Международный союз электросвязи

МСЭ-Т X.1234

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(01/2022)

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

Безопасность киберпространства – Противодействие спаму

Руководящие указания по противодействию распространению спама с использованием услуг передачи мультимедийных сообщений

Рекомендация МСЭ-Т X.1234

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 (1)	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды (1)	X.1140–X.1149
Безопасность приложений (1)	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 (2)	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1319
Безопасность умных электросетей	X.1330–X.1339
Сертифицированная электронная почта	X.1340–X.1349
Безопасность интернета вещей (IoT)	X.1350–X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1399
Безопасность технологии распределенного реестра (DLT)	X.1400–X.1429
Безопасность приложений (2)	X.1450–X.1459
Безопасность веб-среды (2)	X.1470–X.1489
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
Киберзащита	X.1590–X.1599
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
КВАНТОВАЯ СВЯЗЬ	
Терминология	X.1700–X.1701
Квантовый генератор случайных чисел	X.1702–X.1709
Структура безопасности QKDN	X.1710–X.1711
Проектирование безопасности QKDN	X.1712–X.1719
Методы обеспечения безопасности QKDN	X.1720–X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	
Безопасность больших данных	X.1750–X.1759
Защита данных	X.1770–X.1789
БЕЗОПАСНОСТЬ СЕТЕЙ IMT-2020	X.1800–X.1819

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

Рекомендация МСЭ-Т X.1234

Руководящие указания по противодействию распространению спама с использованием услуг передачи мультимедийных сообщений

Резюме

В Рекомендации МСЭ-Т X.1234 содержатся руководящие указания по противодействию распространению спама с использованием MMS. В ней анализируются типичные сценарии, характеристики и методы распознавания MMS-спама, а также предоставлены техническая основа, рабочие процессы и некоторые ключевые технологии распознавания MMS-спама, которые помогут поставщикам и пользователям услуг MMS противодействовать спаму.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1234	07.01.2022 г.	17-я	11.1002/1000/14796

Ключевые слова

Услуга передачи мультимедийных сообщений, спам с использованием услуг передачи мультимедийных сообщений, техническая основа.

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

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним в целях 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/авторскими правами на программное обеспечение, 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 соответствующим базам данных МСЭ-Т, имеющимся на веб-сайте МСЭ-Т по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Введение

Услуга передачи мультимедийных сообщений (MMS) – это стандартный способ передачи сообщений, содержащих мультимедийный контент, на мобильный телефон и с мобильного телефона по сотовой сети. Пользователи и поставщики услуг могут подразумевать под такими сообщениями изображение, видеоизображение, звук, анимацию и т. д. С развитием технологий электросвязи и популярности смартфонов MMS стала основным способом передачи сообщений, особенно для молодежи и медиакомпаний, которые используют ее на коммерческой основе для доставки новостей и развлекательного контента. MMS служит удобным средством общения и передачи красочных сообщений, но также используется спамерами для рассылки MMS-спама. Такой MMS-спам, содержащий непрошенную рекламу, мошенническую информацию и вирусы, становится широко распространенной проблемой для операторов связи, поставщиков услуг и пользователей и приводит к значительной потере прибыли.

Поэтому разработка эффективной технологии противодействия MMS-спаму стала важным направлением в сфере противодействия спаму.

Рекомендация МСЭ-Т X.1234

Руководящие указания по противодействию распространению спама с использованием услуг передачи мультимедийных сообщений

1 Сфера применения

В настоящей Рекомендации предлагается техническая основа для противодействия MMS-спаму в целях обеспечения регулирования и контроля MMS-спама. Эта основа определяет функциональные компоненты, рабочие процессы и некоторые ключевые технологии распознавания MMS-спама. Кроме того, в настоящей Рекомендации рассматриваются типичные сценарии MMS-спама и анализируются различные типы и общие характеристики MMS-спама.

Стоит отметить, что все операции, описанные в этой Рекомендации, должны быть разрешены пользователями и административным регламентом. Весь процесс должен строго соответствовать применимому законодательству во избежание нарушения конфиденциальности пользователей.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы 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 справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

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

[ITU-T X.1247] Рекомендация МСЭ-Т X.1247 (2016 г.), *Техническая основа противодействия спаму при передаче сообщений на мобильные устройства.*

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 услуга передачи мультимедийных сообщений (multimedia messaging service (MMS)) [ITU-T X.1231]: Услугой передачи мультимедийных сообщений называется вид услуг передачи сообщений, появившийся после услуги передачи коротких сообщений (SMS), с помощью которой по сетям подвижной, беспроводной или фиксированной связи могут передаваться различные мультимедийные сообщения, включая текст, графические изображения, аудио-, видеосигналы и т. д.

3.1.2 спам с использованием услуг передачи мультимедийных сообщений (multimedia message service (MMS) spam) [ITU-T X.1247]: Спам, рассылаемый посредством MMS.

3.1.3 спамер (spammer) [ITU-T X.1231]: Спамером называется объект или лицо, создающие и отправляющие спам.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определен следующий термин.

3.2.1 функции обнаружения MMS-спама (MMS spam identification functions (MMSSIF)): Система противодействия MMS-спаму, которая не зависит от центра услуг передачи мультимедийных сообщений (MMSC) и включает в себя следующие функциональные компоненты: функцию мониторинга, функцию сбора данных, функцию предварительной обработки, функцию распознавания, функцию проверки, функцию удаления и функцию управления системой.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

ASR	Automatic Speech Recognition	Автоматическое распознавание речи
MMS	Multimedia Message Service	Услуга передачи мультимедийных сообщений
MMSC	Multimedia Message Service Centre	Центр услуг передачи мультимедийных сообщений
MMSSIF	Multimedia Messaging Service Spam Identification Function	Функция обнаружения спама с использованием услуг передачи мультимедийных сообщений
SMS	Short Message Service	Услуга передачи коротких сообщений
UICC	Universal Integrated Circuit Card	Универсальная карта с интегральной схемой
URL	Uniform Resource Location	Унифицированный указатель ресурсов

5 Соглашения

В настоящей Рекомендации используются следующие соглашения по терминологии.

Ключевое слово **"следует"** или **"должен"** (should) означает требование, которое рекомендуется, но не является абсолютно необходимым; таким образом для заявления о соответствии это требование не является обязательным.

Ключевое слово **"может"** (may) означает необязательное требование, которое допустимо, но не имеет рекомендательного значения.

В тексте настоящей Рекомендации иногда встречается слово **"может"** (can); в этом случае его следует понимать как **"имеется возможность"**.

6 Обзор

MMS – это вид услуги передачи сообщений, появившийся после услуги передачи коротких сообщений (SMS), с помощью которой по сетям подвижной связи или IP-сетям могут передаваться различные мультимедийные сообщения, включая текст, графические изображения, аудио-, видеосигналы и т. п. Благодаря быстро развивающимся технологиям электросвязи и интернет-технологиям, а также быстро растущей популярности смартфонов, MMS, обеспечивающая удобное средство общения и передачу красочных сообщений, представляет собой важный инструмент передачи сообщений, особенно для молодежи и медиакомпаний, которые используют ее на коммерческой основе для доставки новостей и развлекательного контента.

Однако MMS также позволяет спамерам рассылать MMS-спам. Такой MMS-спам, содержащий незапрашиваемую рекламу, мошенническую информацию, вирусы и другие нежелательные сообщения, становится широко распространенной проблемой для операторов связи, поставщиков услуг и пользователей и приводит к значительной потере прибыли. Поэтому поиск технических средств эффективной борьбы с MMS-спамом стал важной задачей в области противодействия спаму.

7 Сценарии и характеристика MMS-спама

Как показано на рисунке 7-1, процедура MMS состоит из трех основных этапов: 1) отправитель подготавливает содержание MMS и отправляет это MMS в MMSC, к которому относится его универсальная карта с интегральной схемой (UICC); 2) MMSC получает содержание MMS, отправленного отправителем, и решает, переслать ли это MMS в следующий центр MMS или отправить его непосредственно получателю; 3) получатель получает MMS от MMSC, который может отличаться от MMSC отправителя.

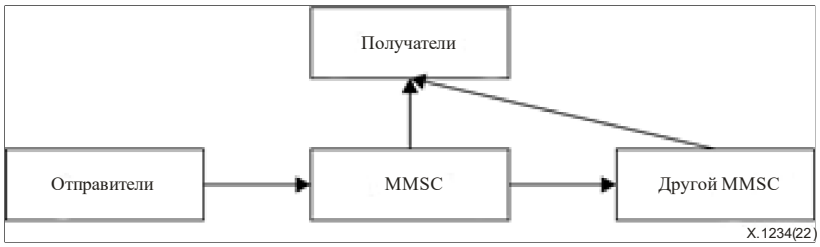


Рисунок 7-1 – Процедура MMS

Спамеры используют описанную выше процедуру для рассылки спама пользователям, что очень раздражает и может привести к потере выгоды для пользователей. Этот спам может включать в себя рекламу, мошенническую информацию и т. д. Ниже приведены некоторые типичные сценарии MMS-спама.

1 Мошеннический спам. Это MMS-спам, который заставляет получателя поверить, что он может получить какие-то выгоды или что нечто является правдой. Если получатель отвечает, как указано в сообщении, то с него взимается плата или его подписывают на какую-либо платную услугу мошеннической компании.

2 Троянский спам. Некоторые виды MMS-спама содержат медиафайл с "троянским конем", и если оказывается, что мобильный телефон уязвим и пользователь телефона открывает медиафайл, тот получает наивысшие права администратора системы телефона, после чего может без ведома получателя похитить из телефона всю секретную информацию.

3 Вирусный спам. MMS-спам может содержать файл определенного типа, который выглядит как обычный, но устанавливает вирус. Как только получатель выполняет установку, вирус начинает разрушать систему телефона разнообразными возможными способами, обычно путем быстрого удаления или дезагрегирования.

4 Нежелательная реклама. Рекламный MMS-спам обычно включает в себя разнообразную рекламу, такую как реклама услуг по предоставлению кредитов, продаже жилья, обучению и т. д. Этот спам рассылается получателям без их разрешения или подписки. Иногда он вводит в заблуждение и может содержать ссылку на рекламу в графическом или видео-MMS, и если получатель нажмет на изображение или видео, веб-браузер будет перенаправлен на страницу с рекламой.

8 Рекомендации по технической основе

8.1 Общая структура

Как показано на рисунке 8-1, отправитель отправляет MMS-сообщение в MMSC, а получатель загружает MMS-сообщение из MMSC, так что в MMSC хранятся все MMS-сообщения. По этой причине рекомендуется, чтобы функции обнаружения MMS-спама (MMSSIF) устанавливались рядом с MMSC.

При любой технологии противодействия спаму трудно гарантировать 100-процентную точность, и для MMSSIF также требуется автономная ручная настройка и управление, поэтому операторы услуг должны быть встроены в структуру, как показано на рисунке 8-1.

В то же время рабочий процесс исходного MMSC следует изменить таким образом, чтобы сразу после получения MMS-сообщения MMSC направлял его в MMSSIF, а не пересылал непосредственно получателю или в следующий MMSC. MMSSIF определяет, является ли MMS-сообщение спамом, и затем подает MMSC соответствующие предложения. На основе этих предложений MMSC решает, отправить ли это MMS-сообщение получателю или в следующий MMSC.

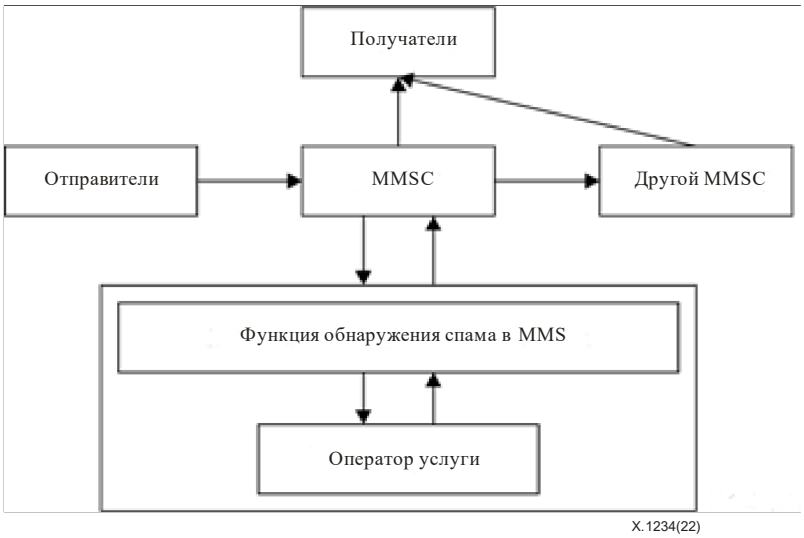


Рисунок 8-1 – Общая структура противодействия MMS-спаму

8.2 Эталонная структура MMSSIF

Эталонная структура MMSSIF состоит обычно из семи модулей, соответствующих различным функциям: мониторинг, сбор данных, предварительная обработка, распознавание, проверка, удаление и управление системой. Рекомендуется, чтобы разные модули были связаны между собой. Также им следует координировать свои действия друг с другом в соответствии с правилами или стратегиями, установленными соответствующими соглашениями.

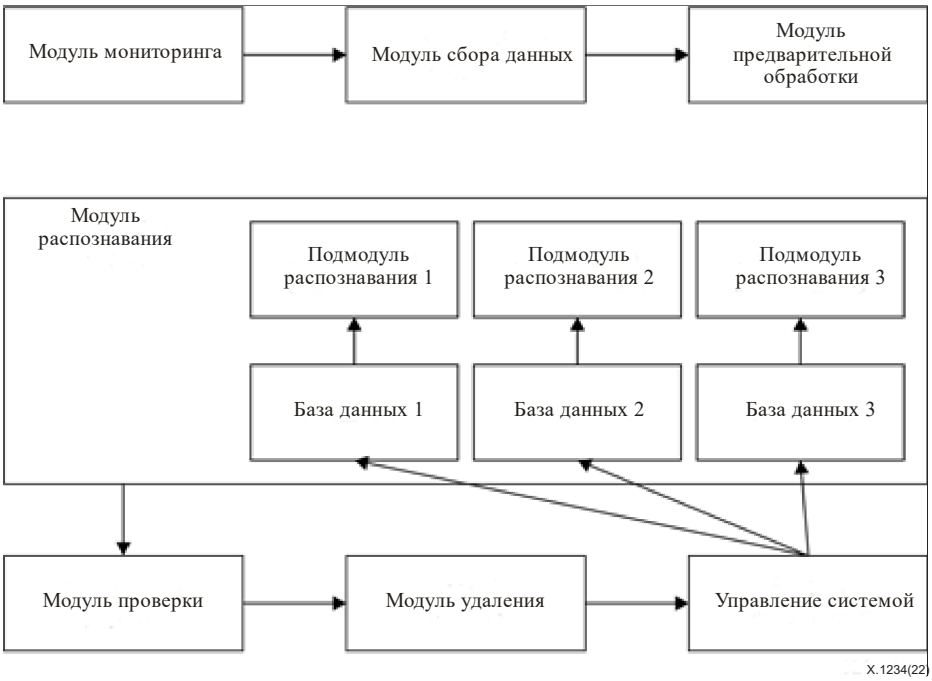


Рисунок 8-2 – Эталонная структура MMSSIF

На рисунке 8-2 модуль мониторинга принимает MMS от MMSC и получает заголовок этого MMS, содержащий тему, номер телефона отправителя, количество вложений, URL-адреса этих вложений и т. д.

Модуль сбора данных получает эти сообщения с заголовком MMS от модуля мониторинга и загружает все вложения с URL-адресов.

Модуль предварительной обработки получает от модуля сбора данных все сообщения, относящиеся к этому MMS, включая заголовок и все вложения, а затем нормализует сообщения по определенным правилам. Сообщения могут состоять из заголовка или тела MMS и могут быть текстом, изображением, видео- или аудиоданными и т. д. Поэтому рекомендуется использовать составные правила, такие как "источник + тип сообщения + сообщение".

Модуль распознавания получает от модуля предварительной обработки нормализованные сообщения и проверяет, не является ли это MMS спамом, с помощью специальных технологий, таких как черный список, распознавание текста, распознавание изображений, распознавание видеоизображения и т. д.

Модуль проверки получает от модуля распознавания вероятный результат и производит дальнейшую оценку, такую как ручное определение, чтобы уменьшить вероятность ложного срабатывания.

Модуль удаления получает от модуля проверки результат распознавания и удаляет MMS, оцененные как спам, например блокируя MMS, направляя спамерам предупредительное сообщение и т. д. Он также передает исходное MMS, журнал удалений и номер телефона отправителя в модуль управления системой.

Модуль управления системой получает информацию от модуля удаления и сохраняет журнал операций и журнал системных событий. Кроме того, он передает номер телефона спамера, ключевые слова и изображения в различные базы данных модуля распознавания для их обновления.

8.3 Функциональные компоненты MMSSIF

8.3.1 Модуль мониторинга

К функциям модуля мониторинга относятся:

- мониторинг поступления нового MMS от MMSC;
- прием всего потока данных MMS;
- анализ потока данных и извлечение заголовка MMS;
- передача темы, номера телефона отправителя, количества вложений, URL-адресов этих вложений и тела MMS в модуль сбора данных.

8.3.2 Модуль сбора данных

К функциям модуля сбора данных относятся:

- прием сообщений от модуля мониторинга и поиск URL-адресов соответствующих вложений;
- загрузка всех вложений;
- передача в модуль предварительной обработки всех сообщений, относящихся к этому MMS, включая заголовок и тело MMS со всеми вложениями.

8.3.3 Модуль предварительной обработки

К функциям модуля предварительной обработки относятся:

- прием всех сообщений от модуля сбора данных;
- проверка всех вложений и определение того, являются ли они текстом, изображением, аудио- или видеоданными, так как в соответствии с текущим транспортным протоколом MMS в них разрешено включать только текст, изображение, аудио- или видеоданные;
- классификация сообщений по типу и их нормализация по правилам, таким как составные правила "источник + тип сообщения + сообщение";
- передача исходного MMS, всех нормализованных сообщений и номера телефона отправителя в модуль распознавания.

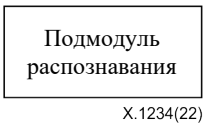
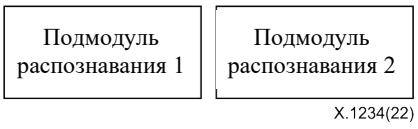
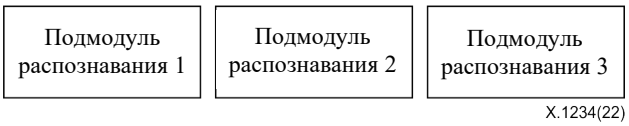
8.3.4 Модуль распознавания

К функциям модуля распознавания относятся:

- анализ MMS-сообщения на предмет того, является ли оно спамом;
- передача результата распознавания в модуль проверки.

Существует три основных вида технологий распознавания спама по разным частям MMS. Первый основан на анализе номера телефона – например, входит ли он в черный список или белый список. Второй основан на анализе текста – например, распознавание текста. Последний способ основан на анализе вложений – например, распознавание изображений, распознавание видеоизображения и т. д. В зависимости от конкретных требований и характеристик поставщика услуг в модуле распознавания могут быть установлены различные подмодули в зависимости от технологии.

Таблица 8-1 – Модели конфигурации модуля распознавания

Модель	Описание
Модель 0	 В модели 0 имеется только один подмодуль и используется технология распознавания одного типа.
Модель 1	 Модель 1 представляет собой схему из подмодуля 1 и подмодуля 2, соединенных между собой. Подмодуль 1 и подмодуль 2 – подмодули любых двух типов из трех.
Модель 2	 Модель 2 представляет собой схему из подмодуля 1, подмодуля 2 и подмодуля 3, соединенных между собой.

В модели 1 и модели 2 результат распознавания может рассчитываться по-разному. Например, в модели 1 подмодуль распознавания 1 выполняет распознавание текста, а подмодуль распознавания 2 – распознавание изображений. Подмодуль распознавания 1 может распознать MMS как спам, а подмодуль распознавания 2 – не распознать то же MMS как спам. Следовательно, для определения того, является ли данное MMS спамом, требуется общая стратегия модуля распознавания. Рекомендуется настроить такую стратегию в соответствии с реальными потребностями и ситуацией.

8.3.5 Модуль проверки

К функциям модуля проверки относятся:

- прием возможных результатов от модуля распознавания;
- дальнейшая оценка, например определение вручную.

8.3.6 Модуль удаления

К функциям модуля удаления относятся:

- прием результата от модуля проверки;
- удаление MMS, если в результате распознавания обнаружено, что MMS представляет собой спам;

- передача результата удаления в модуль управления системой, если MMS распознано как спам;
- передача исходного MMS в MMSC, если MMS не распознано как спам.

8.3.7 Модуль управления системой

К функциям модуля управления системой относятся:

- сохранение журнала операций и журнала системных событий;
- обновление баз данных;
- прием сообщений обратной связи от пользователей.

8.4 Эталонная модель

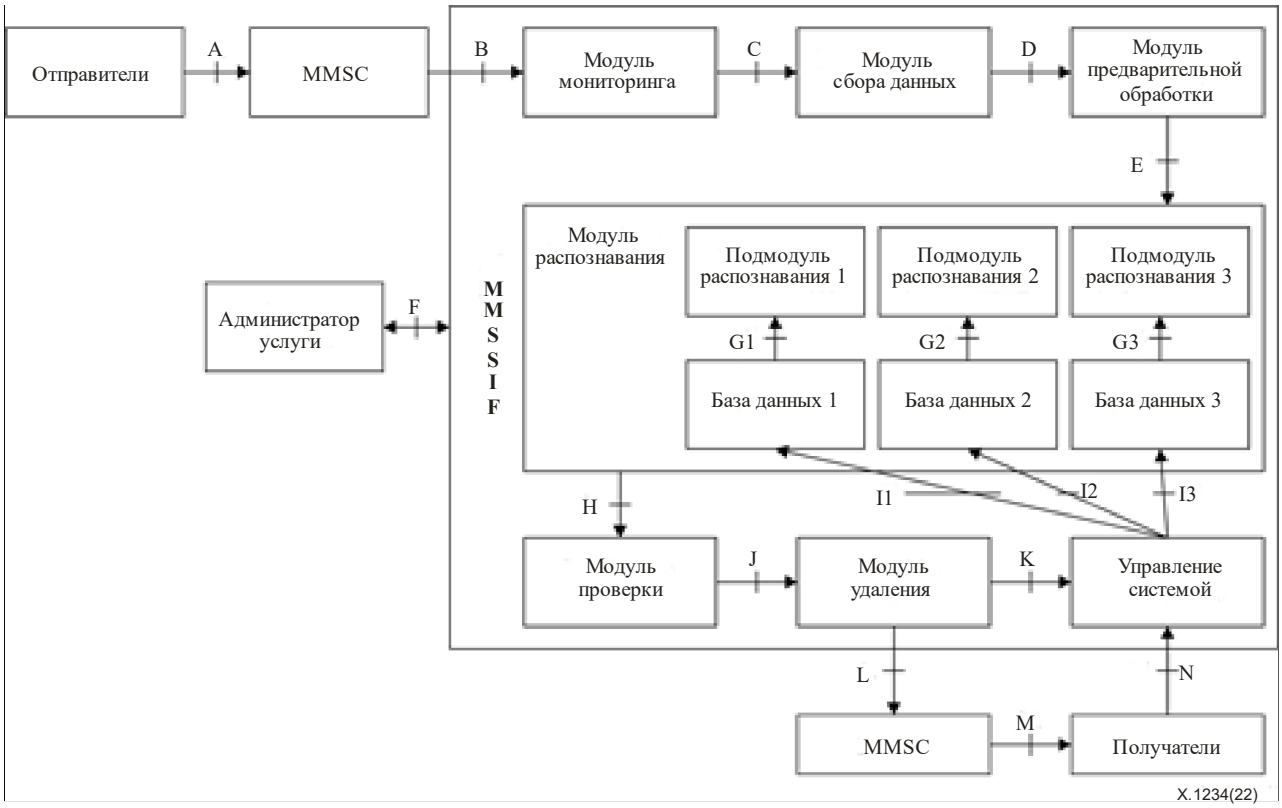


Рисунок 8-3 – Эталонная модель системы противодействия MMS-спаму

Интерфейс A расположен между отправителями и MMSC. Интерфейс A используется для передачи MMS в MMSC. На тот момент, когда поставщик услуг начал предоставлять услуги MMS пользователям, он уже был реализован. И менять его в этой модели не требуется.

Интерфейс B расположен между MMSC и модулем мониторинга. Интерфейс B – это новый интерфейс, который используется для передачи MMS в модуль мониторинга вместо того, чтобы пересылать их непосредственно получателю или в следующий MMSC.

Интерфейс C расположен между модулем мониторинга и модулем сбора данных. Интерфейс C используется для передачи заголовка MMS, номера телефона отправителя, URL-адресов и т. д., которые анализируются модулем мониторинга.

Интерфейс D расположен между модулем сбора данных и модулем предварительной обработки. Интерфейс D используется для передачи всех сообщений, включая заголовок MMS, тело MMS, тему, все вложения и т. д.

Интерфейс E расположен между модулем предварительной обработки и модулем распознавания. Интерфейс E используется для передачи нормализованных сообщений, например "источник + тип сообщения + сообщение". Интерфейс E должен поддерживать FTP и HTTP.

Интерфейс F расположен между оператором услуги и MMSSIF. Интерфейс F используется для передачи правил настройки и статистики спама.

Интерфейс G расположен между базой данных и подмодулем. Интерфейс G не является специальным интерфейсом. Он представляет собой класс интерфейсов, расположенных между разными базами данных и соответствующим подмодулем распознавания. Интерфейс G используется для передачи подозрительных номеров, текста, изображения и т. д., которые сопоставляются с базами данных для распознавания спама.

Интерфейс H расположен между модулем распознавания и модулем проверки. Интерфейс H используется для передачи возможного результата и исходного MMS.

Интерфейс I расположен между модулем управления системой и базой данных. Как и интерфейс G, интерфейс I не является специальным интерфейсом и представляет собой класс интерфейсов, расположенных между разными базами данных и модулем управления системой.

Интерфейс J расположен между модулем проверки и модулем удаления. Интерфейс J используется для передачи результата распознавания и исходного MMS.

Интерфейс K расположен между модулем удаления и модулем управления системой. Интерфейс K используется для передачи номера телефона отправителя, результата распознавания, сообщения об удалении и исходного MMS.

Интерфейс L расположен между модулем удаления и MMSC. Интерфейс L используется для передачи исходного MMS, не распознанного как спам.

Интерфейс M расположен между MMSC и получателями. Интерфейс M используется для передачи MMS получателям. На тот момент, когда поставщик услуг начал предоставлять услуги MMS пользователям, он уже был реализован, и менять его в этой модели не требуется.

Интерфейс N расположен между получателями и модулем управления системой. Интерфейс N используется для передачи получателями сообщений обратной связи.

9 Рабочие процедуры

На рисунке 9-1 показано, что противодействие MMS-спаму включает 12 процедур. Эти процедуры образуют адаптивную систему, способствующую оптимизации работы.

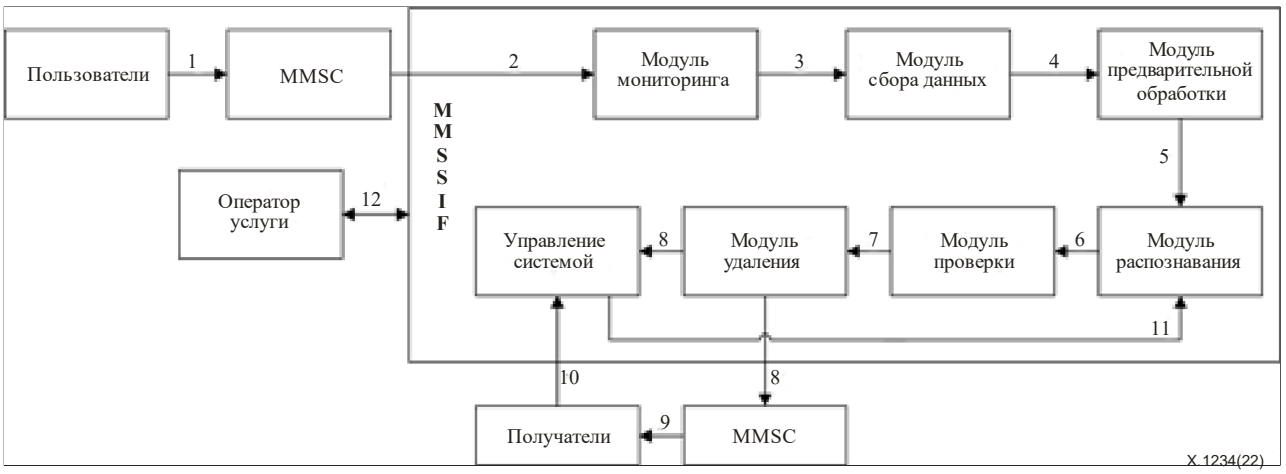


Рисунок 9-1 – Рабочие процедуры системы противодействия MMS-спаму

Процедура 1. Передача MMS в MMSC

Отправитель подготавливает содержание MMS, указывает номер телефона получателя и отправляет это MMS в MMSC.

Процедура 2. Пересылка MMS в модуль мониторинга

MMSC получает MMS-сообщение от MMSC и пересылает его непосредственно в модуль мониторинга.

Процедура 3. Получение заголовка MMS

Модуль мониторинга постоянно отслеживает поступление новых MMS от MMSC. Как только появляется новое MMS, он принимает весь поток данных MMS, анализирует этот поток и получает заголовок MMS, включая тему, номер телефона отправителя, количество вложений и URL-адреса этих вложений. Затем модуль мониторинга передает все сообщения в модуль сбора данных.

Процедура 4. Загрузка всех вложений

Модуль сбора данных получает сообщения от модуля мониторинга, находит URL-адреса этих вложений и загружает все вложения. Получив все сообщения, относящиеся к этому MMS, модуль сбора данных отправляет их в модуль предварительной обработки.

Процедура 5. Нормализация сообщений MMS

Получив сообщения от модуля сбора данных, модуль предварительной обработки проверяет все вложения и определяет, являются ли они текстом, изображением, аудио- или видеоданными. Если все сообщения допустимы, модуль предварительной обработки классифицирует их по типам и нормализует по установленным правилам. Затем он отправляет исходное MMS, все нормализованные сообщения и номер телефона отправителя в модуль распознавания.

Процедура 6. Анализ MMS

Модуль распознавания анализирует MMS на предмет спама в соответствии с технологиями, используемыми в конкретной системе. Затем модуль распознавания отправляет вероятный результат в модуль проверки. За исключением некоторых специальных технологий, модулю распознавания требуются общие методы получения окончательного вероятного результата.

Процедура 7. Дальнейший анализ

Получив вероятный результат от модуля распознавания, модуль проверки осуществляет дальнейший анализ и отправляет результат распознавания в модуль удаления.

Процедура 8. Удаление MMS

Модуль удаления принимает решение в отношении MMS в соответствии с результатом распознавания. Если MMS распознано как спам, модуль удаления удаляет его в соответствии с набором правил, например блокирует MMS, передает предупредительное сообщение спамерам и т. д. Он также передает в модуль управления системой исходное MMS, журнал удалений и номер телефона отправителя. Получатель не получит такое MMS. Если MMS не распознано как спам, модуль удаления передает исходное MMS в MMSC.

Процедура 9. Отправка MMS получателю

MMSC отправляет такое MMS получателю. Иногда он передает MMS в другой MMSC, а тот отправляет его получателю. Это та же процедура, что и раньше, когда функции MMSSIF не было.

Процедура 10. Отзывы получателей

Получатели – потенциальные жертвы спама, поэтому они могут по собственной инициативе отправить свой отзыв в модуль управления услугой. Участие получателей помогает эффективной и действенной борьбе со спамом. Поэтому рекомендуется, чтобы модуль управления системой использовал отзывы получателей при разработке решений или стратегий противодействия спаму.

Процедура 11. Обновление баз данных

Модуль управления системой хранит журнал операций, журнал системных событий и исходные MMS. Он также обновляет базы данных в соответствии с новыми образцами, номерами телефонов, ключевыми словами и т. д.

Процедура 12. Корректировка мер противодействия

На основании статистики спама и аналитического отчета MMSSIF оператор услуги оценивает качество работы MMSSIF на предмет внесения возможных усовершенствований. По результатам оценки меры и стратегии противодействия могут быть скорректированы, а оператор услуги может скорректировать механизмы взаимодействия в модуле распознавания.

10 Рекомендации по ключевым технологиям

MMS могут переносить различные мультимедийные сообщения, включая изображения, текст, видео- и аудиоданные и т. д. Таким образом ключевые технологии распознавания для противодействия MMS-спаму в основном включают в себя распознавание изображений, распознавание текста, распознавание видеоизображения, распознавание звука и т. д.

10.1 Список спам-фильтров

Список спам-фильтров включает в себя черный список, белый список и список подозрительных отправителей. Поставщикам услуг следует настроить MMSSIF на регистрацию подозрительной деятельности или, возможно, сделать так, чтобы она настраивалась автоматически на ведение черного или белого списка (блокируя подозрительные MMS или разрешая нормальные MMS). Поставщикам услуг также следует вести список для обеспечения доступности MMSSIF и продолжения ее стабильной работы. При обнаружении аномалий, когда номера телефона нет в списках, этот номер следует передать на ручную проверку для проведения полной оценки.

10.2 Распознавание изображений

При распознавании изображений сначала вызывается функция представления изображения и создается база данных собственных значений изображения. После этого обнаружение спама превращается в задачу двоичной классификации в пространстве признаков, которая может быть решена с помощью обычного машинного обучения. Или, проще говоря, если собственное значение изображения MMS-сообщения находит соответствие в базе данных, то сообщение распознается как спам. Этот метод зависит от качества базы данных собственных значений изображений.

10.3 Распознавание текста

Распознавание текста в основном состоит из распознавания ключевых слов и семантического распознавания. Сначала функция распознавания ключевых слов создает базу данных ключевых слов. Если текст MMS-сообщения содержит какие-либо ключевые слова, присутствующие в базе данных ключевых слов, то сообщение распознается как спам; кроме того, при распознавании текста могут создаваться модели на основе булевой логики и модель на основе векторного пространства. После обучения создается модель распознавания, способная повысить точность распознавания текста. Этот метод зависит от качества базы данных ключевых слов.

Иногда спамеры весьма изобретательно избегают обнаружения. Например, они могут фальсифицировать обычную электронную почту и рандомизировать контент, чтобы избежать обнаружения ключевых слов спам-фильтрами. Поэтому в алгоритме распознавания ключевых слов можно весьма эффективно и действенно использовать семантическое распознавание для достижения вторичного распознавания (например, подход к обработке естественного языка на основе нечеткого семантического распознавания), что позволит значительно снизить частоту ложноположительных результатов.

10.4 Распознавание видеоизображения

При распознавании видеоизображения обычно сначала создается база данных образцов спама, а затем видеоизображение из MMS последовательно сравнивается с этими образцами. Спам также можно идентифицировать, извлекая ключевые кадры видеоизображения. Основные операции включают следующее: декодирование видеоизображения, его обработку как набора статических изображений, а затем выборку из этих изображений, идентификацию выбранных изображений на основе технологии распознавания изображений и, наконец, получение результата распознавания видеоизображения с использованием результатов комплексного анализа этих выбранных статических изображений.

10.5 Распознавание звука

Распознавание звука может быть реализовано в сочетании с технологией автоматического распознавания речи (ASR). Цель технологии ASR – научить компьютер "диктовать" непрерывную речь или произносить ключевые слова или предложения голосом разных людей, и она способна преобразовывать речь в текст. Кроме того, чтобы идентифицировать похожие или одинаковые аудиоданные, извлекаются спектральные характеристики и вычисляются короткие и надежные "звуковые отпечатки пальцев". Таким образом ASR может распознавать некоторые определенные ключевые слова в аудиозаписях, которые позволяют определить, является ли аудиозапись спамом.

10.6 Отзывы конечных пользователей

Применяются отзывы конечных пользователей, соответствующие рекомендации по реализации, и другая информация, указанная в пункте 8.5 [ITU-T X.1231] и в Приложении A к [ITU-T X.1247].

Некоторые конечные пользователи, получая MMS-спам, часто сразу удаляют его, и лишь немногие сообщают об MMS-спаме в виде официального отзыва клиента. Эффективность этого метода зависит от желания и инициативы конечных пользователей. Для эффективного и действенного противодействия MMS-спаму следует поощрять активное участие конечных пользователей.

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.1241] Рекомендация МСЭ-Т X.1241 (2008 г.), *Техническая основа противодействия 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-ITU-T X.1245] Рекомендация МСЭ-Т X.1245 (2010 г.), *Структура противодействия спаму в мультимедийных IP-приложениях.*

[b-ITU-T X.1246] Рекомендация МСЭ-Т X.1246 (2015 г.), *Технологии, используемые в организациях электросвязи для противодействия голосовому спаму.*

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 протокола Интернет, сети последующих поколений, интернет вещей и умные города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2022 г.