



МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1242

(02/2009)

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

Безопасность в киберпространстве – Противодействие
спаму

**Система фильтрации спама в услуге передачи
коротких сообщений (SMS) на основе
определяемых пользователем правил**

Рекомендация МСЭ-Т X.1242

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

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

Рекомендация МСЭ-Т X.1242

Система фильтрации спама в услуге передачи коротких сообщений (SMS) на основе определяемых пользователем правил

Резюме

В настоящей Рекомендации описана реализация системы фильтрации спама в SMS на основе определяемых пользователем правил. Она определяет структуру системы фильтрации спама в SMS, функции фильтрации спама в SMS, управление услугой пользователя, протоколы связи и базовые функциональные требования к оконечным устройствам с функциями SMS.

Источник

Рекомендация МСЭ-Т X.1242 утверждена 20 февраля 2009 года 17-й Исследовательской комиссией МСЭ-Т (2009–2012 гг.) в соответствии с процедурой, описанной в Резолюции 1 ВАСЭ.

Ключевые слова

Система фильтрации, SMS, спам в SMS, система фильтрации спама в SMS на основе определяемых пользователем правил.

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 I 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/>.

© ITU 2009

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 настоящей Рекомендации.....	2
4 Сокращения и акронимы.....	2
5 Условные обозначения.....	3
6 Описание системы	3
7 Структура системы.....	3
7.1 Общая структура.....	3
7.2 Требования к модулю.....	4
7.3 Требования к устройству	6
8 Функция фильтрации спама в SMS.....	6
8.1 Режимы работы SMS.....	6
8.2 Требования к фильтрации спама в SMS	7
9 Управление услугой со стороны пользователя.....	9
9.1 Методы управления	9
9.2 Возможности управления	11
10 Протоколы связи.....	12
10.1 Структуры протоколов связи.....	12
10.2 Протокол аутентификации.....	13
10.3 Протокол ISMG.....	13
Дополнение I – Требования к программному обеспечению оконечных устройств, поддерживающему фильтрацию спама в SMS	14
I.1 Основные характеристики	14
I.2 Основное программное обеспечение для фильтрации спама в SMS.....	14
I.3 Расширенное программное обеспечение для фильтрации спама в SMS.....	15
Библиография	16

Введение

С ростом популярности услуг подвижной связи SMS стала одной из самых прибыльных дополнительных платных услуг благодаря низкой цене, отличной гибкости и простоте использования. Однако в то же время рассылка спама в SMS быстро растет и влечет за собой следующие серьезные последствия:

- снижение степени удовлетворенности пользователей услугами SMS;
- растрачивание сетевых ресурсов;
- повышение социальной нестабильности;
- оказание других негативных воздействий.

Следовательно, очень важно найти эффективные и действенные решения по противодействию спаму в SMS при сохранении эффективности работы SMS. Однако необходимо принять во внимание следующие принципы:

- свести к минимуму изменения в интерфейсе пользователя SMS;
- повысить доверие пользователей к SMS;
- обеспечить простоту в реализации и развертывании;
- свести к минимуму изменения, вносимые в существующую сетевую систему.

Система фильтрации спама в SMS на основе определяемых пользователем правил, в которой учитываются вышеизложенные принципы, является эффективным и действенным способом противодействия спаму в SMS. Предполагается создание такой системы фильтрации спама в SMS, в которой пользователи могли бы сами устанавливать правила фильтрации SMS и поручить системе, принадлежащей поставщику услуг или оператору сети блокировать короткие сообщения, соответствующие этим правилам.

Эта система имеет следующие достоинства:

- защищает конфиденциальность пользователей от нарушения при помощи правил, определяемых пользователем;
- соответствует требованиям пользователей по мерам противодействия спаму в SMS;
- проста в реализации без изменения существующих сетевых систем;
- работает в качестве дополнительной платной услуги, которая может быть выгодна для поставщиков услуг.

Данная Рекомендация применима для разработки, внедрения и оценки системы фильтрации спама в SMS на основе определяемых пользователем правил в сетях подвижной и фиксированной связи.

Система фильтрации спама в услуге передачи коротких сообщений (SMS) на основе определяемых пользователем правил

1 Сфера применения

В настоящей Рекомендации приводится описание реализации системы фильтрации спама в SMS на основе определяемых пользователем правил, называемой далее системой фильтрации спама в SMS или системой фильтрации. Она определяет:

- структуру системы фильтрации;
- функции фильтрации спама в SMS;
- управление услугой пользователя;
- протоколы связи;
- функциональные требования оконечного устройства.

Данная Рекомендация применима для разработки, внедрения и оценки системы фильтрации спама в SMS на основе определяемых пользователем правил в сетях подвижной и фиксированной связи.

ПРИМЕЧАНИЕ. – Некоторые механизмы фильтрации, описанные в настоящей Рекомендации, могут затрагивать конфиденциальность трафика электросвязи. В связи с этим в реализациях систем фильтрации спама в SMS должны приниматься меры для обеспечения соответствия применимому законодательству. Данная Рекомендация или ее части не могут применяться в Германии вследствие законодательства этой страны.

2 Справочные документы

Нижеследующие Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники являются предметом пересмотра, поэтому всем пользователям данной Рекомендации предлагается рассмотреть возможность применения последнего издания Рекомендаций и других ссылок, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т публикуется регулярно. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус рекомендации.

[ETSI TR 101 632] ETSI TR 101 632 V7.0.0 (2000-06), *Digital cellular telecommunications system (Phase 2+) (GSM); Interface protocols for the connection of Short Message Service Centres (SMSCs) to Short Message Entities (SMEs) (GSM 03.39 version 7.0.0 Release 1998)*.
<<http://pda.etsi.org/exchangefolder/tr-101632v070000p.pdf>>

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 подвижная станция (mobile station (MS)): Объект, имеющий доступ к набору услуг UMTS посредством одного или нескольких интерфейсов. Это может быть стационарный или подвижный объект в пределах зоны обслуживания UMTS, который имеет доступ к услугам UMTS и может одновременно работать с одним или несколькими пользователями. [b-ETSI TR 125 990].

3.1.2 короткое сообщение (short message): Информация, которая передана от отправляющего пользователя к принимающему пользователю через SMSC. [b-ETSI TS 102 507].

3.1.3 объект короткого сообщения (short message entity (SME)): SME – это объект, который создает и удаляет короткое сообщение, может располагаться в HLR, MC, VLR, MS или MSC и быть неотделим от них, либо может находиться за их пределами. [b-ITU-T Q.1742.3].

3.1.4 центр коротких сообщений (short message service centre (SMSC)): Функциональный блок, который отвечает за передачу, хранение и пересылку короткого сообщения (SM) между двумя SM-TE или между SME и MS. SMSC функционально может быть как отделен от сети, так и быть интегрирован в сеть. [b-ETSI ES 201 986].

3.1.5 SMS-DELIVER: Блок данных протокола передачи короткого сообщения, содержащий данные пользователя (короткое сообщение), передаваемый от SC к MS. [b-ETSI TS 100 901].

3.1.6 SMS-STATUS-REPORT: Блок данных протокола передачи короткого сообщения, информирующий принимающую MS о статусе короткого сообщения, поступающего от подвижного объекта, которое ранее было передано мобильной станцией, т. е. о том, готов ли SC передать сообщение или нет, или что сообщение сохранено в SC для последующей передачи. [b-ETSI TS 100 901].

3.1.7 SMS-SUBMIT: Блок данных протокола передачи короткого сообщения, содержащий данные пользователя (короткое сообщение), передаваемый от MS к SC. [b-ETSI TS 100 901].

3.1.8 отчет о состоянии (status report): SC оповещает передающую MS о результатах доставки короткого сообщения к SME. [b-ETSI TS 100 901].

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации даны определения следующих терминов:

3.2.1 шлюз передачи коротких сообщений через интернет (Internet short message gateway (ISMG)): Объект между SP и SMSC, осуществляющий доставку короткого сообщения от SP к SMSC и от SMSC к SP, реализующий преобразование протоколов интерактивной информации между SP и SMSC.

3.2.2 услуга передачи коротких сообщений (short message service (SMS)): Услуги в сетях электросвязи, которые позволяют мобильным телефонам, телефонам и другим объектам коротких сообщений передавать и принимать текстовые сообщения через центры коротких сообщений, на которых эти сообщения хранятся, если с оконечным устройством не может быть установлена связь.

3.2.3 спам (spam): Электронная информация, переданная от отправителей к получателям при помощи оконечных устройств, таких как компьютеры, мобильные телефоны, телефоны и т. д., которая, как правило, не предусмотрена, нежелательна и опасна для получателей.

3.2.4 спам в SMS (SMS spam): Спам, передаваемый с использованием SMS.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

FMD	Filtered Messages Database	База данных отфильтрованных сообщений
ISMG	Internet Short Message Gateway	Шлюз передачи коротких сообщений через интернет
MS	Mobile Station	Подвижная станция
SC	Service Centre	Центр обслуживания
SCM	Service Control Module	Модуль управления услугой
SM MO	Short Message Mobile Originated Point-to-Point	Передача короткого сообщения с мобильного устройства "из пункта в пункт"
SM MT	Short Message Mobile Terminated Point-to-Point	Передача короткого сообщения на мобильное устройство "из пункта в пункт"
SME	Short Message Entity	Объект короткого сообщения
SMPP	Short Message Point to Point	Короткое сообщение "из пункта в пункт"
SMS	Short Message Service	Услуга передачи коротких сообщений

SMSC	Short Message Service Centre	Центр коротких сообщений
SP	Service Provider	Поставщик услуг
SS	Secretary Station	Диспетчерская станция
SSFМ	SMS Spam Filtering Module	Модуль фильтрации спама в SMS
SSFS	SMS Spam Filtering Service	Услуга фильтрации спама в SMS
URD	User-specified Rules Database	База данных правил, определяемых пользователем
USMM	User Service Management Module	Модуль управления услугой пользователя

5 Условные обозначения

Нет.

6 Описание системы

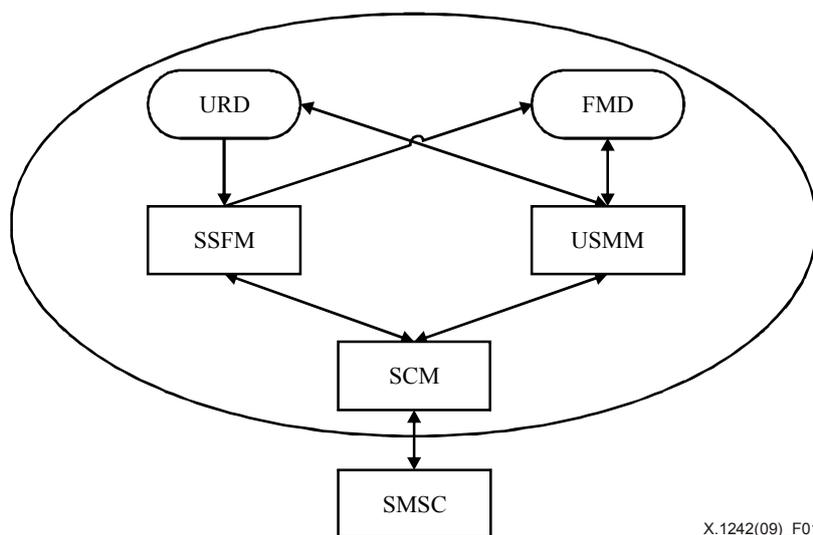
Под системой фильтрации спама в SMS на основе определяемых пользователем правил понимается система фильтрации, соединенная с центром коротких сообщений (SMSC), в которой пользователи могут настраивать (добавлять, удалять и изменять) правила фильтрации, и при этом все короткие сообщения, передаваемые таким пользователям, могут быть отфильтрованы в соответствии с этими правилами фильтрации. Кроме того, пользователи могут управлять (запрашивать, удалять и восстанавливать) отфильтрованные короткие сообщения при помощи определенных методов.

Правила фильтрации могут быть основаны на адресе (номере телефона), времени, содержании и т. д. Кроме того, конкретные правила фильтрации могут использоваться по отдельности или в сочетании с другими правилами фильтрации. Если правила фильтрации используются в сочетании с другими правилами фильтрации, то одним из необходимых шагов при установлении правил является определение приоритетности правил фильтрации. Для того чтобы этой услугой было легко и практично пользоваться, пользователям должен быть предоставлен, по крайней мере, один из следующих методов управления: SMS, веб-интерфейс и диспетчерская станция.

7 Структура системы

7.1 Общая структура

Система фильтрации спама в SMS включает в себя следующие логические модули: модуль управления услугой (SCM), модуль фильтрации спама в SMS (SSFМ), модуль управления услугой пользователя (USMM), база данных правил, определяемых пользователем (URD), и база данных отфильтрованных сообщений (FMD). Структура системы фильтрации спама в SMS показана на рисунке 1.



X.1242(09)_F01

Рисунок 1 – Структура системы фильтрации спама в SMS

В зависимости от своего расположения пять модулей, показанные на рисунке 1, выше, могут быть отнесены к трем уровням: уровню доступа, уровню услуги и уровню данных. Уровень доступа включает SCM; уровень услуги включает USMM и SSFM; уровень данных включает URD и FMD.

7.2 Требования к модулю

7.2.1 Уровень доступа

Уровень доступа, нижний уровень, соединен непосредственно с SMSC и отвечает, главным образом, за элементы внешней системы, включая пользователей, получающие доступ к системе фильтрации.

7.2.1.1 Модуль управления услугой (SCM)

SCM представляет собой комплексную платформу управления услугой системы фильтрации, которая включает в себя следующие функции:

- Выполнение запроса относительно подписки на услугу: фильтрация спама в SMS – это вид дополнительной услуги для пользователей. Таким образом, перед отправкой любого короткого сообщения должен быть передан запрос в SCM, для того чтобы выяснить, подписан ли получатель на услугу фильтрации спама в SMS или нет. Если у получателя такая подписка есть, то короткое сообщение будет доставлено в SSFM для продолжения последующих процессов фильтрации; в противном случае, короткое сообщение будет передано с использованием обычного процесса доставки (без фильтрации).
- Доставка инструкции управления: короткое сообщение, включающее инструкции по управлению услугой (управление состояниями услуги, правилами фильтрации и отфильтрованными короткими сообщениями), должно быть распознано и доставлено от SCM в USMM.

SCM является относительно независимым модулем, который может быть объединен с другими дополнительными платными услугами для формирования интегрированной платформы обслуживания, с тем чтобы обеспечить простоту реализации и развертывания. Как правило, на практике SCM выполняет учетные функции.

7.2.2 Уровень услуги

Уровень услуги реализует основные функции системы фильтрации: фильтрацию спама в SMS, управление правилами фильтрации и управление отфильтрованными короткими сообщениями. На практике уровень услуги включает в себя, по меньшей мере, два модуля: модуль фильтрации спама в SMS (SSFM) и модуль управления услугой пользователя (USMM). SSFM осуществляет фильтрацию спама в SMS, в то время как USMM осуществляет управление правилами фильтрации и управление отфильтрованными короткими сообщениями.

7.2.2.1 Модуль фильтрации спама в SMS (SSFМ)

SSFМ – основной элемент системы фильтрации, который обрабатывает запросы о фильтрации, поступающие от SCM, определяет, является ли короткое сообщение спамом или нет в соответствии с правилами фильтрации, хранящимися в базе данных правил фильтрации, определяемых пользователем, (URD), и затем передает принятое решение в SMSC. Если короткое сообщение является спамом, то оно будет сохранено в базе данных отфильтрованных сообщений (FMD) для дальнейшего управления (запроса, удаления и восстановления); в ином случае, короткое сообщение будет доставлено получателю обычным способом.

Кроме того, в этом модуле должны быть приняты во внимание протоколы интерфейсов между SCM, URD, FMD и SSFМ.

Протокол интерфейса между SSFМ и SCM: SSFМ получает от SCM аутентификационное сообщение, содержащее исходное короткое сообщение, и передает в SCM результаты аутентификации.

Протокол интерфейса между SSFМ и URD: SSFМ получает от URD правила фильтрации, определяемые пользователем.

Протокол интерфейса между SSFМ и FMD: SSFМ сохраняет отфильтрованное короткое сообщение в FMD, чтобы определить, является ли оно спамом.

7.2.2.2 Модуль управления услугой пользователя (USMM)

Модуль USMM используется пользователями для управления правилами фильтрации и отфильтрованными короткими сообщениями. При помощи USMM пользователи могут добавлять, удалять, редактировать и запрашивать правила фильтрации. В то же время при помощи USMM пользователи могут запросить, удалить и восстановить отфильтрованные короткие сообщения. USMM должен поддерживать, по крайней мере, один из следующих методов управления: метод управления через SMS, метод управления через веб-интерфейс и метод управления через диспетчерскую станцию (SS).

Кроме того, в этом модуле во внимание должны быть приняты протоколы интерфейсов между SCM, URD, FMD и USMM.

Протокол интерфейса между USMM и SCM: USMM получает от пользователей через SCM короткое сообщение, которое содержит инструкции управления, касающиеся правил фильтрации и отфильтрованных коротких сообщений, и передает результаты пользователю через SCM.

Протокол интерфейса между USMM и URD: USMM передает URD инструкции управления (добавление, удаление, изменение или запрос правил фильтрации) и получает от URD соответствующую информацию.

Протокол интерфейса между USMM и FMD: USMM передает FMD инструкции управления (восстановление, удаление или запрос отфильтрованных коротких сообщений) и получает от FMD соответствующую информацию.

7.2.3 Уровень данных

Уровень данных отвечает, главным образом, за хранение правил фильтрации и отфильтрованных коротких сообщений. Эти данные должны храниться на постоянных запоминающих устройствах, таких как диски, кассеты и т. д., в формате базы данных или текстовом формате. Кроме того, данные могут быть перенесены и удалены. Если размер файлов данных превышает допустимый предел хранения, система фильтрации должна немедленно оповестить операторов даже при автоматическом создании резервной копии данных.

7.2.3.1 База данных отфильтрованных сообщений (FMD)

FMD используется для хранения коротких сообщений, которые были отфильтрованы SSFМ как спам. Время их хранения может быть указано пользователем. Без четкого определения времени хранения, отфильтрованные короткие сообщения должны храниться в течение, как минимум, 3 месяцев.

Должны быть приняты во внимание протоколы интерфейсов от FMD к SSFМ и к USMM.

7.2.3.2 База данных определяемых пользователем правил (URD)

База данных URD используется для хранения правил фильтрации, определяемых пользователем. Правила фильтрации, определяемые пользователем, могут основываться на адресе, времени и содержании. Обязательно наличие черных списков, основанных на адресе, а белые списки, основанные на адресе, не являются обязательными.

Следует принять во внимание протоколы интерфейсов от URD к SSFM и к USMM.

7.3 Требования к устройству

SCM, SSFM, USMM, FMD, URD – это логические модули системы фильтрации. Они могут устанавливаться как независимые устройства или объединяться в одно или несколько устройств. Для крупного центра коротких сообщений (SMSC) рекомендуется выбивать первый способ в целях улучшения качественных показателей и расширяемости. Кроме того, для полноты системы очень важны функция управления системой и функция проверки записей в журнале загрузок.

8 Функция фильтрации спама в SMS

8.1 Режимы работы SMS

Услуги передачи коротких сообщений "из пункта в пункт" состоят из двух основных услуг:

- SM MT (передача короткого сообщения на мобильное устройство "из пункта в пункт");
- SM MO (передача короткого сообщения с мобильного устройства "из пункта в пункт").

SM MT обозначает возможность передачи короткого сообщения от SMSC на MS получателя и предоставления информации о доставке короткого сообщения либо в виде отчета о доставке, либо в виде отчета о том, что сообщение не доставлено, с определенным механизмом отложенной доставки (см. рисунок 2).

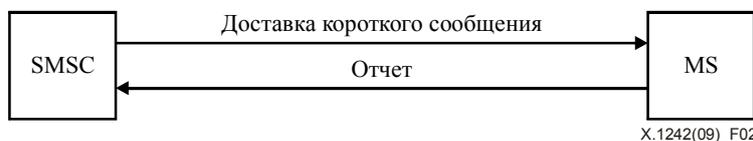


Рисунок 2 – Передача короткого сообщения на мобильное устройство "из пункта в пункт"

SM MO обозначает возможность передачи короткого сообщения от MS отправителя к одному SME через SMSC и предоставления информации о доставке короткого сообщения либо в виде отчета о доставке, либо в виде отчета о том, что сообщение не доставлено. Сообщение должно содержать адрес того SME, которому SMSC должен в результате попытаться передать короткое сообщение (см. рисунок 3).

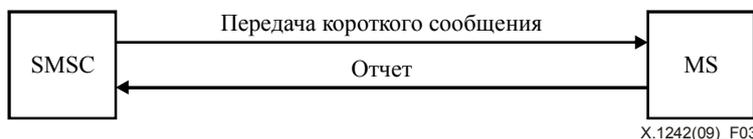


Рисунок 3 – Передача короткого сообщения с мобильного устройства "из пункта в пункт"

Однако после SM MO доставка SMS на MS получателя может осуществляться в двух режимах. В первом режиме после SM MO короткое сообщение будет доставлено напрямую на MS получателя. Во втором режиме после SM MO короткое сообщение будет передано в SMSC на стороне получателя при помощи некоторого механизма связи (т. е. с использованием протокола SMPP, реализованного в IP-сети) и затем доставлено на MS получателя. Несмотря на то что пользователи не ощущают разницы между различными режимами работы по доставке SMS, варианты практической реализации

системы фильтрации в обоих режимах имеют множество различий. Для простоты первый режим работы называется режимом доставки на стороне отправителя, а второй режим работы называется режимом доставки на стороне получателя.

8.2 Реализация фильтрации спама в SMS

Фильтрация спама в SMS – это вид услуги для оформивших подписку получателей, которая обеспечивает получателям возможности по конфигурации правил фильтрации, определяемых пользователем, и возможности по управлению отфильтрованными короткими сообщениями. Правила фильтрации, определяемые пользователями, и отфильтрованные короткие сообщения обычно хранятся в URD и в FMD, установленных на стороне получателя.

В режиме доставки на стороне получателя управление правилами фильтрации, управление отфильтрованными короткими сообщениями и доставка коротких сообщений осуществляются на стороне получателя. Таким образом, система фильтрации в режиме доставки на стороне получателя будет легко реализована, поскольку в изменении нуждаются только устройства на стороне получателя.

В режиме доставки на стороне отправителя, доставка коротких сообщений осуществляется в SMSC на стороне отправителя, в то время как управление правилами фильтрации и отфильтрованными короткими сообщениями выполняется в URD и в FMD, установленных на стороне получателя. Таким образом, требуются механизмы синхронизации между системами фильтрации спама в SMS на стороне отправителя и на стороне получателя. Как правило, короткие сообщения передаются в систему фильтрации на стороне получателя до процесса фильтрации. По сути, реализовать систему фильтрации в режиме доставки на стороне отправителя сложнее, чем в режиме доставки на стороне получателя из-за необходимости механизмов синхронизации.

8.2.1 Реализация фильтрации спама в SMS в режиме доставки на стороне получателя

В режиме доставки на стороне получателя модули SCM, SSFM и USMM можно располагать на стороне получателя, не задействуя устройства или модули на стороне отправителя, см. рисунок 4.

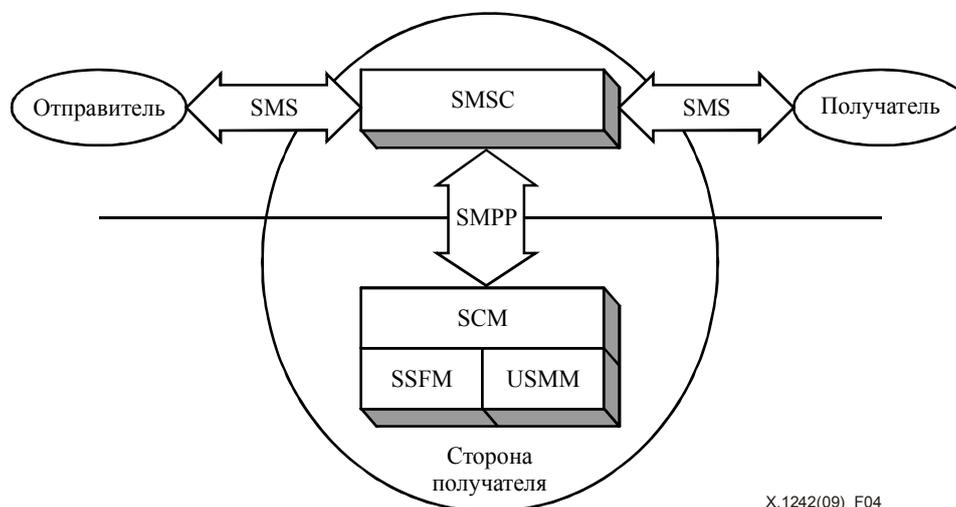


Рисунок 4 – Фильтрация спама в SMS в режиме доставки на стороне получателя

Процесс работы показан на рисунке 5:

- После получения короткого сообщения от отправителя SMSC передает в SCM аутентификационное сообщение SMPP, содержащее исходное короткое сообщение;
- SCM делает запрос относительно подписки на услугу, имеющейся у получателя короткого сообщения. Если получатель подписан на услугу, короткое сообщение передается в модуль SSFM; в ином случае, короткое сообщение доставляется обычным способом;

- SSFM проверяет, является ли короткое сообщение допустимым согласно правилам фильтрации, определенным получателем. Если короткое сообщение соответствует установленным правилам, то система фильтрации должна доставить короткое сообщение получателю, а в SMSC передается сообщение SMPP с положительным ответом; если короткое сообщение является недопустимым, система фильтрации спама в SMS должна заблокировать короткое сообщение и сохранить его в FMD для будущего управления (запроса, удаления и восстановления).

Поскольку количество одновременно обрабатываемых SMS может быть большим, и процесс фильтрации, возможно, займет долгое время, в SMSC необходим таймер, не допускающий потерю и задержку SMS. Если SMSC не может получить ответ SMPP в течение определенного времени, заданного таймером, то короткое сообщение доставляется обычным способом. Обычно время задает оператор сети или оператор, предоставляющий услугу.

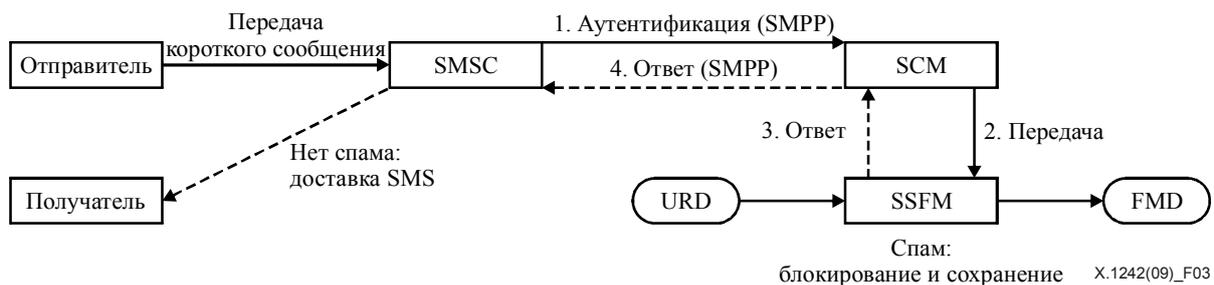


Рисунок 5 – Процессы, происходящие в системе фильтрации спама в SMS в режиме доставки на стороне получателя

8.2.2 Реализация фильтрации спама в SMS в режиме доставки на стороне отправителя

В режиме доставки на стороне отправителя модули SCM, SSFM и USMM могут быть расположены только на стороне отправителя, поскольку доставка коротких сообщений осуществляется на стороне отправителя. Поэтому следует предусмотреть некоторые механизмы синхронизации между системами фильтрации спама в SMS на стороне отправителя и на стороне получателя. Как правило, короткие сообщения передаются в систему фильтрации на стороне отправителя для продолжения процесса фильтрации, приведенного ниже (см. рисунок 6).

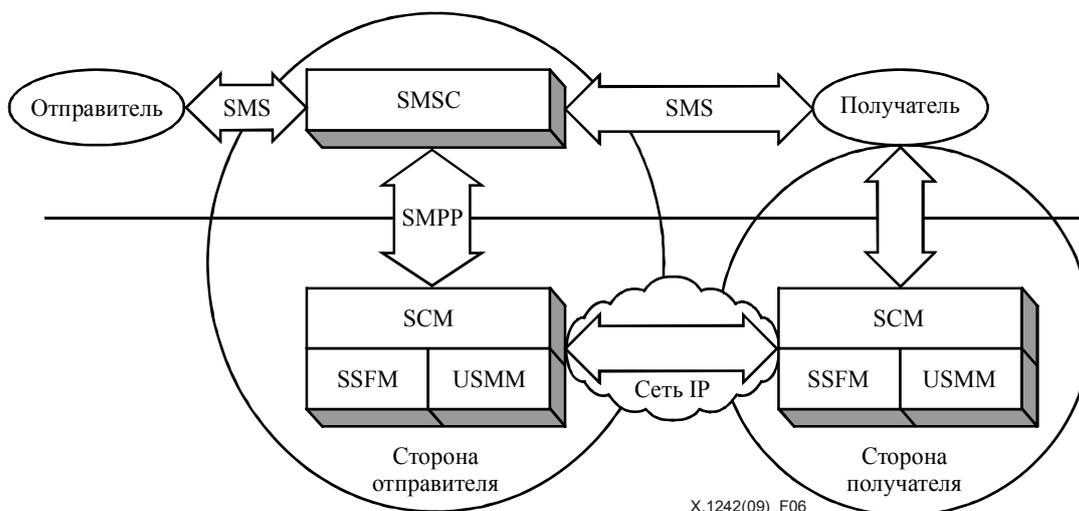


Рисунок 6 – Фильтрация спама в SMS в режиме доставки на стороне отправителя

Процесс работы показан на рисунке 7:

- После получения короткого сообщения от отправителя, SMSC передает в SCM на стороне отправителя аутентификационное сообщение SMPP, содержащее исходное короткое сообщение;
- SCM на стороне отправителя делает запрос относительно статуса подписки на услугу, имеющейся у получателя короткого сообщения. Если получатель подписан на услугу, то короткое сообщение передается в SSFM на стороне отправителя; в противном случае, короткое сообщение доставляется получателю обычным способом;
- SSFM на стороне отправителя передает короткое сообщение в модуль SSFM на стороне получателя. Затем SSFM на стороне получателя определяет, является ли короткое сообщение допустимым согласно правилам фильтрации, определенным получателем и хранящимся в URD. Если короткое сообщение соответствует установленным правилам, то система фильтрации доставляет короткое сообщение получателю, а в SMSC передается сообщение SMPP с положительным ответом; если короткое сообщение является недопустимым, то система фильтрации спама в SMS должна заблокировать короткое сообщение и сохранить его в FMD на стороне получателя для будущего запроса.



Рисунок 7 – Процессы фильтрации спама в SMS в режиме доставки на стороне отправителя

Поскольку количество одновременно обрабатываемых SMS может быть большим, и процесс фильтрации, возможно, займет долгое время, в SMSC необходим таймер, не допускающий потерю и задержку SMS. Если SMSC не может получить ответ SMPP в течение определенного времени, заданного таймером, то короткое сообщение доставляется обычным способом. Обычно время задает оператор сети или оператор, предоставляющий услугу.

9 Управление услугой со стороны пользователя

9.1 Методы управления

Система фильтрации спама в SMS должна предоставить пользователям метод управления через SMS и через веб-интерфейс. Кроме того, в зависимости от практических условий работы сети, например, в зависимости от того, есть ли специально обученные люди, которые могут делать эту работу, может быть применен метод управления через диспетчерскую станцию.

9.1.1 Метод управления через SMS

Пользователи могут управлять определяемыми ими правилами фильтрации и отфильтрованными короткими сообщениями через SMS с помощью объекта короткого сообщения (SME), включенного в USMM в качестве поставщика услуги (SP).

С одной стороны, SME может получать и распознавать SMS с включенными в сообщение инструкциями управления; с другой стороны, SME может передавать инструкции управления в USMM, а USMM может управлять определяемыми пользователями правилами фильтрации и отфильтрованными короткими сообщениями согласно полученным от пользователей инструкциям управления. Этот метод показан на рисунке 8.

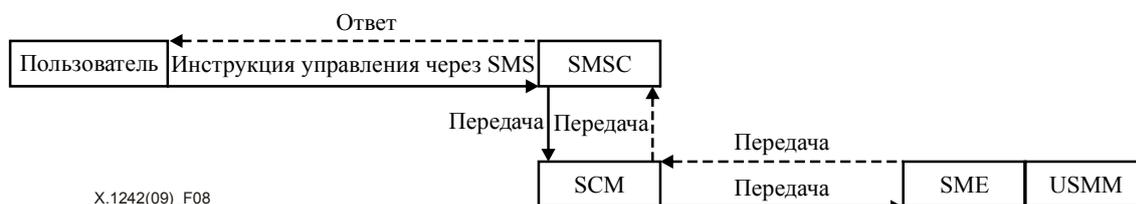


Рисунок 8 – Управление с помощью короткого сообщения

Если пользователи хотят управлять определяемыми ими правилами фильтрации и отфильтрованными короткими сообщениями, то единственное, что должны сделать пользователи, это послать SMS с включенными в него инструкциями управления на определенный номер SME для доступа. Далее, SME должна выполнить эти задачи.

Размер короткого сообщения слишком ограничен (как правило, максимум 160 символов), для того чтобы оно могло содержать достаточно информации. Помимо этого, фактически все оконечные устройства с функцией SMS – это мобильные телефоны, и, как правило, их размеры малы. Поскольку размер экрана ограничен, вводить данные с клавиатуры или просматривать большие объемы данных на экране очень трудно. По этой причине управлять правилами фильтрации и отфильтрованными короткими сообщениями через оконечные устройства с функциями SMS нелегко. Тем не менее, поскольку оконечные устройства с функциями SMS обычно всегда находятся около пользователей, этот способ обладает определенными достоинствами, позволяя пользователям применять одно данное оконечное устройство для управления определяемыми ими правилами фильтрации и отфильтрованными короткими сообщениями, наряду с отправкой и получением коротких сообщений.

9.1.2 Метод управления через веб-интерфейс

Пользователи могут управлять определяемыми ими правилами фильтрации и отфильтрованными короткими сообщениями при помощи веб-интерфейса через веб-сервер, добавленный в модуль USMM.

С одной стороны, веб-сервер может получать инструкции управления; с другой стороны, веб-сервер может направлять инструкции управления в USMM, а USMM может управлять правилами фильтрации, определяемыми пользователями, и отфильтрованными короткими сообщениями в соответствии с инструкциями управления. Этот метод показан на рисунке 9.

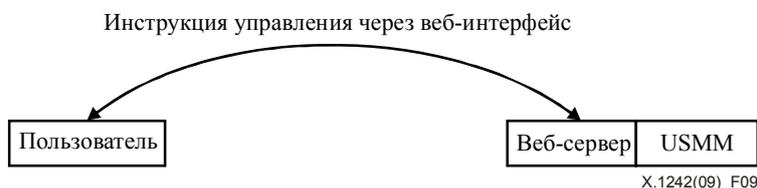


Рисунок 9 – Управление с помощью веб-интерфейса

Процесс работы аналогичен обычной работе в среде веб. Однако метод управления через веб-интерфейс поддерживает больше инструкций управления, чем метод управления с помощью короткого сообщения. С учетом соображений безопасности, метод управления через веб-интерфейс должен поддерживать протокол SSL/TLS (уровень безопасных соединений/безопасность на уровне транспортного протокола) для аутентификации веб-сервера и клиента и затем использовать его для кодирования сообщений между авторизованными сторонами. Фактически использование метода управления через веб-интерфейс является более эффективным, чем использование метода управления по SMS. Однако применение этого метода ограничено количеством точек доступа в интернет.

9.2 Возможности управления

9.2.1 Типы правил фильтрации, определяемых пользователем

Поскольку система фильтрации работает, основываясь на определяемых пользователем правилах, то правила фильтрации весьма важны для системы фильтрации. На практике правила фильтрации могут быть основаны на адресе, времени и содержании.

- *Правило фильтрации, основанное на адресе*

Правило фильтрации, основанное на адресе, определяет, является ли короткое сообщение спамом или нет на базе адреса источника (номера телефона). Существуют два типа правил фильтрации, основанные на адресе: белые списки разрешенных отправителей и черные списки пользователей, подозреваемых в рассылке спама. На практике все короткие сообщения из белых списков доставляются в обычном режиме без дальнейшей проверки; все короткие сообщения из черных списков незамедлительно блокируются. Белые/черные списки могут содержать не только отдельные номера, но и части телефонного номера. Однако белые/черные списки, особенно черные списки, неизбежно будут содержать неточности, известные как ситуации ложного положительного распознавания и ситуации ложного отрицательного распознавания. Тем не менее, фильтрация, основанная на адресе, наиболее эффективна и удобна для борьбы со спамом в SMS. Поэтому, несмотря на то что в методе с использованием белых/черных списков часто принимаются слишком жесткие решения, для большинства пользователей он наиболее приемлем, все же фильтрация, основанная на адресе, является важным правилом фильтрации в системе фильтрации.

- *Правило фильтрации, основанное на времени*

Правило фильтрации, основанное на времени, ограничивает доставку коротких сообщений в определенное время. Таким образом, заблокированные сообщения, которые содержатся в FMD, могут не быть спамом. Как правило, пользователи не хотят получать короткие сообщения ночью, на некоторых совещаниях или в какой-либо другой важный момент, так что они могут использовать правило фильтрации, основанное на времени. В правиле, основанном на времени, пользователи могут задать временной интервал, когда они не хотят получать короткие сообщения. Однако пользователи могут выбрать опцию, определяющую дальнейшие действия с короткими сообщениями, которые были заблокированы по правилу, основанному на времени, по истечении заданного временного интервала: сделать повторную передачу или нет.

- *Правило фильтрации, основанное на содержании*

Фильтрация, основанная на содержании, является наиболее разумным методом фильтрации. Однако правильность фильтрации, основанной на содержании, обычно ниже, чем у других методов фильтрации. Это связано с трудностями обработки лингвистической информации с использованием фильтрации, основанной на содержании. Фактически фильтрация, основанная на ключевых словах, является наиболее полным методом фильтрации, основанной на содержании. В системе фильтрации, правила фильтрации, основанные на ключевых словах, являются обязательными. В то же время система фильтрации должна поддерживать следующие методы соответствия для правил фильтрации, основанных на ключевых словах: точное соответствие и неточное соответствие.

- *Правило смешанной фильтрации*

Фактически правила фильтрации всегда совмещаются. Поэтому к приоритету в правилах фильтрации следует подходить обдуманно. На практике приоритет может быть определен на основе регулирования услуги оператором и практическими требованиями пользователей.

9.2.2 Управление определяемыми пользователем правилами фильтрации

Пользователь может осуществлять следующее управление правилами фильтрации:

- Подключать и отключать заранее заданные правила фильтрации, определенные операторами услуги.

В целях упрощения управления правилами фильтрации для пользователей, операторы услуги должны создавать черные списки или ссылаться на уже известные. Таким образом, пользователи могут использовать такие заранее известные правила фильтрации.

- Управление правилами фильтрации, основанными на адресе, времени и содержании. Пользователи могут добавлять, удалять и запрашивать правила фильтрации. Однако пользователи по-разному относятся к различным методам управления. В методе управления через SMS пользователи могут управлять правилами фильтрации только с помощью одного короткого сообщения для одной инструкции управления, что довольно сложно в реальном применении, в то время как в методе управления через веб-интерфейс пользователи могут очень легко управлять правилами фильтрации.

9.2.3 Формат отфильтрованных коротких сообщений

Любые отфильтрованные короткие сообщения должны храниться в FMD с подробным отчетом. Отчет должен включать в себя, по меньшей мере, следующие позиции:

- отправитель: номер телефона отправителя;
- получатель: номер телефона получателя;
- время: время передачи короткого сообщения;
- содержание: содержание короткого сообщения;
- тип фильтрации: основанный на адресе, основанный на ключевых словах, основанный на времени.

9.2.4 Управление отфильтрованными короткими сообщениями

Пользователи могут управлять отфильтрованными короткими сообщениями. Они могут проводить следующие операции:

- создавать статистику отфильтрованных коротких сообщений;
- просматривать подробные данные об отфильтрованных коротких сообщениях;
- запрашивать отфильтрованные короткие сообщения;
- восстанавливать некоторые отфильтрованные короткие сообщения;
- удалять определенные отфильтрованные короткие сообщения.

10 Протоколы связи

10.1 Структуры протоколов связи

Существует 8 протоколов интерфейса в системе фильтрации (последний используется только для системы фильтрации в режиме доставки на стороне отправителя):

- интерфейс между SMSC и SCM;
- интерфейс между SCM и SSFM;
- интерфейс между SCM и USMM;
- интерфейс между SSFM и URD;
- интерфейс между SSFM и FMD;
- интерфейс между USMM и URD;
- интерфейс между USMM и FMD;
- интерфейс между SSFM на стороне отправителя и на стороне получателя.

Первые три протокола интерфейса – это внешние интерфейсы, которые используются, главным образом, для взаимодействия между различными модулями в одной сети или в разных сетях. Последние пять протоколов интерфейса – это внутренние интерфейсы, которые могут быть разработаны в соответствии с практическими потребностями поставщиков услуг и которые обычно невидимы для внешних интерфейсов.

Как правило, между SMSC и SCM может быть использован протокол аутентификации SMPP. Протокол ISMG может быть использован между SCM и SSFM, а также между SCM и USMM.

Кроме того, следует учитывать взаимосвязь SMS.

10.2 Протокол аутентификации

Протокол аутентификации должен быть основан на расширенном протоколе SMPP (см. [ETSI TR 101 632]). В системе фильтрации спама в SMS используются два сообщения: DELIVER_SM и DELIVER_SM_RESP. Процесс работы показан на рисунке 10.

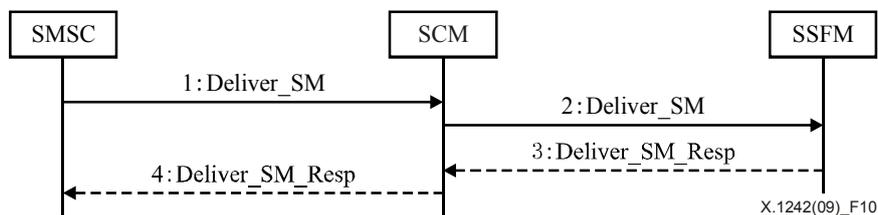


Рисунок 10 – Протокол аутентификации SMPP

DELIVER_SM выдается SMSC или SCM. Используя эту команду, SMSC или SCM могут передать короткое сообщение SCM или SSFM для его доставки.

DELIVER_SM_RESP выдается в качестве ответа на DELIVER_SM с пометкой о том, является ли успешной доставка. Значение параметра DELIVER_SM_RESP может быть разным: 0 указывает на успешную доставку; другие значения указывают на то, что доставка не удалась.

10.3 Протокол ISMG

Протокол ISMG позволяет пользователям формировать определяемые ими правила фильтрации и управлять отфильтрованными короткими сообщениями. Объект короткого сообщения (SME) добавляется в модуль управления услугой пользователя (USMM), с помощью которого пользователи могут управлять правилами фильтрации и отфильтрованными короткими сообщениями, хранящимися в FMD. Межсетевой протокол SMS используется между SMSC и SME. Процесс работы показан на рисунке 11.

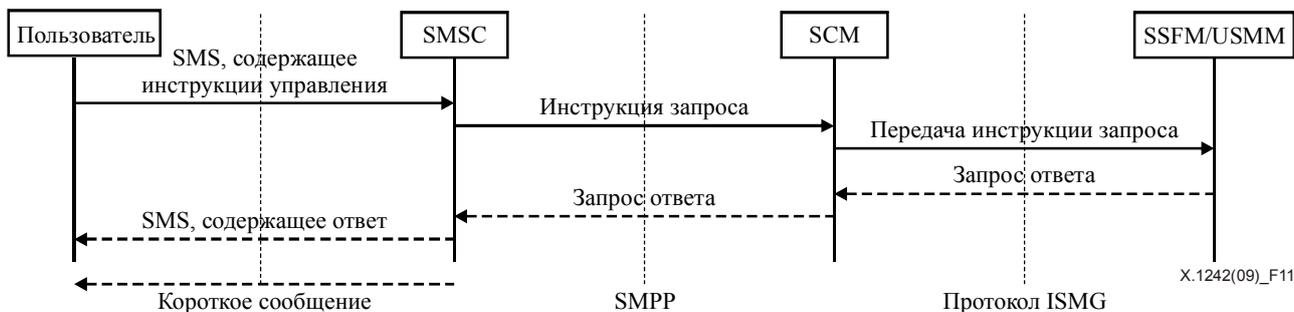


Рисунок 11 – Протокол ISMG

Дополнение I

Требования к программному обеспечению оконечных устройств, поддерживающему фильтрацию спама в SMS

(Настоящее Дополнение не является неотъемлемой частью настоящей Рекомендации)

Настоящее Дополнение применяется для интеллектуальных оконечных устройств.

I.1 Основные характеристики

Почти все оконечные устройства с функцией SMS – это мобильные телефоны, которые, как правило, невелики, имеют ограниченный по размерам экран и маленькую клавиатуру. Поэтому пользователям довольно сложно управлять правилами фильтрации и отфильтрованными короткими сообщениями, используя текстовые команды. Для того чтобы облегчить управление, на основе интеллектуальных оконечных устройств разработано программное обеспечение оконечных устройств, поддерживающее фильтрацию спама в SMS. В основном это программное обеспечение предоставляет пользователям меню операций, где инструкции управления отражаются в пунктах меню. При этом программное обеспечение оконечных устройств должно отвечать двум основным требованиям:

- полное управление правилами фильтрации и отфильтрованными сообщениями;
- понятный и удобный для пользователя интерфейс между пользователем и устройством.

На практике существует два типа программного обеспечения оконечных устройств:

- Основное программное обеспечение для фильтрации спама в SMS.
Функция фильтрации спама в SMS реализована в системе фильтрации, связанной с SMSC. Программное обеспечение оконечных устройств обеспечивает для пользователей только удобный интерфейс между пользователем и устройством.
- Расширенное программное обеспечение для фильтрации спама в SMS.
Программное обеспечение оконечных устройств обладает всеми функциональными модулями системы фильтрации спама в SMS, которые могут самостоятельно отфильтровывать спам в SMS. Как правило, расширение программного обеспечения включает все функции основного программного обеспечения.

I.2 Основное программное обеспечение для фильтрации спама в SMS

I.2.1 Конфигурация правил фильтрации

Должны быть предусмотрены следующие рабочие функции, см. таблицу I.1.

Таблица I.1 – Управление правилами фильтрации

Предварительно определенные правила фильтрации	Загрузка предварительно определенных правил фильтрации
	Отключение предварительно определенных правил фильтрации
Правила фильтрации, основанные на адресе	Добавление пунктов в белый список
	Удаление пунктов из белого списка
	Добавление пунктов в черный список
	Удаление пунктов из черного списка
Правила фильтрации, основанные на ключевых словах	Запрос правил фильтрации, основанных на адресе
	Добавление ключевых слов
	Удаление ключевых слов
	Запрос правил фильтрации, основанных на ключевых словах

Таблица I.1 – Управление правилами фильтрации

Правила фильтрации, основанные на времени	Добавление правил, основанных на времени
	Удаление правил, основанных на времени
	Запрос правил фильтрации, основанных на времени
Запрос всех правил фильтрации	
Удаление всех правил фильтрации, определенных пользователем	
Начало и конец фильтрации спама в SMS	

I.2.2 Конфигурация правил фильтрации

Таблица I.2 – Управление отфильтрованными короткими сообщениями

Составлять статистику отфильтрованных коротких сообщений
Просматривать детали отфильтрованных коротких сообщений
Запрашивать отфильтрованные короткие сообщения
Восстанавливать некоторые отфильтрованные короткие сообщения
Удалять определенные отфильтрованные короткие сообщения

I.3 Расширенное программное обеспечение для фильтрации спама в SMS

Если интеллектуальные оконечные устройства имеют хорошие ресурсы (например, возможности обработки, объем памяти и т. д.), то все функциональные модули могут быть установлены и внедрены в интеллектуальные оконечные устройства. В этом случае программное обеспечение, установленное на интеллектуальные оконечные устройства, обычно называют системой защиты SMS. Тем не менее, интеллектуальным оконечным устройствам по-прежнему необходим доступ в интернет для обновления программного обеспечения и заранее установленных правил фильтрации.

Библиография

- [b-ITU-T Q.1742.3] Recommendation ITU-T Q.1742.3 (2004), *IMT-2000 references (approved as of 30 June 2003) to ANSI-41 evolved core network with cdma2000 access network*.
- [b-ETSI TS 100 901] ETSI TS 100 901 V7.5.0 (2001-12), *Digital cellular telecommunications system (Phase 2+); Technical realization of the Short Message Service (SMS) Point-to-Point (PP) (3GPP TS 03.40 version 7.5.0 Release 1998)*.
http://pda.etsi.org/exchangefolder/ts_100901v070500p.pdf
- [b-ETSI TS 102 507] ETSI TS 102 507 V1.1.1 (2006-03), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Fixed network Short Message Service (F-SMS) for IP networks; Service description*.
http://pda.etsi.org/exchangefolder/ts_102507v010101p.pdf
- [b-ETSI TR 125 990] ETSI TR 125 990 V3.0.0 (2000-01), *Universal Mobile Telecommunications System (UMTS); Vocabulary*.
http://pda.etsi.org/exchangefolder/tr_125990v030000p.pdf
- [b-ETSI ES 201 986] ETSI ES 201 986 V1.1.2 (2002-01), *Services and Protocols for Advanced Networks (SPAN); Short Message Service (SMS) for PSTN/ISDN; Service description*.
http://pda.etsi.org/exchangefolder/es_201986v010102p.pdf

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