МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1231

(04/2008)

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

Безопасность электросвязи

Технические методы противодействия спаму

Рекомендация МСЭ-Т X.1231

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.

Рекомендация МСЭ-Т X.1231

Технические методы противодействия спаму

Резюме

В Рекомендации МСЭ-Т X.1231 представлены технические методы противодействия спаму, в том числе содержатся общие характеристики спама и основные задачи противодействия спаму. Кроме того, поскольку признается, что не существует единственного решения проблемы спама, в данной Рекомендации содержится также перечень контрольных вопросов для оценки перспективных средств противодействия спаму.

Источник

Рекомендация МСЭ-Т X.1231 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

Противодействие спаму, спам, технические методы.

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. Ни одна из частей 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, которые определяются в каких-либо других материалах	1
	3.2 Термины, определяемые в настоящей Рекомендации	1
4	Сокращения и акронимы	2
5	Соглашения о терминах	3
6	Общие аспекты	3
7	Общие задачи	5
8	Технические методы	5
	8.1 Оборудование	6
	8.2 Сеть	7
	8.3 Обслуживание	8
	8.4 Фильтрация	9
	8.5 Обратная связь	10
9	Оценка системы	11
Библиография		12

Введение

Вместе с развитием информационной отрасли спам стал широко распространенной проблемой, ставшей причиной потери прибыли операторов электросвязи, поставщиков услуг и деловых пользователей, а также негативного влияния на обычных пользователей в целом. Спам превратился из обычной помехи в напасть всемирного масштаба.

Поэтому необходимо найти эффективные и действенные способы, чтобы противодействовать спаму. Существует множество аспектов противодействия спаму: законодательство, профессиональная подготовка, международное законодательство и т. п. Настоящая Рекомендация, в основном, сосредоточена на технических способах.

Рекомендация МСЭ-Т X.1231

Технические методы противодействия спаму

1 Сфера применения

В настоящей Рекомендации особое внимание уделяется техническим методам противодействия спаму, а также содержатся общие характеристики спама и основные задачи противодействия спаму. Кроме того, поскольку признается, что не существует единого решения для противодействия спаму, в настоящей Рекомендации приводится также перечень контрольных вопросов для оценки перспективных средств противодействия спаму.

В настоящей Рекомендации описываются технические методы в целом и не определяются технические методы в отношении какого-либо конкретного типа спама. Кроме того, в настоящей Рекомендации приводится иерархическая модель общих категорий, которые могут быть предусмотрены для установления действенной и эффективной инфраструктуры противодействия спаму. В модель входят следующие части:

- технические методы в отношении оборудования;
- технические методы в отношении сетей;
- технические методы в отношении обслуживания;
- технические методы в отношении фильтрации;
- технические методы в отношении обратной связи.

Практически в настоящей Рекомендации приводятся технические методы противодействия различным типам спама, которые одна администрация считает неподходящими, в соответствии с национальными законами и политикой.

2 Справочные документы

Не имеются.

3 Определения

3.1 Термины, которые определяются в каких-либо других материалах

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

3.1.1 аутентификация [b-ITU-T X.811]: Предоставление гарантии заявленной идентичности объекта.

3.1.2 IP-телефон [b-ITU-T Q-Sup.49]: IP-телефоном называется терминал (например, специальный речевой терминал или многоцелевой персональный компьютер), непосредственно соединенный с IP-сетью (например, через интерфейс Ethernet или линию xDSL).

3.1.3 объект короткого сообщения [b-ITU-T Q.1742.3]: Объект, который составляет или разбивает короткие сообщения. Объект SME может располагаться внутри или вне домашнего регистра местоположения (HLR), центра сообщений (MC), визитного регистра местоположения (VLR), подвижной станции (MS) или центра коммутации подвижной связи (MSC) и не отличаться или отличаться от них.

3.2 Термины, определяемые в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины:

3.2.1 мгновенная передача сообщений (IM): Мгновенной передачей сообщений называется передача сообщений между пользователями почти в реальном времени. Обычно эти сообщения являются короткими, но они не обязательно могут быть такими. Передача IM обычно используется в диалоговом режиме, т. е. передача сообщений в обе стороны осуществляется достаточно быстро, чтобы участники поддерживали интерактивный диалог.

3.2.2 мультимедийный IP-спам: Мультимедийным IP-спамом называются незапрашиваемые сообщения или вызовы с использованием реальновременных мультимедийных IP-приложений. В отличие от традиционного спама, рассылаемого по электронной почте, мультимедийным IP-спамом называется спам с использованием недавно появившихся методов связи на основе IP, таких как мгновенная передача сообщений, услуга учета присутствия, передача речи по протоколу Интернет (VoIP) и т. д. Передача спама с помощью интернет-телефонии (SPIT), голосовой спам или VoIP-спам VAM и передача спама при передаче сообщений по интернету (SPIM) – это существующие названия конкретного IP-мультимедийного спама.

3.2.3 модальность: Модальностью называется кодирование информации, содержащей информацию, которую воспринимают люди. Например: модальная информация включает текст, графические изображения, аудио-, видеосигналы или осязаемые данные, используемые в человеко-машинном интерфейсе. Мультимодальная информация может исходить из таких мультимодальных устройств, как микрофон для голосового/звукового ввода, карандаш для тактильного ввода, клавиатура для текстового ввода, мышь для ввода движением, громкоговоритель для получаемого синтезированного голосового сигнала, экран для получаемых графических изображений/текста, вибрирующее устройство для ощущения обратной связи или пишущее азбукой Брайля устройство для лиц с нарушениями зрения, или быть предназначенной для этих устройств.

3.2.4 мультимодальное сообщение: Мультимодальным сообщением называется вид мультимедийного сообщения, содержащего различную кодированную информацию для взаимодействия с помощью многочисленных модальностей.

3.2.5 услуга передачи мультимедийных сообщений (MMS): Услугой передачи мультимедийных сообщений называется вид услуги передачи сообщений после услуги передачи коротких сообщений, с помощью которой по сетям подвижной, беспроводной или фиксированной связи могут передаваться различные мультимедийные сообщения, включая текст, графические изображения, аудио-, видеосигналы и т. п.

3.2.6 услуга передачи коротких сообщений (SMS): Услугой передачи коротких сообщений называется один из видов услуг передачи сообщений, который позволяет мобильному телефону и другим объектам коротких сообщений передавать и принимать текстовые сообщений с помощью устройства, называемого центром обслуживания, которое реализует такие функции, как хранение и доставка.

3.2.7 спамер: Спамером называется объект или лицо, создающие и отправляющие спам.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

DDoS	Distributed Denial of Service		Распределенный отказ в обслуживании
DoS	Denial of Service		Отказ в обслуживании
E-mail	Electronic Mail	Эл. почта	Электронная почта
HLR	Home Location Register		Домашний регистр местоположения
IM	Instant Messaging		Мгновенная передача сообщений
IP	Internet Protocol		Протокол Интернет
MC	Message Centre		Центр сообщений
MMS	Multimedia Messaging Service		Услуга передачи мультимедийных сообщений
MC	Mobile Station		Мобильная станция
MSC	Mobile Switching Centre		Центр коммутации подвижной связи
PSTN	Public Switched Telephone Network	КТСОП	Коммутируемая телефонная сеть общего пользования
SME	Short Message Entity		Объект короткого сообщения
SMS	Short Message Service		Услуга передачи коротких сообщений
SMTP	Simple Mail Transfer Protocol		Простой протокол для электронной почты
SPIM	Spam over Internet Messaging		Передача спама при мгновенной передаче сообщений

SPIT	Spam over Internet Telephony	Передача спама с помощью интернет-телефонии
VAM	Voice Spam or VoIP Spam	Голосовой спам или VoIP-спам
VLR	Visitor Location Register	Визитный регистр местоположения
VoIP	Voice over IP	Передача речи по протоколу Интернет

5 Соглашения о терминах

Не имеются.

6 Общие аспекты

Спам – это электронная информация, доставляемая от отправителя получателям с помощью терминалов, таких как компьютеры, мобильные телефоны, телефоны и пр., которая обычно является незапрашиваемой, нежелательной и вредной для получателей. Спам может переноситься в электронной почте, при передаче сообщений на мобильные телефоны (SMS, MMS и т. д.), в IP-мультимедиа и в других электронных формах. Фактически, понимание того, что такое "спам", зависит от определенных представлений определенных наций, организаций или частных лиц. В частности, понимание этого развивается и расширяется по мере развития информационно-коммуникационных технологий, которые предоставляют новые возможности для создания спама. Как правило, спам имеет следующие общие характеристики:

Электронный: Спам – это электронная информация, обычно передаваемая по открытой сети электросвязи, особенно по интернету, которая существенно отличается от традиционных методов распространения путем почтовых рассылок, бумажных рекламных объявлений или прямого маркетинга. Спам дешев, удобен, его просто замаскировать.

Незапрашиваемый: Спам, как правило, содержит рекламные объявления, информацию мошеннического характера или вирусы и т. п.

Кроме того, обычно спам имеет все следующие характеристики или часть из них:

Большое количество и повторяемость: Спам в виде сообщений и спам в виде электронной почты обычно передается в большом количестве и беспорядочно, тогда как спам с использованием связи в реальном времени всегда инициируется несколько раз. Однако тот, кто рассылает спам, не знает ничего кроме адреса связи получателя (например, адресов электронной почты, телефонного номера получателя).

Использование адреса без согласия владельца: Спамеры часто используют адреса связи, полученные без непосредственного согласия их владельцев, для рассылки спама. Действительно, с помощью некоторых компьютерных программ можно осуществлять сбор адресов связи в веб-сети или создавать адреса связи автоматически.

Скрытое или ложное происхождение сообщений: Спам обычно направляется таким образом, чтобы скрыть его отправителя путем использования ложного заголовка сообщения или просто не показывать отправителя. Те, кто рассылают спам, обычно используют несанкционированные серверы третьих сторон, которые не проверяют информацию отправителя.

Сложность блокирования: Спам очень трудно обнаружить из-за большого объема сообщений. Попытки заблокировать спам могут быть связаны с трудностями и иногда приводят к ошибочному распознаванию или нераспознаванию спама.

Методы должны быть технически нейтральными и результативными для оценки ряда факторов: какое конкретное средство связи неправильно используется или создает проблемы в рамках данной юрисдикции, какое средство связи может с большой вероятностью неправильно использоваться в будущем, и в отношении какого средства связи неправильное использование маловероятно. Общими случаями являются:

Электронная почта

В настоящее время спам по электронной почте является наиболее серьезной проблемой по отношению к другим типам спама, ввиду уязвимости протокола электронной почты и слабой защиты базовой инфраструктуры, т. е. интернета, по которому ретранслируется электронная почта. Наиболее распространенным протоколом для передачи электронной почты является SMTP (Простой протокол передачи электронной почты). Протокол SMTP определяет оболочку и заголовок сообщения

электронной почты. Оболочка содержит адрес получателя, который не может его видеть. Он используется в качестве адреса назначения для передачи сообщения от отправителя получателю. Как правило, в течение передачи адрес назначения, содержащийся в оболочке, может быть скопирован в заголовок сообщения электронной почты, который получатель видит. Те, кто рассылают спам, используют два типа уязвимости в процессе аутентификации SMTP:

- Отсутствие необходимости в аутентификации, вследствие чего пользователи могут скрывать или фальсифицировать свои адреса.
- Большинство записей в оболочке и заголовке сообщения электронной почты могут быть фальсифицированы.

Кроме того, затраты на отправку спама по электронной почте весьма невелики, тогда как негативное влияние всегда очень велико.

Услуга передачи сообщений по сети подвижной связи

Замечательными преимуществами подвижной связи являются удобство, эффективность, низкая стоимость и простота использования. Однако в настоящее время пользователи, наслаждаясь преимуществами подвижной связи, сталкиваются со спамом при передаче сообщений по сети подвижной связи. Спам при передаче сообщений по сети подвижной связи – это термин, обычно используемый в отношении незапрашиваемых сообщений, направляемых с помощью SMS или MMS. основными типами спама на базе коротких сообщений являются:

- мошенничество, связанное с абонированием обслуживания;
- рекламная информация;
- незаконное мошенничество;
- информация порнографического характера.

Эти виды сообщений обычно являются обманными или жульническими и известны также как мошеннические сообщения.

Важно отметить, что в настоящее время с появлением услуг мобильной электронной почты стало общепринятым принимать электронную почту на мобильные устройства, что облегчает ее использование спамерами.

IP-мультимедиа

По мере развития IP-мультимедиа принцип спама стал широко использоваться в отношении IP-мультимедиа, например спам при мгновенной передаче сообщений, спам в IP-телефонии, спам при учете присутствия, спам в блогах, спам в группе сетевых новостей, передача спама в онлайновых играх и т. п. В некоторых случаях существует иная терминология в отношении спама, доставляемого с использованием определенных информационных средств, например SPIM (передача спама при мгновенной передаче сообщений), SPIT (передача спама с помощью интернет-телефонии) и т. д. Кроме того, спам затрагивает также мультимодальные взаимодействия, как, например, новые типы мультимедиа, когда один мультимедийный "спам" может иметь множество представлений на интерфейсе пользователя. Например, то или иное "спамовое" сетевое сообщение может привести к проигрыванию "спамового" аудиоклипа, демонстрированию "спамового" видеоклипа и показу "спамового" текстового сообщения на экране; каждое из них может иметь одно и то же или различное содержание. По этой причине мультимодальности увеличивают подверженность мультимедийному "спаму" и, следовательно, ожидается, что проблема мультимодального "спама" обострится после того, как мультимодальные взаимодействия станут более широко распространенными.

SPIM: Мгновенная передача сообщений является быстроразвивающимся методом удобной и дешевой связи в реальном времени по интернету. В основном, она используется для личной связи. Между тем, приложения мгновенной передачи сообщений все шире применяются на предприятиях. Однако, к сожалению, все больше и больше незаконной информации, такой как вирусы, вредоносные коды и т. п., распространяется при мгновенной передаче сообщений, которая обычно называется SPIM. Несмотря на то что SPIM представляет собой небольшой процент от всего спама, ее объем быстро возрастает.

SPIT: Ряд проблем, выявленных до настоящего времени, включает проблемы, обычно связанные с IP-сетями, и другие более сложные угрозы, такие как представление неправильных данных, перехват информации, атаки типа отказа в обслуживании, относящиеся к VoIP, ввод пакетов и нежелательных сообщений (спам при VoIP или SPIT). Последнее имеет место, главным образом, из-за предоставляемой VoIP возможности направления голосовых сообщений по очень низкой стоимости, что может привести к ситуации, аналогичной уже отмечавшейся в случае распространения спама по электронной почте: большие количества нежелательных сообщений голосовой почты могут быть направлены по всему миру за считанные секунды.

Развитие спама

Спам не ограничивается вышеупомянутыми вариантами. Спам будет повсеместно развиваться по мере все большего внедрения информационно-коммуникационных технологий и приложений. Кроме того, любые технологии и приложения связи могут быть носителями спама, если предлагаемые решения по противодйствию спаму не являются действенными.

7 Общие задачи

Назначением настоящего пункта является описание конечных целей противодействия спаму. Внимание сосредоточено на том, что должно быть достигнуто, а не на определении конкретных шагов по реализации.

Задачи по противодействию спаму:

– Проверка объектов на предмет того, есть ли у них привилегии направлять сообщения или инициировать связь после аутентификации и/или при наличии разрешения.

– Защита адреса и/или другой важной информации о сообщениях или связи, направляемых законными объектами, от сокрытия или маскирования.

– Защита конфиденциальности при передаче информации.

– Ответственность всех объектов за свое собственное поведение при передаче или ретрансляции информации.

– Защита сетей электросвязи от несанкционированных доступа или работы в целях обеспечения эффективной и действенной доступности.

– Предоставление необходимой информации об отправителе в целях обеспечения будущей отслеживаемости.

– В целях обеспечения доступности служебное оборудование должно быть защищено от вирусов и несанкционированного доступа.

– Фильтрация спама и, если необходимо, хранение спама в определенном запоминающем устройстве для обеспечения отслеживаемости и проведения судебного анализа.

– Предоставление платформы обратной связи, которая не только содействует точной и эффективной отчетности об информации, но также используется в целях международного сотрудничества, соблюдения законодательства и т. п.

– Применение общеизвестных международных протоколов для соответствующего обмена информацией и ее распространения, а также противодействии спаму.

Кроме того, решение вышеупомянутых задач должно быть основано на конкретном оборудовании.

8 Технические методы

Для противодействия спаму необходим многосторонний подход, включающий следующие аспекты: определяемая отраслью технология, отраслевая самодисциплина, международное сотрудничество, законодательство, обратная связь и профессиональная подготовка. Среди этих аспектов технология является важной для гарантирования реализации других аспектов. В настоящей Рекомендации внимание сосредоточено, главным образом, на технических методах противодействия спаму.

В целях упрощения анализа, прежде всего, лучше сгруппировать услуги. В соответствии с методом передачи услуги могут быть сгруппированы в класс "хранения и отправки" и класс "связи в реальном времени". Класс "хранения и отправки" включает услуги электронной почты, услуги передачи коротких сообщений по сети подвижной связи, услуги передачи мультимедийных сообщений и т. п. Класс "связи в реальном времени" включает IP-телефонию, IP-факс, мгновенную передачу сообщений и т. п. Методы противодействия спаму для разных услуг различны; поэтому необходим подробный анализ общих технических методов в отношении конкретной услуги.

Для эффективного противодействия спаму рекомендуется внедрить иерархическую модель с различными частями. Более того, чем больше частей реализуется, тем более эффективной является модель. На рисунке 1 показана иерархическая модель противодействия спаму, описываемая следующим образом:

Методы фильтрации	Методы осуществления обратной связи
Методы обслуживания	
Методы, относящиеся к оборудованию	Методы, относящиеся к сетям

Рисунок 1 – Иерархическая модель противодействия спаму

В этой иерархической модели пять частей поделены на три уровня: уровень инфраструктуры, уровень обслуживания и прикладной уровень. На уровне инфраструктуры находятся методы, относящиеся к оборудованию, и методы, относящиеся к сетям, которые являются основой иерархической модели. Реализация этих методов может быть прочным и надежным основанием для технических методов в верхних уровнях. Кстати, методы, относящиеся к оборудованию, и методы, относящиеся к сетям, оказывают влияние друг на друга. Безопасные сети нуждаются в безопасном оборудовании, тогда как для безопасного оборудования необходимы соответствующие сети. Методы обслуживания, которые относятся к уровню обслуживания, являются наиболее важными среди пяти частей, поскольку этот уровень непосредственно отвечает за предоставление услуги. Требования к фильтрации и требования к обратной связи относятся к прикладному уровню, который находится ближе к пользователям в отношении противодействия спаму; однако они взаимодействуют между собой. На рисунке 2 показана взаимосвязь между различными частями:

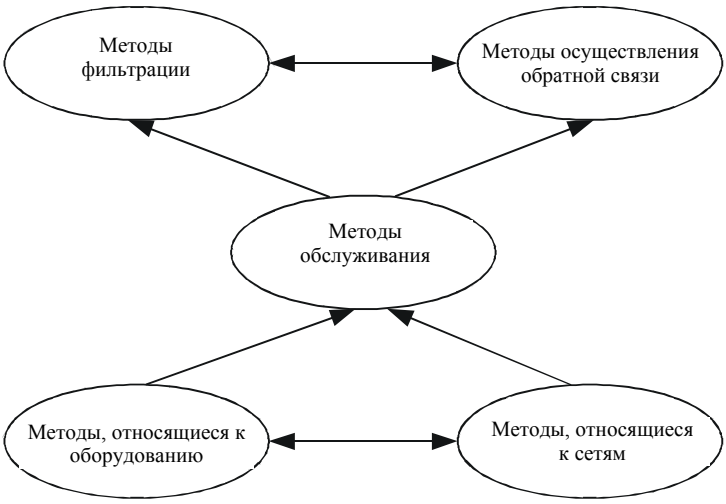

Рисунок 2 – Взаимосвязь между различными частями

Кроме того, для осуществления этих технических методов рекомендуется применять широко известные международные протоколы. Но если все технические методы выполняются, то затраты могут быть слишком большими по сравнению со стоимостью защищаемых услуг. Поэтому весьма важно адаптировать технические методы в соответствии с прикладными сценариями. Помимо этого, предоставление методов противодействия спаму должно осуществляться таким образом, чтобы позволить адаптацию. Ввиду большого количества сочетаний технических методов желательно иметь профили, охватывающие широкий диапазон услуг. Стандартизация в отрасли и деятельность исследовательских организаций будут содействовать повторному использованию решений и продуктов. В то же время возможен более оперативный ввод в действие технических решений для противодействия спаму с меньшими затратами.

8.1 Методы, относящиеся к оборудованию

Оборудование является основанием инфраструктуры противодействия спаму. Поэтому защита оборудования имеет важность для противодействия спаму.

8.1.1 Повышение безопасности программного обеспечения соответствующего оборудования

Те, кто рассылают спам, могут распространять его путем использования компьютерных или сетевых ресурсов, принадлежащих третьим сторонам, как только у этих ресурсов появляются очевидные уязвимости. Ресурсы превращаются в "жертвы" и называются компьютерами-ботнетами или "зомби". Те, кто рассылают спам, могут дистанционно управлять "жертвами" и распространять спам. Действенной мерой является установка безопасных операционной системы и прикладного программного обеспечения, а также своевременное обновление антивирусного программного обеспечения для защиты соответствующего оборудования от вирусов.

8.1.2 Обеспечение различных ролей управления

Ввиду важности служебных систем должно обеспечиваться выполнение различных ролей управления. Они, по крайней мере, должны включать роль управления пользователями, роль управления системой и роль управления проверками. Роль управления пользователями используется для управления конфигурациями администраторов, операторов и аудиторов. Роль управления системой используется для обслуживания и эксплуатации оборудования. Роль управления проверками используется для проверки эксплуатационных журналов и системных журналов. Кроме того, для некоторых конкретных услуг могут понадобиться некоторые конкретные роли управления.

8.1.3 Предоставление эксплуатационных журналов и системных журналов

От системы требуется обеспечивать ведение эксплуатационных журналов и системных журналов, с тем чтобы гарантировать нормальную эксплуатацию системы и поддерживать ее нормальное состояние функционирования.

Эксплуатационные журналы используются для предоставления информации об истории эксплуатации. В них должны быть зарегистрированы все события, относящиеся к входу в систему и эксплуатации. Эксплуатационные журналы должны включать, по крайней мере, следующие поля: имя оператора, время работы, рабочая команда и результат работы.

Системные журналы могут предоставлять информацию об имевших место состояниях функционирования системы. Она, главным образом, включает информацию о качестве работы, информацию об отказах и т. д. Записи в системных журналах могут различаться в зависимости от разных систем и разных услуг.

Однако эксплуатационные журналы и системные журналы не могут использоваться только для технического обслуживания системы, они также помогают администраторам обеспечивать выполнение эксплуатационных процедур, не производя деструктивных действий.

8.1.4 Повышение безопасности и гибкости терминалов

Терминалы являются наиболее важным оборудованием конечных пользователей, которое всегда непосредственно страдает от спама. Поскольку функции всегда различаются в зависимости от типов терминалов, можно представить только общие методы. Они перечислены ниже, но не ограничены следующими методами:

– обеспечение аутентификации и санкционирования, особенно для интеллектуальных терминалов;
– обеспечение черного списка и/или белого списка;
– обеспечение антивирусного программного обеспечения, особенно для интеллектуальных терминалов.

8.2 Методы, относящиеся к сетям

Аналогично требованиям к оборудованию безопасность сетей также является основой для противодействия спаму. Спам может быть заметно снижен путем правильной разработки топологии сети и развертывания различного оборудования обеспечения безопасности, таких как брандмауэры, безопасные маршрутизаторы, безопасные шлюзы и т. д.

8.2.1 Защита служебных сетей от интернета

Различные сетевые услуги подвергаются угрозам со стороны интернета, поскольку большинство этих услуг основано на IP-технологиях с открытыми стандартами.

Необходимы следующие функции:

– Защита служебных сетей от атак со стороны интернета, таких как атаки DoS и DDoS. Служебные сети имеют большую важность и обычно управляются администраторами дистанционно. Поскольку интернет открыт для всех, служебные сети должны быть способны противостоять уязвимостям интернета. Обычно для защиты служебных сетей от этих уязвимостей используются брандмауэры и другие безопасное оборудование.

– Защита сигналов протокола в плоскости управления для блокирования незаконных вторжений. Это особенно важно для VoIP. КТСОП всегда безопасна и надежна, тогда как интернет небезопасен и ненадежен. Поэтому шлюзы VoIP должны быть способны блокировать незаконные сигналы протокола в целях достижения того же уровня безопасности, что и у КТСОП.

8.2.2 Обеспечение механизма дублирования и резервирования для сохранения устойчивости служебной сети

Служебные оборудование и сети имеют настолько важное значение, что должны быть обеспечены дублирующее оборудование и резервные маршруты. Кроме того, механизм дублирования и резервирования должен быть удобным, действенным и экономически приемлемыми.

8.3 Методы обслуживания

Методы обслуживания являются наиболее важной частью иерархической модели, поскольку услуги непосредственно удовлетворяют требованиям пользователей. Но существует так много видов услуг с различными функциями и различными уязвимостями. Поэтому в разных услугах методы обслуживания для противодействия спаму различаются между собой. Однако в отношении разных услуг применяются те же общие методы по противодействию спаму, которые перечислены ниже.

8.3.1 Обеспечение аутентификации

Когда объекты (пользователь или оборудование) осуществляют доступ к услугам, служебные системы должны обеспечивать строгую аутентификацию. С одной стороны, строгая аутентификация может предотвратить доступ недействительного объекта к услугам. С другой стороны, точные записи об аутентификации могут быть использованы в целях обеспечения отслеживаемости. В настоящее время в некоторых странах на сетях подвижной связи достигнуты большие успехи благодаря внедрению механизмов аутентификации и реальных имен.

8.3.2 Обеспечение конфигурируемого адреса ретрансляции

Открытая ретрансляция должна быть выключена, и в служебном оборудовании должна быть принята ограниченная ретрансляция. Служебное оборудование должно обеспечивать наличие списка конфигурируемых адресов ретрансляции. Они ретранслируют сообщения только из разрешенных адресов. Напротив, сообщения от других адресов будут заблокированы.

8.3.3 Обеспечение строгого формата сообщения

В отношении конкретных сообщений, особенно коммерческих, должно быть обеспечено строгое определение формата сообщения. Поэтому служебные системы могут предоставить достаточную информацию для рассмотрения сообщений.

8.3.4 Совместимость с международными стандартами

В целях укрепления возможности присоединения и взаимодействия требуется совместимость протоколов связи услуг с международными стандартами.

8.3.5 Улучшение отслеживаемости спама

С одной стороны, служебные системы должны определять и аутентифицировать объекты (пользователей или оборудование) и получать точную информацию о происхождении объектов, а затем вносить соответствующую информацию в базы данных. С другой стороны, служебные системы должны обеспечивать выполнение функций проверки для отслеживания на основе записей в базах данных.

8.3.6 Обеспечение управления потоками

Системные администраторы могут ограничивать ширину полосы связи или число сообщений, передаваемых на каждом конкретном интервале времени.

8.3.7 Предоставление статистических функций

Статистическая информация обращает внимание системных администраторов на текущее состояние системы, например на объем трафика, и данные об обратившихся пользователях.

8.4 Методы фильтрации

Фильтрация – это наиболее общая антиспамовая технология. Основное преимущество фильтрации состоит в их простоте и гибкости внедрения.

8.4.1 Обеспечение фильтрации спама

Обычно существует два типа фильтрации: фильтрация на основе адресов и фильтрация на основе содержания (включая фильтрацию на основе ключевых слов).

Фильтрация на основе адресов может использоваться как для услуги "хранения и отправки", так и для реальновременной услуги. В отношении услуг "хранения и отправки" фильтрация на основе адресов используется, с тем чтобы отфильтровать сообщения или электронную почту в соответствии с адресами их отправителей. Действенной мерой является недопущение отправки или ретрансляции служебными системами спамовых сообщений и электронной почты. Что касается реальновременных услуг, то фильтрация на основе адресов используется, с тем чтобы блокировать вызовы в соответствии с телефонными номерами или адресами вызывающих абонентов. Вообще говоря, фильтрация на основе адресов эффективна и удобна для противодействия спаму.

Фильтрация на основе содержания может также использоваться как для услуг "хранения и отправки", так и для реальновременных услуг. В отношении услуг "хранения и отправки" фильтрация на основе содержания используется, с тем чтобы отфильтровать сообщения или электронную почту по содержанию или ключевым словам. Что касается реальновременных услуг, то фильтрация на основе содержания используется, с тем чтобы прервать сообщения, основываясь на их содержании. Теоретически фильтрация на основе содержания является более подходящей по сравнению с фильтрацией на основе адресов. Однако фильтрация на основе содержания всегда требует расхода большого объема ресурсов, а точность фильтрация на основе содержания тесно связана с алгоритмом анализа.

Ни один из двух методов фильтрации не может отфильтровать весь спам. Поэтому лучше использовать оба метода одновременно. Кроме того, служебное оборудование должно обеспечивать фильтрацию вирусов.

8.4.2 Обеспечение механизма архивирования/записи для фильтрации спама

В случае услуг "хранения и отправки" служебное оборудование должно автоматически архивировать спам. В случае реальновременных услуг служебное оборудование должно автоматически записывать профили спама. Та и другая информация хранится для возможного будущего запроса.

8.4.3 Требования к качеству осуществления фильтрации спама

Качество работы представляет собой очень важную характеристику фильтрации спама. Ложноположительное отношение и ложноотрицательное отношение являются наиболее важными факторами для оценки качества осуществления фильтрации спама. Термин "ложноположительный" относится к отрицательным случаям, обнаруженным при отсутствии отрицательных случаев, а термин "ложноотрицательный" относится к положительным случаям, обнаруженным при наличии отрицательных случаев. Поэтому ложноположительное отношение – это доля отрицательных случаев, о которых ошибочно сообщено как о положительных случаях. Ложноотрицательное отношение – это доля положительных случаев, о которых ошибочно сообщено как об отрицательных случаях. В таблице 1 представлен результат фильтрации спама.

Таблица 1 – Результат фильтрации спама

		Реальные условия	
		Положительные случаи	**Отрицательные случаи**
Результат испытания	Обнаружены положительные случаи	A	B
	Обнаружены отрицательные случаи	C	D
ПРИМЕЧАНИЕ. – Положительный случай – это спам, отрицательный случай – отсутствие спама.			

Общее число испытательные случаев – T.

T = A + B + C + D

Количество ложноположительных случаев – B.

Количество ложноотрицательных случаев – C.

Ложноположительное отношение = B / (B + D)

Ложноотрицательное отношение = C / (A +C)

Ложноположительное отношение и ложноотрицательное отношение являются строго коррелятивными. Обычно, чем больше ложноположительное отношение, тем меньше ложноотрицательное отношение. Однако какое отношение имеет большую важность, зависит от фактических условий. В коммерческой практике лучше увеличить ложноотрицательное отношение, чем ложноположительное отношение.

8.4.4 Обеспечение простой и гибкой конфигурации фильтрации

С учетом многочисленности и разнообразия спама должна быть обеспечена простая и гибкая конфигурация фильтрации, например удобные для пользователя интерфейсы, выбираемые методы конфигурации и т. д. Кроме того, общие правила фильтрации должны быть сгруппированы по различным категориям фильтрации, данные о которых будут размещены в базах данных или хранилищах. При необходимости такие категории фильтрации могут быть легко выбраны и использованы.

8.4.5 Как можно большее снижение затрат на фильтрацию

Лучше всего фильтровать спам как можно раньше до того, как он займет большой объем ресурсов. Поэтому спам должен фильтроваться в начале передачи, и он не должен попадать в последующее служебное оборудование.

8.4.6 Обеспечение черных и белых списков

Существует два типа фильтрации на основе адресов: белые списки допустимых отправителей и черные списки тех, кто подозревается в распространении спама.

Черные списки основаны на перечислении отправителей спама. Этот список может включать названия машин, IP-адресов, MAC-адресо или других электронных адресов. Система фильтрации будет фильтровать сообщения или блокировать связь в соответствии с черными списками.

Белые списки основаны на перечислении допустимых отправителей. Механизм работы аналогичен черным спискам, с той разницей, что белые списки – это списки допустимых адресов.

В действительности, метод белых/черных списков обычно является довольно грубым для большинства пользователей. Однако такие методы очень просты и не требуют значительных ресурсов. В целях повышения эффективности фильтрации фильтры должны обеспечивать работу с белыми и черными списками, особенно с черными списками в целях противодействия спаму.

8.4.7 Обеспечение фильтрации многомодальных сообщений

В отношении многомодальных сообщений требуется:

– обеспечение возможности полного блокирования определенных многомодальных сообщений;

– обеспечение возможности изъятия определенных многомодальных вложений в сообщениях или части многомодального содержания мультимедийного сообщения;

– обеспечение возможности фильтрации входящих (принимаемых) и/или исходящих (направляемых) многомодальных сообщений.

8.5 Методы осуществления обратной связи

Конечные пользователи являются конечными получателями спама, возможными жертвами вирусов и мошенничества. Участие конечных пользователей будет полезно для эффективного и действенного противодействия спаму. Поэтому при разработке решений противодействия спаму должна учитываться обратная связь с конечными пользователями. Однако участие конечного пользователя в механизме обратной связи должно быть добровольным.

8.5.1 Обеспечение платформы обратной связи в отношении спама

Лицам, пострадавшим от вредного спама, должна быть предоставлена возможность обращения за помощью. Права физических лиц, получающих спам, должны быть защищены законодательством. Поэтому в их распоряжение необходимо предоставить средства для обращения за помощью. Следует создать механизмы для обеспечения этой цели, в том числе способы сообщения надлежащему органу о нарушениях, связанных со спамом. Такие процедуры обработки сообщений обратной связи должны быть прозрачными, действенными и эффективными. Такую роль может играть платформа обратной связи.

8.5.2 Предоставление стандартных форматов для обмена данными обратной связи

Необходимо, чтобы платформа обратной связи записывала информацию обратной связи в принятом стандартном формате записи. Таким образом, различные операторы и структуры смогут обмениваться данными обратной связи. Благодаря обмену данными обратной связи могут быть получены основные адреса тех, кто рассылает спам, которые могут быть использованы в черных списках.

9 Оценка системы

Для оценки действенности и эффективности технологий и систем противодействия спаму должны учитываться следующие аспекты:

– Ложноположительное отношение.

– Ложноотрицательное отношение.

– Затраты: Методы противодействия спаму должны быть гибкими в целях предоставления индивидуальных решений. Ввиду большого числа возможных сочетаний стратегий желательно располагать профилями, охватывающими широкий спектр услуг.

– Взаимодействие существующей системы: Непременное условие противодействия спаму – это гарантирование нормальной работы существующей системы. Другими словами, внедрение решений по противодействию спаму не может нарушить работу существующих систем.

– Соответствие международным стандартам: Технические решения должны быть основаны предпочтительно на международных стандартах в целях достижения межсетевого взаимодействия и распространения в мировом масштабе. Кроме того, стандартизация будет содействовать повторному использованию решений и компонентов. Это поможет быстро и с небольшими затратами внедрять новые решения по противодействию спаму.

Перечисленные выше аспекты являются общими критериями оценки мер по противодействию спаму. В реальной служебной сети необходимо учитывать другие конкретные аспекты.

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-ITU-T Q-Sup.49] Recommendation ITU-T Q-series Recommendations – Supplement 49 (2004), *Technical Report TRQ.2840: Signalling requirements to support IP telephony*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.811] Рекомендация МСЭ-Т X.811 (1995 г.) | ИСО/МЭК 10181-2:1996, *Информационная технология – Взаимосвязь открытых систем – Структуры безопасности для открытых систем: структура аутентификации*.

[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 2635] IETF RFC 2635 (1999), *DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*)* <http://www.ietf.org/rfc/rfc2635.txt>.

[b-IETF RFC 2821] IETF RFC 2821 (2001), *Simple Mail Transfer Protocol* <http://www.ietf.org/rfc/rfc2821.txt>.

[b-IETF RFC 3685] IETF RFC 3685 (2004), *SIEVE Email Filtering: Spamtest and VirusTest Extensions* <http://www.ietf.org/rfc/rfc3685.txt>.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	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

Отпечатано в Швейцарии
Женева, 2009 г.