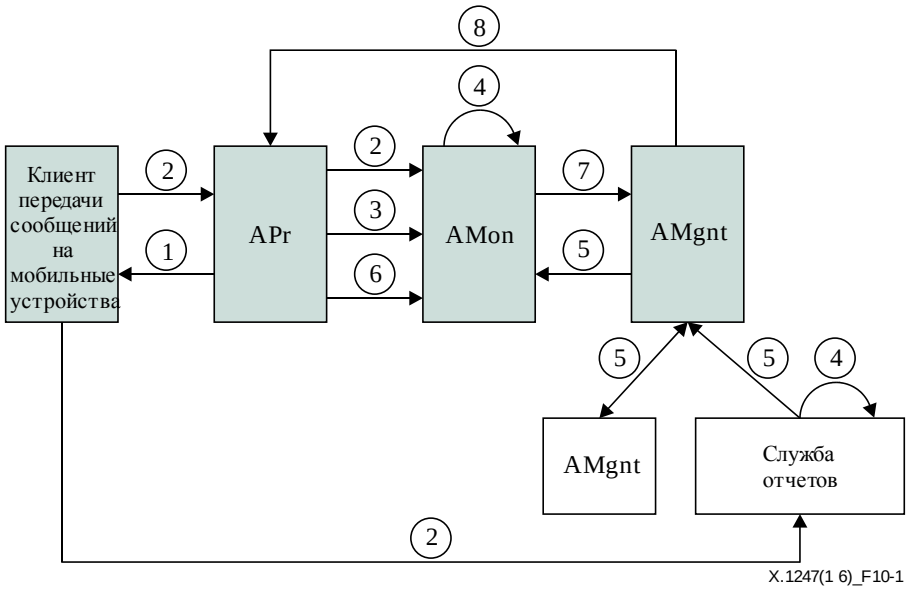

Рисунок 10-1 – Процедуры антиспамовой обработки

Процедура 1: Фильтрация сообщений

На основании стратегий и правил фильтрации APr особым образом помечает или фильтрует спамовые сообщения до отправки этих сообщений получателю. Эти правила фильтрации могут устанавливаться операторами или настраиваться пользователями.

Процедура 2: Отправка пользователем откликов в рамках обратной связи

Клиент передачи сообщений на мобильные устройства отправляет жалобы пользователя службе сообщений для указания о неотфильтрованном спаме, а также отправляет отклики пользователей функции AMon для указания о принимаемых сообщениях, ошибочно помеченных как спам. Это поможет операторам совершенствовать свои правила фильтрации.

Процедура 3: Пересылка подозрительного спама

APr отправляет подозрительный спам, собранный ловушкой, функции AMon для верификации.

Процедура 4: Верификация спама

AMon занимается подозрительным спамом, осуществляя верификацию, а служба отчетов занимается пользовательским отчетом о спаме. Эта сложная процедура, которая основана на минимальном ручном вмешательстве и отвечает применимым нормативам и национальным законам. Для верификации должны использоваться отпечатки пальцев или хешированные данные о спаме, а не контент передаваемых сообщений. В дополнение к этой оценке может использоваться определенная информация, например репутация отправителя и представляющего отчет, то есть отчетам пользователя присваивается рейтинг доверия.

Процедура 5: Совместное использование информации

AMgmt осуществляет обмен данными о спаме с доверенными одноранговыми объектами, а также AMgmt принимает индивидуализированный анализ спама от службы отчетов. В соответствии с достигнутым при согласовании консенсусом данные могут включать статистику отчетов пользователей, список спамеров, жалобы в рамках обратной связи и новые характеристики спама. Эти данные о спаме должны тщательно обрабатываться, с тем чтобы убедиться, что не включен пользовательский контент.

Процедура 6: Мониторинг функционирования системы

На AMon лежит также задача мониторинга функционирования системы фильтрации спама. AMon собирает данные от APr для составления отчетов о функционировании и их анализа. Отчет о функционировании может включать цифровые данные о функционировании в реальном времени, пропорцию спама, коэффициент ложноотрицательных результатов и т. д.

Процедура 7: Анализ спама

Подтвержденные данные от службы отчетов, доверенных одноранговых объектов и AMon собираются и сохраняют с учетом нормативов и национальных законов. Периодически Amon может осуществлять анализ этих данных и изучать новые шаблоны и характеристики спама. Наконец, эти аналитические данные используются для выработки статистических данных смапа и отчета об анализе спама, который будет передаваться функции AMgmt.

Процедура 8: Корректировка мер противодействия

В соответствии со статистикой спама и аналитическим отчетом от Amon функция AMgmt оценивает эффективность противодействия спаму системы фильтрации спама на предмет возможных улучшений. На основе результатов оценки меры и стратегии могут корректироваться, и могут вноситься изменения в механизмы взаимодействия с другими доменами. Будут приниматься соответствующие меры, такие как установление или прекращение доверительных отношений и распространение новых правил и стратегий фильтрации между функциями APr.

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.1242] Рекомендация МСЭ-Т X.1242 (2009 г.), *Система фильтрации спама в услуге передачи коротких сообщений (SMS) на основе определяемых пользователем правил*.

[b-M3AAWG report] M3AAWG, *Mobile Messaging Best Practices for Service Providers*, Updated August 2015.
https://www.m3aawg.org/sites/default/files/M3AAWG-Mobile-Messaging-Best-Practices-Service-Providers-2015-08.pdf

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, 2017 г.