



МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1241

(04/2008)

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

Безопасность электросвязи

**Техническая основа противодействия спаму,
рассылаемому по электронной почте**

Рекомендация МСЭ-Т X.1241

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X
СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	
Службы и услуги	X.1–X.19
Интерфейсы	X.20–X.49
Передача, сигнализация и коммутация	X.50–X.89
Сетевые аспекты	X.90–X.149
Техническое обслуживание	X.150–X.179
Административные предписания	X.180–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	
Модель и обозначение	X.200–X.209
Определения служб	X.210–X.219
Спецификации протоколов с установлением соединений	X.220–X.229
Спецификации протоколов без установления соединений	X.230–X.239
Проформы PICS	X.240–X.259
Идентификация протоколов	X.260–X.269
Протоколы обеспечения безопасности	X.270–X.279
Управляемые объекты уровня	X.280–X.289
Испытание на соответствие	X.290–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	
Общие положения	X.300–X.349
Спутниковые системы передачи данных	X.350–X.369
Сети, основанные на протоколе Интернет	X.370–X.379
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	
Организация сети	X.600–X.629
Эффективность	X.630–X.639
Качество обслуживания	X.640–X.649
Наименование, адресация и регистрация	X.650–X.679
Абстрактно-синтаксическая нотация 1 (ASN.1)	X.680–X.699
УПРАВЛЕНИЕ В ВОС	
Структура и архитектура управления системами	X.700–X.709
Служба и протокол связи для общего управления	X.710–X.719
Структура управляющей информации	X.720–X.729
Функции общего управления и функции ODMA	X.730–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	
Фиксация, параллельность и восстановление	X.850–X.859
Обработка транзакций	X.860–X.879
Удаленные операции	X.880–X.889
Общие приложения ASN.1	X.890–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ЭЛЕКТРОСВЯЗИ	X.1000–

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

Техническая основа противодействия спаму, рассылаемому по электронной почте

Резюме

В Рекомендации МСЭ-Т X.1241 приводится техническая основа противодействия спаму, рассылаемому по электронной почте. В рамках этой основы описывается одна из рекомендуемых структур домена антиспамовой обработки сообщений и определяются функции ее основных модулей. Главным в данной основе является то, что она устанавливает механизм обмена информацией о спаме, рассылаемом по электронной почте, между различными серверами электронной почты. Применение такой основы повысило бы эффективность всей совокупности взаимодействующих систем.

Источник

Рекомендация МСЭ-Т X.1241 утверждена 18 апреля 2008 года 17-й Исследовательской комиссией МСЭ-Т (2005–2008 гг.) в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

Ключевые слова

Антиспам, электронная почта, взаимодействие, спам, техническая основа.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи. 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 носит добровольный характер. Однако в Рекомендации могут содержаться определенные обязательные положения (например, для обеспечения возможности взаимодействия или применимости), и соблюдение положений данной Рекомендации достигается в случае выполнения всех этих обязательных положений. Для выражения необходимости выполнения требований используется синтаксис долженствования и соответствующие слова (такие, как "должен" и т.п.), а также их отрицательные эквиваленты. Использование этих слов не предполагает, что соблюдение положений данной Рекомендации является обязательным для какой-либо из сторон.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или реализация этой Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, обоснованности или применимости заявленных прав интеллектуальной собственности, независимо от того, отстаиваются ли они членами МСЭ или другими сторонами вне процесса подготовки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения этой Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что это 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. Никакая часть данной публикации не может быть воспроизведена с помощью каких-либо 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	1
4	Сокращения и акронимы	2
5	Соглашения о терминах	2
6	Общая структура домена антиспамовой обработки	2
	6.1 Общая структура	2
	6.2 Эталонная модель	4
7	Функции домена антиспамовой обработки	5
	7.1 Функции клиента электронной почты	5
	7.2 Функции сервера электронной почты	5
	7.3 Функции объекта антиспамовой обработки	6
	7.4 Функции подобъекта антиспамовой обработки	6
8	Выявление спама, рассылаемого по электронной почте	6
	8.1 Известные характерные особенности спама, рассылаемого по электронной почте	6
	8.2 Общие правила борьбы со спамом, рассылаемым по электронной почте	7
9	Методы противодействия спаму, рассылаемому по электронной почте	8
	9.1 Отключение функции открытой ретрансляции	8
	9.2 Совершенствование процедур проверки полномочий на доставку электронной почты	9
	9.3 Метод фильтрации	9
	9.4 Изучение возможности отслеживания	9
10	Взаимодействие между доменами антиспамовой обработки	10
	10.1 Взаимодействие между объектами обработки верхнего уровня	10
	10.2 Взаимодействие между объектом и подобъектом обработки	11
	10.3 Взаимодействие между подобъектом обработки и сервером электронной почты	11
	Библиография	12

Введение

С развитием сетей электросвязи, базирующихся на протоколе Интернет (IP), пользователи производят обмен электронной почтой в больших количествах. В то же время через интернет пользователям направляется все больше и больше спам-сообщений, что создает для них серьезные проблемы.

Спам, рассылаемый по электронной почте, превратился в бедствие, ухудшающее возможности оказания услуг в сетях электросвязи на базе IP. Поставщики услуг вынуждены тратить значительные средства для нейтрализации проблем, создаваемых спамом. Пользователям приходится тратить много времени, для того чтобы удалить спам, рассылаемый по электронной почте.

Был предложен ряд методов обнаружения и удаления спама, рассылаемого по электронной почте. Однако спамеры весьма изобретательно избегают обнаружения. Так, например, они могут фальсифицировать обычную электронную почту и рандомизировать содержимое, с тем чтобы избежать обнаружения спам-фильтрами. Поэтому необходимо срочно разработать эффективную техническую основу, для того чтобы противодействовать глобальной проблеме спама, рассылаемого по электронной почте.

Различные антиспамовые решения могут использовать различные методы противодействия спаму, рассылаемому по электронной почте. Эти антиспамовые технологии постоянно совершенствуются. Очень сложно найти какое-либо неизменяемое описание, которое в деталях охватывало бы антиспамовые технологии в долгосрочной перспективе.

Поэтому необходимо разработать открытую основу, содержащую эти различные решения. Эта основа должна быть совместимой со всеми антиспамовыми технологиями и не должна ограничиваться тем или иным техническим исполнением. К данной основе предъявляются следующие требования:

- Способность систематически оценивать, является или не является спамом то или иное электронное сообщение.
- Обеспечение для различных систем электронной почты возможности обмениваться друг с другом информацией, касающейся борьбы со спамом.
- Способность повысить точность антиспамовых инструментальных средств систем электронной почты.
- Обеспечение для объектов, относящихся к различным административным доменам, возможности обмениваться друг с другом информацией, касающейся противодействия спаму.

Техническая структура противодействия спаму, рассылаемому по электронной почте

1 Сфера применения

В настоящей Рекомендации приводится техническая основа противодействия спаму, рассылаемому по электронной почте. В рамках этой основы описывается одна из рекомендуемых структур домена антиспамовой обработки сообщений и определяются функции ее основных модулей. Главным в данной основе является то, что она устанавливает механизм обмена информацией о спаме, рассылаемом по электронной почте, между различными серверами электронной почты. Применение такой основы повысило бы эффективность всей совокупности взаимодействующих систем.

2 Справочные документы

Не имеются.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 поля заголовков [b-IETF RFC 2822]: Поля заголовков имеют одну и ту же общую синтаксическую структуру: имя поля, после которого следует двоеточие, после которого следует текстовая часть поля.

3.1.2 элемент почтового сообщения [b-IETF RFC 2821]: Элемент почтового сообщения транспортируется с помощью протокола SMTP. Каждый элемент почтового сообщения включает конверт и содержание.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации даны определения следующих терминов:

3.2.1 домен антиспамовой обработки: Это независимая система, содержащая объект антиспамовой обработки, подобъекты антиспамовой обработки, серверы электронной почты и клиенты электронной почты.

3.2.2 объект антиспамовой обработки: Объект антиспамовой обработки является ядром домена антиспамовой обработки. Он собирает информацию о спаме, рассылаемом по электронной почте, от объектов более низких уровней и затем создает унифицированную и комплексную систему на базе правил. И наконец, эта система на базе правил должна быть представлена всем объектам более низких уровней.

3.2.3 подобъект антиспамовой обработки: Подобъект антиспамовой обработки соединен с одним или несколькими поставщиками услуг электронной почты. Он получает информацию о спаме, рассылаемом по электронной почте, от серверов электронной почты или антиспамового оборудования и сообщает информацию объектам высокого уровня, периодически анализируя ее. Кроме того, он периодически получает обновляемые правила от объектов высокого уровня и распространяет их среди подобъектов.

3.2.4 сложное правило: Сложное правило состоит из двух или нескольких простых правил.

3.2.5 электронная почта: Этот термин используется главным образом для обозначения электронной почты, передаваемой через сеть электросвязи.

3.2.6 спам, рассылаемый по электронной почте: Этот термин используется для описания незапрашиваемых электронных сообщений, обычно направляемых через электронную почту в конкретных целях.

3.2.7 правило: Правило – это совокупность условий и основных действий. Правила включают многочисленные формы, например виды поведения, фильтры и т. д.

3.2.8 электронное сообщение-образец: Этот термин используется для описания любого электронного сообщения, полученного от серверов электронной почты в соответствии с определенными правилами.

3.2.9 спамер: Этот термин используется для описания объекта или человека, создающего и посылающего спам по электронной почте.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

DNS	Domain Name Server	Система наименований доменов
E-mail	Electronic mail	Электронная почта
ESMTP	Extended Simple Mail Transfer Protocol	Расширенный простой протокол передачи электронной почты
FTP	File Transfer Protocol	Протокол передачи файлов
HTTP	Hypertext Transfer Protocol	Протокол передачи гипертекста
IMAP4	Internet Message Access Protocol v4	Протокол доступа к сообщениям интернета, версия 4
IP	Internet Protocol	Протокол Интернет
POP3	Post Office Protocol v3	Почтовый протокол, версия 3
RBL	The term is commonly used to describe Real-time Blacklist.	Этот термин обычно используется для описания "черного списка" в реальном масштабе времени.
SASL	Simple Authentication and Security Layer	Уровень простой аутентификации и безопасности
SMTP	Simple Mail Transfer Protocol	Простой протокол передачи электронной почты
URL	Uniform Resource Locator	Унифицированный указатель ресурса

5 Соглашения о терминах

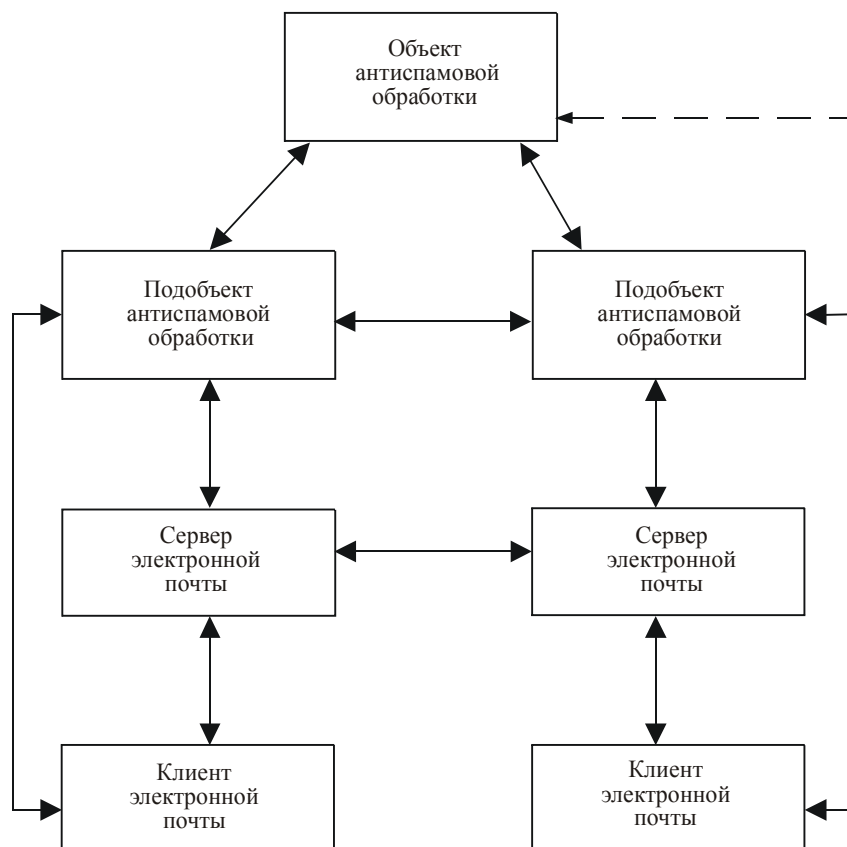
Не имеются.

6 Общая структура домена антиспамовой обработки

6.1 Общая структура

В настоящей Рекомендации описываются компоненты этой основы. Она включает в себя объект антиспамовой обработки, подобъект антиспамовой обработки, серверы электронной почты и клиентов электронной почты.

Эти компоненты могут связываться друг с другом посредством общедоступных протоколов передачи сообщений. Характерные особенности этих компонентов представлены в данном пункте.



ПРИМЕЧАНИЕ. – Сплошные линии показывают путь прохождения информации, которой обмениваются компоненты домена антиспамовой обработки.

Рисунок 1 – Общая структура

На рисунке 1 объект антиспамовой обработки получает сообщения от подобъектов антиспамовой обработки и доставляет им новые правила.

Подобъекты антиспамовой обработки должны проверять период действия правил, поступающих от объекта антиспамовой обработки, и вносить в них улучшения.

Клиент электронной почты является объектом, с которым непосредственно взаимодействуют пользователи. Сервер электронной почты осуществляет доставку электронной почты в сети электросвязи на базе IP.

Клиент электронной почты направляет жалобы подобъекту антиспамовой обработки. В конкретных ситуациях клиент электронной почты может направить жалобу напрямую объекту антиспамовой обработки верхнего уровня.

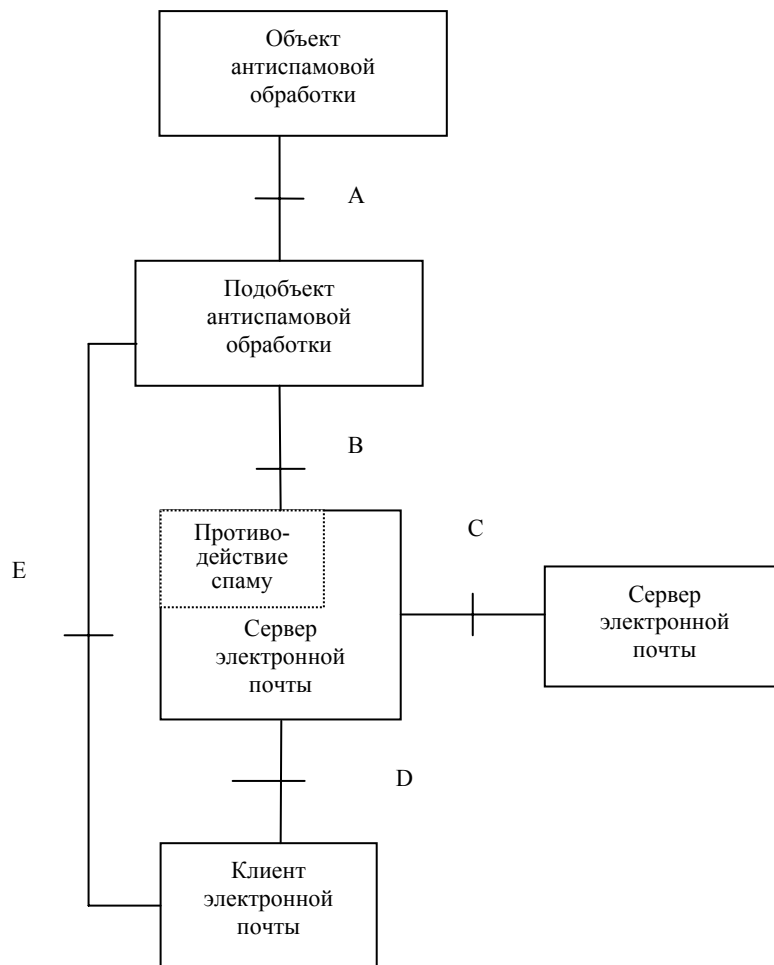


Рисунок 2 – Эталонная модель

Интерфейс А находится между объектом антиспамовой обработки и подобъектом антиспамовой обработки. Сообщения о жалобах и правила, касающиеся противодействия спаму, передаются через интерфейс А. Правила могут представлять собой сложные правила, например "источник IP + URL". Интерфейс А должен поддерживать протоколы FTP и HTTP.

Интерфейс В находится между подобъектом антиспамовой обработки и сервером электронной почты. Он используется для передачи Сообщений о жалобах, а также правил. Аналогичным образом, правила могут представлять собой сложные правила, например "источник IP + URL". Интерфейс В должен поддерживать протоколы FTP и HTTP. В конкретных ситуациях сервер электронной почты может напрямую связываться с объектом антиспамовой обработки верхнего уровня.

Интерфейс С находится между серверами электронной почты, через которые передаются сообщения с использованием SMTP.

Интерфейс D находится между сервером электронной почты и клиентом электронной почты. Для передачи электронной почты могут использоваться различные протоколы, например POP3, IMAP4.

Интерфейс Е находится между клиентом электронной почты и подобъектом антиспамовой обработки. Клиент электронной почты может направлять жалобы подобъекту антиспамовой обработки. В конкретных ситуациях клиент электронной почты может направлять жалобы напрямую объекту антиспамовой обработки верхнего уровня. В этом интерфейсе может использоваться программное обеспечение для работы в сети в онлайн-режиме, для телефонной связи, обмена электронной почтой, а также клиентское программное обеспечение.

7 Функции домена антиспамовой обработки

7.1 Функции клиента электронной почты

Функции клиента электронной почты включают:

- Помимо выполнения общих функций передачи электронных сообщений, клиент электронной почты обеспечивает механизм, помогающий пользователям направлять жалобы о спамовой информации объекту антиспамовой обработки. Получателям электронной почты нужно всего лишь определить, является ли то или иное электронное сообщение спамом, исходя из его содержания, названия или адреса. Так, например, если получатели не желают получать рекламные материалы, электронные публикации или пропагандистские материалы, они могут направить жалобу относительно таких электронных сообщений объекту антиспамовой обработки с помощью механизма клиента электронной почты.
- Клиент электронной почты может загружать правила, фильтрующие спам, автоматически из объекта антиспамовой обработки. Правила фильтрации устанавливаются согласно сообщениям о жалобах, поступающим от клиентов электронной почты. Они включают предельный размер одного электронного сообщения, количество электронных сообщений, направляемых за определенный период времени, ключевые слова в основном тексте электронных сообщений и т. д. Правила фильтрации периодически обновляются согласно сообщениям о жалобах. Они снабжены указателями имени пользователя почтового ящика, выходного IP-адреса и наименования домена.
- Клиент электронной почты может переслать спам, рассылаемый по электронной почте, объекту антиспамовой обработки для дальнейшей обработки или удаления некоторых правил фильтрации, вызывающих ошибочное срабатывание. Объект антиспамовой обработки может немедленно обновить правила фильтрации в соответствии с требованиями или жалобами от клиента электронной почты.
- Клиент электронной почты может непосредственно отфильтровать спам, рассылаемый по электронной почте. Обычно получатели должны знать о результатах фильтрации, с тем чтобы не допустить возникновения проблемы ошибочного срабатывания.

7.2 Функции сервера электронной почты

Функции сервера электронной почты включают:

- Осуществляя общие функции передачи электронной почты, сервер электронной почты выполняет свои обычные действия по обмену электронной почтой с другим сервером электронной почты или по отправке и получению электронной почты между клиентами электронной почты; в то же время сервер электронной почты должен запретить функцию открытой ретрансляции, с тем чтобы спамеры не смогли вынудить его передать спам-сообщение другому серверу электронной почты.
- Любой абонент должен пройти проверку, прежде чем он направит электронное сообщение через сервер электронной почты. Разные системы электронной почты могут использовать разные механизмы проверки. Проверка производится между сервером электронной почты и клиентом электронной почты.
- Любой поставщик услуг электронной почты может вести "черный список" спамеров, в котором содержится некоторая информация о спамерах (например, наименование хоста, наименование домена или адрес электронной почты). Сервер электронной почты отказывается получать электронные сообщения, исходящие от этих спамеров.
- Сервер электронной почты может вернуть команду проверки источнику, который указан в информации об отправителе электронного сообщения (например, DNS, наименование хоста или другие). Если команда проверки не подтвердит аутентичность источника, то сервер электронной почты отклонит данное электронное сообщение.
- Некоторые команды SMTP могут использоваться спамерами, для того чтобы угадать действительную учетную запись сервера электронной почты. Сервер электронной почты запрещает эти команды, например EXPN и VRFY.
- Некоторые виды электронных сообщений рекламного и пропагандистского характера направляются без предоставления какой бы то ни было информации об отправителе. Сервер электронной почты должен автоматически добавить ссылку HTTP в текст электронного сообщения. Абоненты могут представлять сообщения о жалобах в любое удобное время.

- Серверы электронной почты обнаруживают спам-сообщения с помощью антиспамовых технологий, сообщают о спаме подобъекту антиспамовой обработки и загружают из него правила фильтрации.
- В случае обнаружения спама сервер электронной почты должен осуществить резервное копирование исходного спама, включающее по меньшей мере заголовок электронной почты источника, и представить его в фильтр.
- Сервер электронной почты должен предоставлять информацию системного журнала и свои статистические данные, которые периодически копируются, и передавать их подобъекту антиспамовой обработки.
- Сервер электронной почты возвращает другой номер состояния в соответствии с другими правилами.
- Сервер электронной почты может ограничить объем трафика, направляемого конкретным абонентом электронной почты.

7.3 Функции объекта антиспамовой обработки

Функции объекта антиспамовой обработки включают:

- Обмен правилами фильтрации с другими объектами антиспамовой обработки. Для передачи информации могут использоваться различные протоколы, например FTP и HTTP.
- Хранение исходной информации о спам-сообщениях, полученных от абонентов, и объекта антиспамовой обработки.
- Широковещательная передача правил фильтрации подобъектам антиспамовой обработки и предупреждение их об опасных электронных сообщениях.
- Объект антиспамовой обработки должен управлять правилами фильтрации и поддерживать их. Эти правила могут быть получены через веб-сайт для:
 - получения сообщений от абонентов и подобъектов антиспамовой обработки;
 - широковещательной передачи достоверной информации, в том числе информации, касающейся контроля и управления.

7.4 Функции подобъекта антиспамовой обработки

Функции подобъекта антиспамовой обработки включают:

- Получение сообщений о жалобах от абонентов и правил фильтрации от объекта антиспамовой обработки.
- Хранение исходной информации о спаме (по крайней мере, заголовок спама), полученной от абонентов и различных организаций.
- Широковещательная передача правил фильтрации серверам электронной почты или клиентам электронной почты и предупреждение об опасных электронных сообщениях любого пользователя, который в этом нуждается.
- Отслеживание распространения спама и сбор соответствующей информации.
- Сообщение о состоянии распространения спама и передача соответствующей информации объектам на более высоких уровнях.
- Создание новых правил фильтрации из резервных копий сомнительных электронных сообщений, проверка и изменение действующих правил фильтрации. Эти правила могут быть получены через веб-сайт для:
 - создания сообщений о спаме от абонентов и серверов электронной почты;
 - создания новых правил фильтрации.

8 Выявление спама, рассылаемого по электронной почте

В настоящем пункте содержится описание известных характерных особенностей и критериев спама, рассылаемого по электронной почте.

8.1 Известные характерные особенности спама, рассылаемого по электронной почте

Ниже приводится перечень некоторых известных характерных особенностей спама, рассылаемого по электронной почте:

- Соккрытие или подделка настоящего адреса отправителя или указание ложного адреса отправителя
В поля отправителя "from" или "sender" включено пустое или неправильное содержимое.

- Скрытие или подделка действительного источника электронного сообщения
Содержимое поля идентификации "message-id" является пустым или неправильным.
- Отправитель является известным спамером
В поле отправителя "from" или "sender" содержится адрес спамера из "черного списка".
- Ложная информация о получателях
Содержимое, включенное в поле получателя ("to") или в поле получателя копии ("cc"), является ложным или имеет отношение к спамерам.
- Наличие общих слов, используемых спамерами
Общие слова, используемые спамерами, включены в поле предмета ("subject") или в содержимое электронного сообщения.
- Ложная информация о ретрансляции
Содержимое, включенное в поле пересылки "resent-from" или "resent-sender" является ложным.
- Ложная информация для отслеживания
В поле отслеживания включено ложное содержимое.
- Ненадлежащий размер
Размер всего электронного сообщения, поля заголовка или содержимого электронного сообщения аналогичен размеру полей заголовка и содержимого электронного сообщения в спаме, рассылаемом по электронной почте.
- Слишком много получателей
В определенном поле значится слишком много получателей.
- Слишком много повторных передач
В поле отслеживания содержится слишком много следов.
- В определенных полях содержится IP-адрес отправителя
Информация, имеющая отношение к спамерам, включена в поле отправителя "from" или "sender".
- В определенных полях содержится IP-адрес сервера электронной почты
Информация, имеющая отношение к спамерам, включена в поле отслеживания "received" и в поле пересылки "resent-from" или "resent-sender".
- Новый спам
Объект антиспамовой обработки может обобщать характерные особенности на основе нового образца спама и создать соответствующие правила фильтрации.

8.2 Общие правила борьбы со спамом, рассылаемым по электронной почте

Отдельные правила могут быть объединены в сложное правило с различными приоритетами.

Сервер электронной почты может применять отдельное и/или сложное правило для борьбы со спамом, рассылаемым по электронной почте.

8.2.1 Общие важнейшие правила

Сервер электронной почты может устанавливать критерии согласно следующим факторам:

- В поле отправителя ("from" или "sender") включено пустое либо неправильное содержимое.
- В поле идентификации сообщений ("message-id") включено пустое либо неправильное содержимое.
- Поле отправителя ("from" или "sender") содержит установленные ключевые слова, перечисленные в "черном списке".
- Ключевые слова, перечисленные в "черном списке", включены в поле получателя ("to") или в поле получателя копии ("cc").
- Поле предмета ("subject") или содержимое электронного сообщения включает установленные ключевые слова.
- Действительный первоисточник не может быть найден в поле пересылки "resent-from" или "resent-sender" или в содержимом поля отслеживания.

- Размер всего электронного сообщения, поля заголовка или содержимого электронного сообщения (приблизительно) равен некоторому заданному значению.
- Общее число адресов, заданных в поле отправителя "to", "cc" и "bcc" поля отправителя превышает предельное значение, установленное сервером электронной почты; или число раз, которое должно доставляться одно электронное сообщение, превышает предельное значение, заданное сервером электронной почты.
- Количество следов в поле отслеживания превышает предельное значение, установленное поставщиком услуг электронной почты или администратором данного домена.
- Результат, который получается при обратном DNS-преобразовании информации, содержащейся в поле отправителя "from" или "sender", включен в "черный список".
- Результат, который должен получаться при обратном DNS-преобразовании информации, содержащейся в поле отслеживания "received", а также в поле пересылки "resent-from" или "resent-sender", включен в "черный список".
- Спам, рассылаемый по электронной почте, нельзя выявить с использованием лишь одного правила; требуется использовать сложное правило.

8.2.2 Приоритетность критериев

Требуется подтверждать приоритетность критериев. Если одно электронное сообщение подчиняется нескольким правилам (что называется конфликтом правил), то оно будет рассматриваться согласно правилу с наивысшим приоритетом. Если приоритеты правил равны, то применяется итоговое правило, основанное на принципе приоритета в случае конфликтов. Следует избегать конфликта по мере возможности.

8.2.3 Обнаружение конфликта критериев

Эта функция используется для обнаружения конфликтов между различными установленными критериями. Ниже приводится описание известных конфликтующих условий:

- Одновременно и "условия правил" включают один и тот же вид "простых правил" (основных правил) класса поиска по ключевым словам (например, "предмет включает XXX", "то, что расшифровано из первых 10 линий, включает XXX" и т. д.), и ключевые слова в обоих "простых правилах" являются одними и теми же, и одно ключевое слово включает другое.
- Одновременно и "условие правил" включает один и тот же вид "простых правил" класса ограничения по IP (например, "IP клиента – XXX" и т. д.), и участки IP, указанные в "простых правилах", являются одними и теми же или имеют множество пересечений.
- Одновременно и "условие правил" включает один и тот же вид "простых правил" класса ограничения по размеру, и условия ограничения по размеру согласуются с формой "размер XXX представляет собой заданное значение" (он не может быть "больше чем" или "менее чем"), и значения являются одинаковыми. Например, два правила включают одно и то же простое правило: "размер текста электронного сообщения составляет 5343 байт".

9 Методы противодействия спаму, рассылаемому по электронной почте

Основные методы противодействия спаму, рассылаемому по электронной почте, включают отключение функции открытой ретрансляции сервера электронной почты, совершенствование процедур проверки полномочий на доставку электронной почты, а также использование методов фильтрации. Система противодействия спаму, рассылаемому по электронной почте, должна поддерживать или может дополнительно поддерживать следующие методы.

9.1 Отключение функции открытой ретрансляции

Открытая ретрансляция подразумевает передачу сервером электронной почты всей поступающей электронной почты, независимо от того, являются или не являются отправители или получатели электронных сообщений установленными абонентами. Как правило, если на сервере электронной почты включена функция неограниченной ретрансляции, то считается, что он осуществляет открытую ретрансляцию.

9.2 Совершенствование процедур проверки полномочий на доставку электронной почты

Чтобы не допустить использования сервера электронной почты неавторизованными абонентами:

- отправители должны являться законными абонентами этого сервера;
- сервер должен сертифицировать IP-адреса отправителей;
- во избежание экспоненциального распространения спама количество пересылок электронных сообщений ограничивается;
- сервер электронной почты может проверить источник электронных сообщений, чтобы убедиться в его действительности.

9.3 Метод фильтрации

Технологию фильтрации можно разделить на два класса: фильтрация IP-адреса и фильтрация путем сканирования текста.

9.3.1 Фильтрация IP-адреса

Фильтрация IP-адреса может ограничить соединение с системой электронной почты по протоколу SMTP. Ее важными атрибутами являются диапазон IP-адресов и режимы ограничения.

Диапазон IP-адресов включает:

- диапазон IP-адресов в реальном времени, поступающих от объекта антиспамовой обработки;
- диапазон IP-адресов в реальном времени, поступающих от правил фильтрации других организаций;
- диапазон IP-адресов в реальном времени, которые добавились сами.

Режимы ограничения включают:

- отказ в соединении;
- безусловное разрешение на установление соединения;
- повторные соединения с сервером электронной почты, осуществляемые с IP-адреса какого-либо клиента, должны быть ограничены определенным периодом времени.

Если IP-адрес какого-либо клиента принадлежит к определенному диапазону IP-адресов, то будут введены режимы ограничения.

9.3.2 Фильтрация путем сканирования текста

Правила фильтрации могут устанавливаться сервером электронной почты и загружаться из объекта антиспамовой обработки. Правила фильтрации могут изменяться администраторами при определенных условиях.

Если электронное сообщение совпадает с определенным правилом, то это сообщение будет классифицировано на основе соответствующего поведения. Виды поведения правил сканирования текста включают:

- отклонение: возврат отклоненного сообщения отправителю после извлечения его характеристик;
- исключение: нормальный ответ на каждую команду без какого-либо поведения;
- доставка: нормальная доставка. Игнорирование удаления после выбора доставки;
- метка: добавление специальной метки в заголовок;
- сообщение: сообщение в центр оповещения о характеристике, выделенной из соответствующего электронного сообщения;
- буфер: хранение электронного сообщения, по возможности, в нетронутым виде и передача его копии в объект антиспамовой обработки.

9.4 Изучение возможности отслеживания

Временами трудно определить, является ли отправитель законным абонентом. Ввиду того, что сервер, принимающий электронные сообщения, не может обладать всей информацией о сервере, направляющем электронные сообщения, то он не может сертифицировать всю информацию для законных абонентов.

Электронные сообщения можно разделить на два вида: сообщения, поддающиеся отслеживанию, и сообщения, не поддающиеся отслеживанию. Нежелательные электронные сообщения, поддающиеся отслеживанию, будут отражены в правилах фильтрации, если оповещения не потребуют усилий. Трудно избавиться от нежелательных электронных сообщений, не поддающихся отслеживанию, поскольку они обычно используют подложный источник электронного сообщения. Большинство сообщений, не поддающихся отслеживанию, являются нежелательными электронными сообщениями, и поэтому изучение возможности отслеживания лежит в основе противодействия технологиям спама, рассылаемого по электронной почте. Предлагаются следующие три этапа:

Первый этап: требование:

- Большинство серверов, принимающих электронные сообщения ("MX" в наименовании домена), являются серверами, направляющими электронные сообщения.
- Большинство отдельных серверов, принимающих электронные сообщения, и серверов, направляющих электронные сообщения, имеют соседние IP-адреса, следующие друг за другом.
- Другие компьютеры, которым разрешено доставлять электронную почту, могут иметь соседние IP-адреса с серверами электронной почты "MX".
- Некоторые серверы электронной почты могут быть найдены с помощью обратного DNS-преобразования, и полученный результат является таким же, как и в жалобе абонента.

Второй этап: механизм уведомления о возможности отслеживания:

Поддержание сертификации в сети электросвязи:

- Подтверждение того, что поле адреса электронной почты отправителя разрешено.
- Подтверждение того, что отправитель является законным абонентом соответствующего поля адреса электронной почты.

Третий этап: механизм обратной связи:

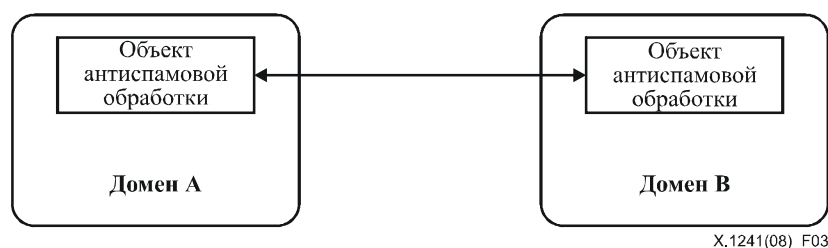
- Услуга, поддающаяся отслеживанию, и изучение, поддающееся отслеживанию, образуют цепь обратной связи.
- Цепь обратной связи нельзя сфальсифицировать.
- Сфальсифицированную и истинную части легко отличить.

Система отслеживания может провести расследование автоматически с использованием цепи обратной связи.

10 Взаимодействие между доменами антиспамовой обработки

При взаимодействии доменов антиспамовой обработки друг с другом можно выбрать один из трех следующих режимов: взаимодействие между объектами обработки верхнего уровня, взаимодействие между объектами и подобъектами обработки, взаимодействие между подобъектами обработки и серверами электронной почты. Каждый выбор может соответствовать определенным сценариям или требованиям.

10.1 Взаимодействие между объектами обработки верхнего уровня



X.1241(08)_F03

Рисунок 3 – Взаимодействие между объектами обработки верхнего уровня

Этот режим взаимодействия представляет собой двустороннюю связь между объектами обработки верхнего уровня. Эти два объекта обмениваются только правилами. Если один из объектов получает информацию от другого, то он применяет определенные механизмы и процедуры, для того чтобы выбрать полезные правила из полученной информации.

10.2 Взаимодействие между объектом и подобъектом обработки

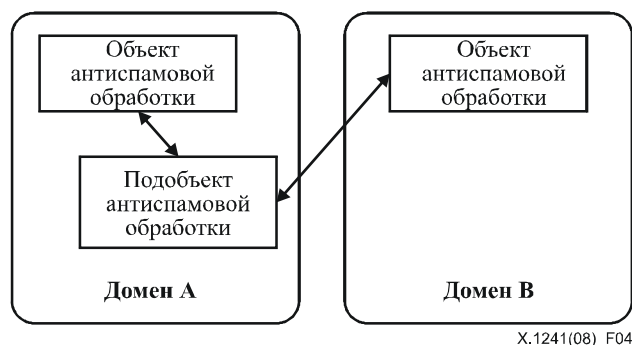


Рисунок 4 – Взаимодействие между объектом и подобъектом обработки

Этот режим взаимодействия представляет собой двустороннюю связь между объектом и подобъектом обработки. Подобъект должен загрузить две таблицы правил фильтрации из двух объектов обработки. Подобъект создает правила согласно сомнительным сообщениям от присоединенных серверов. Он должен сообщить эти правила двум объектам.

Этот режим обеспечивает определенную безопасность. Однако ввиду того, что он подразумевает наличие сложной управляющей взаимосвязи между подобъектом и двумя объектами, этот режим может сталкиваться с проблемами масштабируемости. Он не обеспечивает полное взаимодействие между доменами.

10.3 Взаимодействие между подобъектом обработки и сервером электронной почты

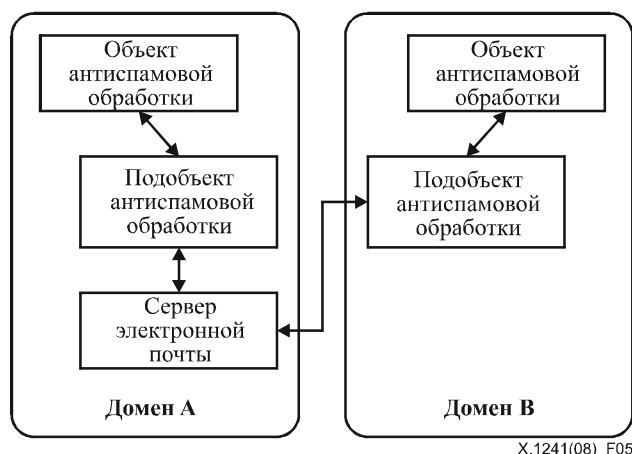


Рисунок 5 – Взаимодействие между подобъектом обработки и сервером электронной почты

Этот режим взаимодействия представляет собой двустороннюю связь между подобъектом обработки и сервером электронной почты. Сервер электронной почты загружает правила фильтрации спама из подобъекта и сообщит о нежелательных электронных сообщениях подобъекту другого домена. Этот подобъект получает сообщения о нежелательных электронных сообщениях от сервера электронной почты и публикует свои собственные правила для сервера другого домена.

Этот режим несложно реализовать между доменами. Однако домен антиспамовой обработки может быть атакован серверами, находящимися вне домена, и поэтому этот режим может испытывать проблемы с точки зрения безопасности. Кроме того, он имеет проблемы, связанные с масштабируемостью. Поэтому он не обеспечивает полное взаимодействие между доменами. Режим, описанный в пункте 10.1, является надежным и рекомендуемым режимом взаимодействия.

Библиография

- [b-IETF RFC 1869] IETF RFC 1869 (1995), *SMTP Service Extensions*
<<http://www.ietf.org/rfc/rfc1869.txt>>.
- [b-IETF RFC 1939] IETF RFC 1939 (1996), *Post Office Protocol – Version 3*
<<http://www.ietf.org/rfc/rfc1939.txt>>.
- [b-IETF RFC 2060] IETF RFC 2060 (1996), *Internet Message Access Protocol - Version 4rev*
<<http://www.ietf.org/rfc/rfc2060.txt>>.
- [b-IETF RFC 2222] IETF RFC 2222 (1997), *Simple Authentication and Security Layer*
<<http://www.ietf.org/rfc/rfc2222.txt>>.
- [b-IETF RFC 2505] IETF RFC 2505 (1999), *Anti-Spam Recommendations for SMTP MTAs*
<<http://www.ietf.org/rfc/rfc2505.txt>>.
- [b-IETF RFC 2554] IETF RFC 2554 (1999), *SMTP Service Extension for Authentication*
<<http://www.ietf.org/rfc/rfc2554.txt>>.
- [b-IETF RFC 2821] IETF RFC 2821 (2001), *Simple Mail Transfer Protocol*.
<<http://www.ietf.org/rfc/rfc2821.txt>>.
- [b-IETF RFC 2822] IETF RFC 2822 (2001), *Internet Message Format*
<<http://www.ietf.org/rfc/rfc2822.txt>>.

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