



МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1240

(04/2008)

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

Безопасность электросвязи

**Технологии, применяемые
при противодействии спаму,
рассылаемому по электронной почте**

Рекомендация МСЭ-Т X.1240

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.1240

Технологии, применяемые при противодействии спаму, рассылаемому по электронной почте

Резюме

В Рекомендации МСЭ-Т X.1240 дается определение основных понятий, относящихся к спаму, рассылаемому по электронной почте, указываются его характеристики и последствия, а также технологии, применяемые при противодействии такому спаму. Кроме того, в ней представляются современные технические решения и связанная с этим деятельность различных организаций, занимающихся разработкой стандартов, и соответствующих организаций, занимающихся вопросами противодействия спаму, рассылаемому по электронной почте. В ней приводятся руководящие указания и информация для пользователей, желающих выработать технические решения для противодействия спаму, рассылаемому по электронной почте. Данная Рекомендация будет использоваться в качестве основы для дальнейшей разработки технических Рекомендаций по противодействию спаму, рассылаемому по электронной почте.

Источник

Рекомендация МСЭ-Т X.1240 была утверждена 18 апреля 2008 года 17-й Исследовательской комиссией МСЭ-Т (2005–2008 гг.) в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

ПРЕДИСЛОВИЕ

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

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

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

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

ПРИМЕЧАНИЕ

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

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

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

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

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: <http://www.itu.int/ITU-T/ipr/>.

© ITU 2009

Все права сохранены. Ни одна из частей данной публикации не может быть воспроизведена с помощью каких бы то ни было средств без предварительного письменного разрешения МСЭ.

СОДЕРЖАНИЕ

	Стр.
1 Сфера применения	1
2 Справочные документы	1
3 Определения	1
4 Сокращения и акронимы	1
5 Соглашения.....	2
6 Введение в вопрос противодействия спаму, рассылаемому по электронной почте.....	2
6.1 Понятие и характеристики спама.....	2
6.2 Подходы к противодействию спаму, рассылаемому по электронной почте	3
7 Антиспамовые технологии.....	4
7.1 Краткое описание	4
7.2 Значение инструментальных средств /технологических условий	5
7.3 Комбинированные тесты	5
7.4 Типы антиспамовых технологий	6
7.5 Существование домена отправителя и выявление ответа	7
7.6 Существование записи указателя (PTR).....	7
7.7 "Черные"/"белые списки"	7
7.8 Адрес сервера-отправителя, рассматриваемый либо в качестве "динамического" либо "стационарного" адреса	8
7.9 Фильтрация	8
7.10 HELO/CSV	10
7.11 Составление "серых списков"	10
7.12 Метки/пароли.....	10
7.13 Различные методы	11
7.14 Как использовать этот анализ технологий, и факторы, которые следует принимать во внимание	12
7.15 Отказ в сеансе SMTP.....	12
7.16 Молчаливый отказ.....	13
7.17 Отказ путем направления DSN (уведомление о статусе доставки или "сбой") .	13
7.18 Доставка в почтовый ящик для спама	13
7.19 Маркировка.....	13
Дополнение I – Деятельность по противодействию спаму, рассылаемому по электронной почте	14
I.1 Введение.....	14
I.2 Международная деятельность в области противодействия спаму	14
I.3 Разработка технических спецификаций для противодействия спаму.....	16
I.4 Перечень промышленных альянсов и инициатив в области противодействия спаму	17
Библиография	21

Введение

В соответствии с просьбой, содержащейся в Резолюции 52 ВАСЭ 2004 года "Противодействие распространению спама техническими средствами", была проведена работа в области стандартизации для разработки Рекомендаций МСЭ-Т, помогающих противодействовать спаму, рассылаемому по электронной почте, техническими средствами. Настоящая Рекомендация является первой в серии Рекомендаций МСЭ-Т по противодействию спаму, рассылаемому по электронной почте, которые состоят из руководящих указаний, требований, технической основы и технических стратегий. Другие Рекомендации МСЭ-Т по противодействию спаму для мультимедийных приложений, основанных на IP, таких как IP-телефония, мгновенный обмен сообщениями и конференция, будут представлены в виде отдельных документов.

Рекомендация МСЭ-Т X.1240

Технологии, применяемые при противодействии спаму, рассылаемому по электронной почте

1 Сфера применения

В настоящей Рекомендации дается описание технологий, применяемых при противодействии такому спаму, рассылаемому по электронной почте. В ней представляются современные технические решения и связанная с этим деятельность различных организаций, занимающихся разработкой стандартов, и соответствующих организаций, занимающихся вопросами противодействия спаму, рассылаемому по электронной почте. Цель настоящей Рекомендации состоит в том, чтобы предоставить полезную информацию для пользователей, желающих выработать технические решения для противодействия спаму, рассылаемому по электронной почте. Данная Рекомендация будет использоваться в качестве основы для дальнейшей разработки технических Рекомендаций по противодействию спаму, рассылаемому по электронной почте.

ПРИМЕЧАНИЕ. – Использование в настоящей Рекомендации термина "идентичность" не указывает на его абсолютное значение. В частности, он не означает какого-либо подтверждения правильности.

2 Справочные документы

Не имеются.

3 Определения

В настоящей Рекомендации даны определения следующих терминов:

3.1 фишер: Организация или лицо, организующие фишинговые атаки.

3.2 фишинг: В фишинговых атаках используются как приемы психологической атаки, так и технические ухищрения в целях хищения данных опознания личности потребителя и данных финансового счета. Приемы психологической атаки используют "фиктивную" электронную почту, для того чтобы вывести потребителей на фальшивые веб-сайты, предназначенные для получения обманном образом финансовых данных пользователей, например номеров кредитных карт, имен пользователей, их паролей и номеров карт социального обеспечения. Совершив хищение фирменных знаков банков, предприятий розничной электронной торговли и компаний-эмитентов кредитных карт, фишеры часто убеждают пользователей ответить. Технические ухищрения основываются на внедрении криминального программного обеспечения в ПК с целью прямого хищения данных, часто с использованием троянского клавиатурного шпионского программного обеспечения.

3.3 спам: Значение слова "спам" зависит от того, что понимается под конфиденциальностью в каждой стране, и от того, что представляет собой спам с точки зрения национальных технологий, а также социально-экономической и практической точек зрения. В частности, с развитием технологий значение этого слова изменяется, становясь все шире и открывая все новые возможности для злоупотреблений электронными сообщениями. И хотя согласованного на международном уровне определения спама не существует, этот термин обычно используется для обозначения рассылаемых в массовом порядке по электронной почте или подвижной связи незапрашиваемых сообщений, целью которых является, как правило, продвижение продуктов или услуг коммерческого характера.

3.4 спамер: Организация или лицо, создающее и рассылающее спам.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

API	Application Programming Interface	Прикладной программный интерфейс
DKIM	DomainKeys Identified Mail	Идентификация почты с использованием доменных ключей
CSV	Certified Server Validation	Сертифицированная проверка сервера
DNS	Domain Name System	Система наименований доменов

DSN	Delivery Status Notification		Уведомление о статусе доставки
HTML	HyperText Markup Language		Язык разметки гипертекста
IM	Instant Messaging		Мгновенный обмен сообщениями
ISP	Internet Service Provider	ПУИ	Поставщик услуг интернета
META	Message Enhancements for Transmission Authorization		Повышение качества сообщений для получения разрешения на передачу
MMS	Multimedia Messaging Service		Услуга передачи мультимедийных сообщений
MTA	Mail Transfer Agent		Агент передачи сообщений электронной почты
OECD	Organization for Economic Co-Operation and Development	ОЭСР	Организация экономического сотрудничества и развития
OPES	Open Pluggable Edge Services		Открытые встраиваемые пограничные услуги
PGP	Pretty Good Privacy		Надежная конфиденциальность
PTR	Pointer Record		Запись указателя
SMS	Short Message Service		Услуга передачи коротких сообщений
SMTP	Simple Mail Transfer Protocol		Упрощенный протокол передачи сообщений электронной почты
SPF	Sender Policy Framework		Структура политики отправителя
TEOS	Trusted Email Open Standard		Открытый стандарт для проверенной электронной почты

5 Соглашения

Не имеются.

6 Введение в вопрос противодействия спаму, рассылаемому по электронной почте

6.1 Понятие и характеристики спама

Хотя общепринятое определение спама отсутствует, обычно этим термином обозначают рассылаемые по электронной почте или подвижной связи (SMS, MMS) незапрашиваемые сообщения, а также услуги мгновенной передачи сообщений, целью которых является, как правило, продвижение продуктов или услуг коммерческого характера.

Хотя наиболее широко признанной формой спама является спам, рассылаемый по электронной почте, этот термин применяется также к аналогичным злоупотреблениям в других средствах передачи информации, например спаму в виде сообщений на мобильные телефоны, спаму в интернет-телефонии, спаму в виде мгновенной передачи сообщений, спаму в виде группы новостей Usenet (сетевые новости), спаму в сетевой поисковой машине и спаму в блоге, размещенном в сети. Диапазон содержаний спам-сообщений колеблется от рекламы товаров до отвратительного порнографического материала. Спам, рассылаемый по электронной почте, оказывает на пользователей услуг электронной почты и поставщиков услуг интернета неблагоприятное воздействие различного рода:

- получатели спама и поставщики услуг интернета тратят много времени, средств и усилий, для того чтобы выявить, удалить и отфильтровать спам;
- спам, рассылаемый по электронной почте, может включать вводящие в заблуждение сообщения, прельщающие получателей спама, или содержать материал для взрослых, не приемлемый для детей;
- пользователи услуг электронной почты и поставщики услуг интернета испытывают избыточный расход ресурса интернета и памяти;
- распространение вирусов и шпионских программ может представлять угрозу для безопасности интернета;
- спам, рассылаемый по электронной почте, затрудняет распознавание обычной и важной электронной почты.

В последнее время все чаще наблюдается такое явление, как использование спама для поддержки мошеннической и уголовно наказуемой деятельности, включая попытки завладения финансовой информацией (например, номерами счетов и паролями) путем направления сообщений, якобы исходящих от солидных компаний ("спуфинг брендов" или "фишинг"), а также для распространения вирусов и червей.

Фишинговые атаки используют как приемы психологической атаки, так и технические ухищрения в целях хищения данных опознания личности потребителя и данных финансового счета. Приемы психологической атаки используют "фиктивную" электронную почту, для того чтобы вывести потребителей на фальшивые веб-сайты, предназначенные для получения обманным образом финансовых данных пользователей, например номеров кредитных карт, имен пользователей, их паролей и номеров карт социального обеспечения. Совершив хищение фирменных знаков банков, предприятий розничной электронной торговли и компаний-эмитентов кредитных карт, фишеры часто убеждают пользователей ответить. Технические ухищрения основываются на внедрении криминального программного обеспечения в ПК с целью прямого хищения данных доступа, часто с использованием троянского клавиатурного шпионского программного обеспечения. Криминальное программное обеспечение в виде фарминга сводится к автоматическому перенаправлению пользователей на фальшивые сайты или серверы-посредники, обычно посредством незаконного присвоения или порчи системы наименований доменов (DNS).

Стремясь избежать обнаружения, сами спамеры проявляют большую изобретательность, в том числе фальсифицируя источник электронной почты и располагая в случайном порядке контент, с тем чтобы пройти через спам-фильтры. Проблема выросла до таких масштабов, что ряд стран в спешном порядке приступили к принятию законов по борьбе со спамом, хотя при этом используются различные национальные подходы и средства. В то же время все шире признается тот факт, что вопрос, касающийся противодействия спаму, требует координации и сотрудничества на международном уровне.

6.2 Подходы к противодействию спаму, рассылаемому по электронной почте

Поскольку спам, рассылаемый по электронной почте, наносит большой ущерб пользователям услуг электронной почты, поставщикам услуг интернета (ПУИ) и операторам сетей, во многих странах были разработаны технологии и приняты регламентарные положения, для того чтобы оказать помощь в противодействии спаму. Однако трудно эффективно противодействовать спаму посредством лишь одной меры, например фильтрации или юридического наказания, поскольку противодействие спаму – непростая проблема. Поэтому для того чтобы эффективно противодействовать спаму, необходимо одновременно применять различные методы:

- Регулирование: Должны быть приняты правовые нормы по борьбе со спамом, для того чтобы облегчить возможность соответствующего реагирования пользователями услуг на спам, рассылаемый по электронной почте, и усилить воздействие антиспамовых технологий, таких как фильтрация. Кроме того, регулирование может помочь защитить пользователей услуг и поставщиков услуг интернета от незаконного спама.
- Технологии: Разработка антиспамовых технологий имеет важное значение для эффективного противодействия большому количеству спама, рассылаемого по электронной почте. Необходимо разработать различного вида технологии для предотвращения рассылки спама, а также эффективного выявления и отфильтровывания спама.
- Действия отрасли: Участники со стороны отрасли, например поставщики услуг интернета или операторы сетей, должны разработать и установить различные виды антиспамовых технологий, в том числе "черные" или "белые списки" и функции фильтрации. Поставщики услуг интернета могут также выработать политику в отношении противодействия спаму, рассылаемому по электронной почте.
- Международное сотрудничество: Международное сотрудничество является необходимым, поскольку сети электросвязи не имеют границ, а спам по своему происхождению и воздействию имеет международный характер. Международное сотрудничество полезно также для обмена информацией о принятии эффективных норм по регламентации, развития антиспамовых технологий, а также для обучения пользователей и поставщиков услуг.
- Обучение: Для того чтобы минимизировать вред, который причиняет спам, рассылаемый по электронной почте, важное значение имеет обучение пользователей и поставщиков услуг интернета. Обучение должно помочь пользователям электронной почты научиться

принимать надлежащие действия в отношении спама, рассылаемого по электронной почте, а поставщиков услуг интернета – осваивать методы и технологии по борьбе со спамом.

Из числа различных мер борьбы со спамом, представленных выше, в настоящей Рекомендации будут рассмотрены в основном технические меры противодействия спаму, такие как разработка и применение антиспамовых технологий.

7 Антиспамовые технологии

В докладе целевой группы ОЭСР по проблемам спама [b-OECD TF] представлен ряд элементов для противодействия спаму, рассылаемому по электронной почте, включая регламентарные подходы, обеспечение исполнения законов и технические решения. В настоящей Рекомендации в данном пункте содержится ссылка на часть этого доклада – "Элемент IV – антиспамовые технологии". Рассмотрение этого вопроса необходимо, поскольку набор инструментов по борьбе со спамом был опубликован в мае 2006 года и с тех пор не обновлялся.

В настоящем разделе рассматриваются различные виды технологий по борьбе со спамом и возможности, которыми они обладают, а также методы, которые необходимо использовать при получении спама. Всякая попытка эффективной борьбы со спамом должна сопровождаться разумным управлением целым рядом технологий в их взаимодействии. Ни один из вышеупомянутых методов не даст полностью удовлетворительных результатов, если они будут использоваться автономно. Если ряд технологий по борьбе со спамом будет эффективно использоваться во взаимодействии друг с другом, то это может привести к радикальному уменьшению уровня спама, воздействующего на систему.

7.1 Краткое описание

Спам ставит сложные технические проблемы, и поэтому решения по его устранению должны быть подкреплены соответствующими техническими мерами. Хотя действия правительства и законодательные меры являются полезными, их недостаточно, для того чтобы решить проблемы, которые ставит спам. В действительности, спам является прежде всего технической проблемой, возникающей в результате бреши в протоколе SMTP. Технический характер проблемы создает особенно серьезные трудности для тех, кто следит за соблюдением закона при выявлении спамеров, а следовательно, и их наказании.

Несмотря на различия в определении спама, существуют различные технологии и методы, которые могут быть использованы для решения проблемы нежелательной электронной почты. В данном пункте содержится нейтральный обзор различных видов технических инструментальных средств и методов, а также факторов, которые необходимо учитывать перед тем, как они могут быть использованы. В нем, в особенности, представлены инструментальные средства в отличие от решений. Хотя технологии разработаны для того чтобы решить многие из проблем, создаваемых спамом, и действительно могут "решить" некоторые конкретные вопросы, связанные со спамом, комплексное решение проблемы спама может быть достигнуто только посредством многостороннего подхода, включающего вопросы технологий, политики (в том числе регламентацию, когда это целесообразно), практической деятельности и образования.

Антиспамовые инструментальные средства работают на многих уровнях, – в месте происхождения, в магистральной сети, в шлюзе и в компьютере получателя, и могут использоваться отдельно или в сочетании с другими средствами. С обновленной информацией и ресурсами можно ознакомиться на веб-сайте, содержащем комплект материалов: www.oecd-antispam.org.

Данный пункт адресован, в частности, администраторам почтовых серверов, для того чтобы они могли лучше понять сильные и слабые стороны каждого метода фильтрации и выбрать программное обеспечение, соответствующее их политике и потребностям в отношении электронной почты, в зависимости от планируемой ими архитектуры. Основное внимание в настоящем пункте уделяется практике в отношении входящей почты, хотя практика, направленная на сокращения исходящего спама, также будет полезной. Помимо операторов принимающих серверов, важную роль должны сыграть операторы отправляющих серверов. Операторы отправляющих серверов могут использовать ограничение исходящей скорости и блокирование 25-го порта, а также другие меры для уменьшения объема спама, рассылаемого их серверами.

Инструментальные средства борьбы со спамом должны быть ориентированы как на электронную почту, так и на режим, в котором она работает. В условиях действия этих многочисленных факторов многие инструменты и методы основываются на наборе правил или допущений, работающих

отдельно или в каком-либо сочетании для выявления подозрительной почты. Со временем масштабы спама выросли и уже стали включать вирусы и вредоносные программные средства. Это потребовало разработки технологий защиты, выходящих за пределы инструментария, основанного на тексте, и предусматривающих анализ поведенческих и контекстуальных факторов при определении того, принять или не принять ту или иную конкретную почту или даже саму попытку установления связи. С учетом возросшей угрозы для безопасности, которую представляет собой спам, мы рассчитываем, что антиспамовые технологии либо будут содержать больше современных технологий в области безопасности и аутентификации, либо должны будут работать во взаимодействии.

7.2 Значение инструментальных средств/технологических условий

Одни из инструментальных средств/технологий, рассматриваемых в данном пункте, специально предназначены для внедрения на входе платформы электронной почты, в то время как другие целесообразнее разворачивать после получения сообщений, однако до того, как почта будет доставлена конечному потребителю. Важно отметить, что некоторые инструментальные средства расположены в компьютере получателя. На каждом этапе применения фильтра цель введения того или иного правила может состоять в отказе или непринятии электронного сообщения либо просто в его маркировке или доставке в почтовый ящик для спама пользователя.

Поэтому значимость и полезность каждого правила можно оценить только исходя из конкретных условий, в которых оно применяется, уровня, на котором оно применяется в процессе распространения сообщений, а также того, что в конечном итоге происходит с сообщениями.

7.3 Комбинированные тесты

В основе любого подхода, направленного на борьбу со спамом, должна лежать технология. Каждый должен понимать, что ни одна из технологий, которые будут рассмотрены в пунктах ниже, не будет действовать как "серебряная пуля" или универсальное решение проблем, создаваемых спамом. Все технологии являются, скорее, взаимодополняющими и будут наиболее эффективными лишь тогда, когда будут использоваться во взаимодействии друг с другом. Комбинирование ряда технологий необходимо для уменьшения вредного воздействия спама на систему.

Тесты не обязательно проводить в режиме "все или ничего". Напротив, целесообразнее скомбинировать тесты, с тем чтобы перехватить максимальный объем спама, рассылаемого по электронной почте, при этом сводя к минимуму количество законных электронных сообщений, перехваченных или не принятых непреднамеренно.

- Отказ в режиме "все или ничего" – это один из возможных ответов служб, использующих "черный список". Любое сообщение, не прошедшее тест, получает отказ. Однако наличие ошибки зависит от того, в каком месте в процессе распределения расположен контролирующий инструмент.
- Привилегия доступа – это один из возможных ответов получаемых от серверов, использующих "белый список". Любое сообщение, прошедшее тест, принимается. При этом риск отказа законного сообщения отсутствует, однако может произойти ошибка нераспознавания. Например, "белый список" домена не представляет большого интереса, если домен отправителя не аутентифицирован (посредством структуры политики отправителя или идентификации почты с использованием доменных ключей (DKIM)).
- Считается, что многие спам-сообщения или "черви" происходят из признанных торговых марок в надежде получить привилегию доступа.
- Количественная оценка – это то, как программы комбинируют свои тесты. Количественная оценка настоятельно рекомендуется, так как позволяет избежать неудобств режима "все или ничего". Однако она является дорогостоящей с точки зрения машинных ресурсов и из-за постоянной необходимости обновления ее коэффициентов, для того чтобы максимально увеличить число обращений и свести к минимуму количество случаев ложного распознавания.

Традиционный метод заключается в проведении нескольких испытаний в режиме "все или ничего" и последующей оценке сообщений, которые были допущены.

7.4 Типы антиспамовых технологий

7.4.1 Аутентификация электронной почты

Методы аутентификации почты относятся к той категории контролирующих инструментов, которые, хотя и помогают в борьбе со спамом, не являются специальными антиспамовыми технологиями.

Это может пояснить следующая аналогия. Удостоверения личности не являются надежным признаком, поскольку преступники также могут иметь удостоверение личности. Однако требование прозрачности принесет больше пользы законным отправителям, чем спамерам.

7.4.2 SPF и/или идентификатор отправителя

Главным фактором, способствующим быстрому распространению спама, является способность спамеров прятать подлинный обратный адрес своих сообщений. Архитектура электронной почты не предполагает наличия предварительного контакта между отправителем и получателем. Поэтому рассчитывать на систематическую аутентификацию не представляется возможным. Эта проблема вызывает растущее беспокойство, поскольку мошенники, прибегающие к фишингу, используют вымышленные адреса для "выживания" у получателей сообщений информации о номерах их кредитных карт и других личных сведений.

Эта технология еще только начинает применяться, и поэтому не она стандартизирована, а аутентификация осуществляется путем маркировки электронных сообщений, подлинных отправителей которых нельзя проверить. Принимающий сервер может заблокировать неаутентифицированные сообщения, однако данная технология не требует, чтобы он делал это. Эта технология лишь маркирует соответствующее сообщение. Главное преимущество аутентификации уровня домена состоит в том, что она позволит значительно сократить количество случаев ложного распознавания и обеспечить более надежную фильтрацию на основе оценки репутации. Повышение затрат отправителей компенсируется гарантированной доставкой сообщения, если отправители аутентифицируются и используют соответствующую систему на законных основаниях, или возможностью привлечения к юридической ответственности за ненадлежащее использование фирменного знака. Детали процесса проверки различаются в зависимости от выбранной модели, и в настоящее время существует несколько моделей аутентификации сервера. Двумя наиболее распространенными моделями являются структура политики отправителя (SPF) и идентификатор отправителя (Sender-ID).

Эти два метода могут быть рассмотрены совместно, так как они имеют несколько общих характеристик. Однако вопрос выбора между ними является не столь простым.

SPF и идентификатор отправителя могут быть использованы для тестирования того, разрешается ли серверу электронной почты направлять электронную почту от имени данного домена. Это делается путем публикации записи в системе наименований доменов (DSN), в которой содержится перечень разрешенных серверов электронной почты для того или иного домена. Эти два метода отличаются прежде всего по выбору тестируемого идентификатора. SPF тестирует MAIL FROM [b-IETF RFC 2821] оболочки, тогда как идентификатор отправителя тестирует заголовки [b-IETF RFC 2822].

Администраторы серверов осуществляют два вида действий: публикуют записи SPF в DNS и тестируют их на входе. Согласно недавнему отчету компании [B-Lyris] использование неправильной записи SPF в настоящее время значительно ухудшает шансы доставки сообщений.

Аутентификация электронной почты путем проверки IP-адресов сервера отправителя поможет уменьшить количество спама и устранить его в будущем. Это может потребовать создания услуг более высокого по сравнению с аутентификацией уровня, например частных "белых списков", услуг оценки репутации и сертификации.

7.4.3 DKIM и/или META

DKIM и повышение качества сообщений для получения разрешения на передачу (META) используются для аутентификации домена отправителя с помощью криптографической подписи, добавляемой автоматически сервером электронной почты. Аутентификация электронной почты путем криптографической подписи сообщения должна помочь уменьшить количество спама и устранить его в будущем.

DKIM является наиболее рекламируемой из этих моделей. В основе функционирования этой модели лежит требование цифровой подписи или личного ключа для всех исходящих сообщений. Входящие сообщения аутентифицируются на уровне домена и сервера почты, обеспечивая совпадение личного

ключа и открытого ключа, который уже имеется в файле. Этот метод гарантирует то, что сообщение может исходить только от исходящего поставщика услуг интернета. DKIM полезна для домена отправителя, обеспечивая доставку сообщений поставщикам услуг интернета, которые эксплуатируют алгоритм DKIM. DKIM недавно была утверждена целевой группой по инженерным проблемам интернета в качестве RFC (запроса для комментариев), тем самым превратив ее в стандарт IETF.

7.5 Существование домена отправителя и выявление ответа

Многие спамеры направляют почту с несуществующими адресами отправителей. Контролирующий инструмент может быть использован, для того чтобы отклонить эти сообщения, например директива Postfix reject_unknown_sender_domain или директива j-chkmail BadMX. Другая возможность состоит в проверке достоверности записи для входящего сервера (MX) для домена, указанного в поле "from" соответствующего сообщения. Некоторые спамеры устанавливают фиктивную запись MX, для того чтобы избежать гневных ответов протеста (например, MX переходит в 127.0.0.1, что подразумевает местного отправителя).

Эти контролирующие инструменты требуют небольшого объема трафика DNS, что, вероятно, и будет наблюдаться, во всяком случае во время ответа, и они могут также отсечь некоторое количества спама.

7.6 Существование записи указателя (PTR)

Запись PTR DNS может быть использована для преобразования IP-адреса сервера отправителя в какое-либо имя, хотя и без необходимой проверки соответствия этого имени домену отправителя.

Добавление таких записей не всегда находится под контролем домена отправителя (например, если IP не делегировал addr.arpa), который, даже в том случае если он является законным, может оказаться неспособным выполнить это обязательство. Эти записи могут быть использованы для определения источника электронного сообщения, а также того, можно ли ему доверять и в какой степени. Они могут также использоваться для определения того, исходит ли та или иная почта от стационарного IP-адреса, или для того чтобы вернуть ошибочное сообщение на правильный сервер.

7.7 "Черные"/"белые списки"

Традиционная фильтрация, а также жалобы по поводу отслеживания со стороны пользователей в конечном итоге могут привести к созданию "белых списков" приемлемых отправителей и "черных списков" подозреваемых спамеров. Подход, связанный с использованием "белых"/"черных" списков, часто является слишком радикальным решением, чтобы быть приемлемым для большинства пользователей. Создание "белых списков" требует больших затрат времени и постоянного обновления содержащейся в них информации. "Черные списки" требуют аналогичного контроля. Все списки нуждаются в механизмах и процедурах обновления, чтобы исключить жалобы по поводу в случаях ложного распознавания и мошенничества при составлении списков. Спуфинг и открытые ретрансляции также могут поставить вопросы, связанные с созданием видимости того, что почта исходит от того или иного источника.

"Черные списки" основываются на принципе перечисления источников спама. Такой список может включать имена машин, IP-адреса или электронные адреса. Он может быть подготовлен какой-либо организацией для совместного использования или устанавливаться и вестись конкретным сервером, использующим его для своих собственных нужд.

При наличии действующих агентов передачи сообщений электронной почты (MTA) этот тест может быть осуществлен в сеансе SMTP и поэтому привести к неприятию сообщения даже до того, как оно будет отправлено. Некоторые списки содержат открытые ретрансляции, которые сами не ответственны за отправку спама. Конфигурация их открытых ретрансляций может рассматриваться платформами, которым направляются соответствующие сообщения, как незаконное поведение.

Качество "черных списков" значительно колеблется, в зависимости от профессионализма того, кто их составляет. Многие списки ведутся плохо, остаются без внимания или оказываются в сомнительном состоянии: имена могут добавляться в спешке, применяемые критерии могут быть непонятными, а исключение из списка может оказаться фактически невозможным или производиться исключительно на платной основе. Такая проблема возникает главным образом из-за отсутствия кодекса поведения или какого-либо регулирования, для того чтобы навести дисциплину и ограничить функционирование "черных списков". Если такое решение будет использоваться в будущем, то

потребуется совместные усилия по созданию перечня рекомендуемых норм, четко определяющих случаи, при которых адреса могут быть занесены в "черные списки", а также условия, при которых они будут из них исключаться.

"Черные списки" будут неизбежно содержать неточности, которые не позволят законным сообщениям дойти до потребителя. Эта проблема, известная как проблема ложного распознавания, вызвала законные нарекания со стороны законных отправителей, считавших, что они были ошибочно занесены в "черные списки" поставщиков услуг интернета. К тому же проблема ложного распознавания в отношении индивидуальных пользователей может привести к серьезной ошибке, заключающейся в опоре лишь на традиционные технологии фильтрации для борьбы со спамом. Однако появление случаев ложного распознавания может стать результатом большинства мер борьбы со спамом. Аутентификация уровня домена должна ограничить число случаев ложного распознавания.

Хотя использование "черных списков" вызывает множество проблем, они являются быстрым решением, позволяющим отказать в установлении связи машинам, чье поведение угрожает безопасности и качеству услуг платформы, на которую отправляется почта, или отклонить сообщения от некоторых серверов.

7.8 Адрес сервера-отправителя, рассматриваемый либо в качестве "динамического" либо "стационарного" адреса

Это является особой формой "черных списков", в которой критерием для добавления к списку служит факт соответствия блокируемого IP-адреса машине индивидуального абонента поставщика услуг интернета, а не почтовому серверу какой-либо организации. Идея состоит в том, что обычный абонент направляет свою почту не напрямую в SMTP, а через РТА своего провайдера. Это в большинстве случаев означает, что блокируемая машина направляет спам-сообщения непосредственно от спамера, или чаще, что сообщения направляются без ведома владельца (т. е. система защиты машины взломана, а сама она превращена в "зомби", для того чтобы рассылать сообщения).

Список таких адресов не всегда достоверен, поскольку большинство из них составлены с использованием эвристики, например присутствие "adsl" в имени машины. Управление такими списками также требует значительных ресурсов.

В отличие от этого некоторые из этих списков, в частности те, которые составлены использующим их сервером, могут использоваться, для того чтобы различать серверы, разрешенные для того или иного домена, и списки стационарных адресов. Кроме того, некоторые домены публикуют диапазоны стационарных адресов для своего домена.

Этот тест может рассматриваться как избирательный между "чистыми потребителями" и "провайдерами". Последние считают законной политику, в соответствии с которой владелец домена отказывается соединять свою машину со стационарными адресами, поскольку в настоящее время они являются основным источником спама. Однако потребители утверждают, что спам существует, и свобода пользования электронной почтой должна быть защищена.

7.9 Фильтрация

Фильтрация является наиболее широко известной технологией борьбы со спамом. Основными преимуществами фильтров являются простота установки и гибкость, которая предоставляется пользователям при решении вопроса о том, какие сообщения следует рассматривать в качестве спама. Эвристические фильтры требуют, чтобы пользователь установил критерии, например ключевые слова или адрес отправителя, которые укажут фильтру на необходимость блокирования некоторых сообщений и недопущения их в почтовый ящик потребителя. Спамеры, умышленно делающие ошибки в написании слов или пишущие их на разных языках, без труда обходят технологии, основанные на использовании ключевых слов. Байесовские фильтры основываются на опыте. Они создают статистические данные о сообщениях в таблице для распознавания, которыми будут пользоваться индивидуальные пользователи, с тем чтобы отличать спам от законных сообщений. Поэтому фильтр пропустит только те сообщения, которые похожи на предыдущие законные сообщения пользователя. Как показало исследование, проведенное в 2005 году Федеральной торговой комиссией США [b-FTC], фильтры могут заблокировать 90% спама.

7.9.1 Эвристические фильтры

Работа этих фильтров основана принципе тестирования на присутствие в соответствующем сообщении некоторых типичных признаков спама, таких как исключительное использование HTML или тип потребителя, которому направляется соответствующая почта. Тесту присваивается вес в процессе изучения на основе набора известных спам-сообщений и набора сообщений, о законности которых хорошо известно (поэтому количественная оценка не проводится человеком, для того чтобы уменьшить ее субъективизм).

Опасность использования этих фильтров связана с тем, что сообщения, использующие методы, к которым прибегают спамеры, – например, типичные сообщения в HTML, – будут классифицироваться как спам. Кроме того, следует отметить, что фильтры задействуют значительный объем машинного ресурса.

Эти фильтры могут обнаружить высокую долю посланий, содержащих спам, и они не требуют обучения или настройки. Однако поскольку они используют большое количество тестов, всегда лучше знать, что существует возможность замены тестов и количественной оценки, используемой для отнесения сообщений к категории спама.

7.9.2 Фильтры, работающие по принципу ключевых слов

Это бинарные фильтры, основанные на поиске ключевого слова ("Viagra" и т. д.). Опасность случаев ложного распознавания весьма велика. Возможность обойти эти фильтры путем включения пробелов, чередования букв и неправильного написания слов также существенна.

7.9.3 Фильтры, основанные на сводке или значении хэш-функции

Фильтры, основанные на значении хэш-функции, создают значение хэш-функции представленного им сообщения и указывают, было ли оно уже идентифицировано как спам. Возникает много ошибок нераспознавания, поскольку многие виды электронных посланий, содержащих спам, не поддаются выявлению даже в том случае, если сервер сканирует их с использованием фильтров, основанных на значении хэш-функции. Кроме того, иногда это сообщение изменяется и этого уже достаточно, чтобы создать другое значение хэш-функции. Одно из решений данной проблемы заключается в том, чтобы отложить соответствующее сообщение (как это делается при составлении "серых списков"). Эти фильтры создают мало случаев ложного распознавания.

7.9.4 Байесовские фильтры

Принцип работы байесовского фильтра основан на подготовке процессора фильтра путем изучения набора электронных посланий, содержащих спам, а также набора сообщений, о законности которых хорошо известно, и затем, освоив перечень используемых спамерами команд из этого известного перечня, фильтр использует байесовские вероятности, для того чтобы определить, является ли то или иное сообщение спамом. В случае группового фильтра обучение проводится, как правило, системным администратором.

Поскольку данные фильтры основаны на концепте терминологии, касающейся спама, они могут создавать проблемы в тех случаях, когда они используются на совместной основе. В ограниченной и достаточно однородной среде (например, отдел фирмы или кафедра университета, где каждый работает в одной и той же области и пользуется аналогичной терминологией) это может быть приемлемо. Однако дело будет, несомненно, обстоять иначе в отношении провайдеров электронной почты и, в частности, публичных провайдеров, если база группы не предложит каждому индивидуальному пользователю возможность настройки фильтра на его/ее почтовый ящик. Проблема состоит в том, что та терминология, которая является приемлемой для некоторых пользователей, может приводить в действие фильтр, если группа сочтет, что эта терминология является терминологией спамеров.

Несмотря на потенциальные проблемы, которые могут возникнуть на уровне группы, эти фильтры являются высокоэффективными при использовании их индивидуальными пользователями и являются одним из немногих решений, которые, в случае если они будут использоваться автономно, после надлежащей подготовки могут отфильтровать почти все спам-сообщения.

7.9.5 Фильтры, основанные на поведении

Работа этих фильтров основана на изучении поведения соответствующего удаленного сервера, например количества сообщений, направленных за единицу времени. Одним из примеров фильтрации такого вида является ограничение скорости. Идея состоит в том, что обычные сообщения

направляются только индивидуально или в очень небольшом количестве, тогда как сообщения, содержащие спам, рассылаются очень большими пакетами.

Фильтр подобного типа является очень чувствительным, поскольку обычно невозможно отличить сервер спамера от сервера со списком законной рассылки, например группы новостей.

И все же, по мнению некоторых экспертов, та или иная платформа может на законных основаниях отклонить некоторый объем почты главным образом из-за ее размера или ее миссии по обеспечению безопасности своих сетей. По-видимому, было бы также разумным просить отправителей массовой почты беречь ресурсы удаленной платформы, взяв на себя расходы по распространению своих сообщений и не пытаясь разослать их слишком быстро, для того чтобы самим освободиться от затрат, связанных с использованием электронной почты как канала связи.

7.10 HELO/CSV

В начале каждой транзакции SMTP компьютер, направляющий сообщение, идентифицирует себя по имени перед принимающим компьютером с помощью команды SMTP, "EHLO" или "HELO".

Сертифицированная проверка сервера (CSV) представляет собой услугу, обеспечивающую для сервера, получающего почту, механизм оценки сервера, посылающего почту. Она основывается на существующей практике поставщиков услуг, аттестующих сети, из которых передающие системы устанавливают связь.

Тесты HELO проводятся для проверки того, чтобы удаленный MTA был надлежащим образом сконфигурирован, однако они не указывают на то, спамер это или не спамер. Тесты CSV дополняют тест вероятности относительно имени: действительно ли оно соответствует какому-либо домену? В отличие от SPF или DKIM, CSV аутентифицирует не домен, направляющий сообщение, а домен почтового сервера (который может быть другим, например, в случаях, когда провайдер обслуживает большое число клиентов).

Директивы конфигурации – например, директива Postfix reject_invalid_hostname – тестируют имя, объявленное сервером. Использование обычных тестов HELO приводит к отклонению слишком большого количества законных сообщений. Однако в настоящее время лишь немногие узлы знают, как изменить тест HELO, чтобы он работал надлежащим образом. Вероятно, что в будущем такое положение изменится, поскольку все большее количество узлов будут использовать тест HELO, создавая тем самым стимулы для его совершенствования.

7.11 Составление "серых списков"

Это преднамеренное направление по SMTP кода ошибки 4xx (временная ошибка в противоположность критической ошибке 5xx, см. [b-IETF RFC 2821]) при появлении нового отправителя. Последний, если это обычный MTA, позднее (обычно через 15 минут) вновь попытается направить свое сообщение, и тогда оно будет принято. Большинство спамовых компьютерных программ не рассчитаны на то, чтобы производить несколько попыток для отправления сообщений. Этот метод весьма эффективен и позволяет блокировать все сообщения, содержащие спам, направляемые через открытую ретрансляцию, или MTA провайдера. Он предотвращает получение некоторых сообщений от плохо сконфигурированных серверов и особенно хорошо подходит для использования в сочетании с "белым списком".

7.12 Метки/пароли

Цель этих методов состоит в том, чтобы включить пароль в адрес, на который направляется сообщение, или использовать систему проблема/ответ, такую как определение, кто отвечает. Программное обеспечение спамера не будет знать этот пароль и не сможет пройти тест.

Эти методы не имеют ошибок нераспознавания, если конечно спамеры для выполнения этой работы не решат нанять тысячи человек за очень низкую плату.

Некоторое число законных пользователей откажутся или не смогут пройти этот тест. Поэтому будет много случаев ложного распознавания. Эти методы представляют интерес лишь для пользующихся большой популярностью получателей, которые уже получают массовые почтовые отправления в больших объемах, в том числе законную почту, или для любого получателя, желающего уменьшить количество получаемых сообщений, что соответствует принципу свободы коммуникаций. Следует четко осознавать, что не каждый сервер примет навязываемый ему тест. Обучение пользователей

преимуществам этой технологии и проведение тестирования может помочь сократить количество отказов при приеме.

7.13 Различные методы

В данном пункте описываются различные методы, носящие в основном экспериментальный характер или недостаточно протестированные.

7.13.1 Тестирование оболочки (проверка тега адреса рикошета (BATV) и подписанный адрес отправителя (SES))

Эти методы являются последними разработками и использовались пока еще не достаточно, чтобы их следовало принимать во внимание.

7.13.2 Сертификация массовых почтовых отправок – Оценка репутации отправителя

Хотя аутентификация фактического отправителя поставит перед поставщиками услуг интернета гораздо более ясную задачу в борьбе со спамом, она является лишь предварительным шагом на пути к устранению спама. После того как отправитель может быть идентифицирован, необходимо задействовать такие факторы, как репутация и сертификация, для того чтобы определить, следует ли рассматривать то или иное сообщение как спам до того, как оно будет доставлено пользователю. Управлять процессом сертификации и устанавливать соответствующие критерии будут независимые органы. Надзирать за органами сертификации будет совет по надзору, в который войдут представители от всего сектора.

Для этих целей компанией ePrivacy Group был разработан открытый стандарт для проверенной электронной почты (TEOS). TEOS разработан в рамках программы ePrivacy Group по саморегулированию отрасли, цель которой состоит в том, чтобы отделять законные электронные сообщения от спама. TEOS далеко выходит за рамки аутентификации и создает надежную символику для отправителей электронных сообщений, основанную на подписи в колонтитулах электронных сообщений. В отличие от подписей аутентификации DKIM, подписи TEOS представляют собой видимые печати на сообщениях, подтверждающие, что отправитель соответствует установленным критериям.

Для того чтобы ослабить проблему массовых почтовых отправок, ошибочно отфильтровываемых как спам, отрасль продолжает обсуждать вопрос об эффективности механизма сертификации массовых почтовых отправок. Так, например, законные массовые отправки могут быть идентифицированы на уровне поставщиков услуг интернета с отметкой, которая признается соответствующим сервером, что позволяет с большей уверенностью пользоваться почтовыми фильтрами. В процессе сертификации в качестве входных данных могут использоваться различные критерии, например обязательство строгого следования практике сохранения конфиденциальности. Франция, например, работает со своим агентством по защите данных (CNIL) в направлении введения сертификации для отправителей, извещающих об использовании ими клиентских записей.

Каждый поставщик услуг интернета будет вести "белый список" сертифицированных клиентов. Данное предложение требует заключения соглашения между поставщиками услуг интернета о процедуре сертификации и не предусматривает никакого внешнего вмешательства. Однако чтобы этот метод эффективно работал, потребуются наличие критической массы участия поставщиков услуг интернета, а также доверие между самими поставщиками услуг интернета, поскольку внешний надзор за процессом сертификации не ведется. Кроме того, присвоение какого-либо постоянного числа определению массовости почтовых отправок могло бы оказаться проблематичным. Изворотливые спамеры могут использовать множество бесплатных счетов электронной почты для рассылки спама в больших количествах, при этом каждый счет рассылает спам в количествах чуть ниже предварительно установленного порогового значения для массовых почтовых отправок.

7.13.3 Сервер проверки отправителя?

Для будущих исследований.

7.13.4 Подписи PGP

Для будущих исследований.

7.13.5 Конфигурация системы

Примерами использования конфигурации системы как технологии борьбы со спамом являются внедрение как на уровне отрасли, так и на уровне отдельных пользователей передового опыта обеспечения безопасности портов, брандмауэров, сетей, маршрутизаторов, серверов-посредников, доступа, паролей, защиты ключа доступа и установки программного обеспечения. Отконфигурировав свою систему на блокирование нежелательной почты, можно перехватить лишь тот или иной процент спама. Однако поскольку все больше и больше систем устанавливают подобные механизмы, спамеры, несомненно, также будут проявлять все большую изобретательность, однако при этом у них будет все меньше желания заниматься рассылкой спама, поскольку на их пути появится больше препятствий. В настоящее время люди занимаются рассылкой спама, потому что это просто, быстро и дешево. Поскольку положение изменяется, и над этим уже работают сотни и тысячи системных администраторов, успешно рассылать спам будет все сложнее.

7.13.6 Антивирусные средства

Антивирусные средства являются важными технологиями, позволяющими уменьшить опасность заражения компьютерных систем от спам-сообщений. Вредные спам-сообщения, как правило, содержат в приложении файлы, возбуждающие вирус. Антивирусное программное обеспечение может отсканировать почтовые ящики и предотвратить заражение вирусом.

Некоторые поставщики услуг интернета работают над постоянным мониторингом и обновлением антивирусного интерфейса прикладного программирования (API), VSAPI с сервером станции. Эта технология позволяет обеспечить антивирусное сканирование почтовых ящиков пользователя, с тем чтобы перенести процесс сканирования на сетевую периферию и тем самым уменьшить влияние вирусов и зараженной вирусом почты на сетевую инфраструктуру. Можно также предотвратить выход зараженной почты из организации путем сканирования исходящей почты помимо сканирования входящей почты.

7.14 Как использовать этот анализ технологий и факторы, которые следует принимать во внимание

Полезность любого(ых) инструментального(ых) средства (средств) будет зависеть от потребностей, технических возможностей и инфраструктуры пользователя этого средства. Инструментальные средства предназначены для развертывания на различных участках системы и преследуют различные цели. Пользователи должны будут всесторонне изучить свои потребности и стратегии защиты по мере выбора и использования инструментальных средств борьбы со спамом. Сами инструментальные средства различаются по уровню технической зрелости, эффективности, надежности и использованию. Одни инструментальные средства больше предрасположены к ложному распознаванию, другие более эффективны в определенных областях, а третьи имеют высокие издержки с точки зрения затрат, инфраструктуры, пропускной способности/производительности и требуют специальных технических знаний. Некоторые из этих факторов были перечислены, для того чтобы принимать их во внимание, однако пользователи должны будут сами откалибровать свои инструментальные средства с учетом конкретных условий, в которых им придется работать.

Одни из вышеупомянутых тестов предназначены для борьбы со спамом, в то время как другие имеют целью предотвратить некоторые виды поведения, которые представляют угрозу для безопасности и не учитывают ресурсы платформы, которой направляется почта, или просто не соответствуют принятым правилам отправления электронных сообщений. Если определенный контролирующий инструмент используется после получения данных, представляющих собой сообщение, которое необходимо доставить, то остается решить вопрос о том, что делать с этим сообщением. Очевидно, это будет зависеть от результатов проведенных тестов. Одни тесты более надежны, по сравнению с другими, и поэтому могут оправдывать использование более жестких мер. Кроме того, может быть принято решение провести в отношении некоторых сообщений другие, более дорогостоящие тесты.

Ниже представлены различные варианты действий в отношении того или иного сообщения в зависимости от места расположения внедренного контролирующего инструмента.

7.15 Отказ в сеансе SMTP

Преимущество такого отказа заключается в непринятии на себя управления электронным сообщением, распространение которого остается в сфере ответственности удаленного сервера, который получил информацию о сложившейся ситуации. Кроме того, это позволяет сохранить пропускную способность, во-первых, потому что сообщение не получено и, во-вторых, потому что

удаленный сервер не обязан будет направлять уведомление о статусе доставки (DSN, т. е. сообщение, создаваемое в ответ на отказ, см. [b-IETF RFC 3461]), которое может создать это сообщение. Задача выдачи такого сообщения о недоставке перекладывается на отправителя.

Однако отказ такого вида означает невозможность сохранения копии данного сообщения (и поэтому извлечения законного сообщения, которое, возможно, не было принято, или просто изучения причин отказа).

Кроме того, не все серверы SMTP в настоящее время могут проводить некоторые виды тестирования во время сеанса SMTP. Однако ситуация изменяется по мере все более широкого использования новых продуктов и, в частности, интерфейсов отправки почты, таких как "milter" – сервера политики системы Postfix или будущего OPES, который сможет соединить любую программу с сеансом SMTP.

7.16 Молчаливый отказ

Этот метод часто сбивает с толку обычных пользователей, рассчитывающих на то, что их почта будет доставлена, или, по крайней мере, что им сообщат, что она отклонена. Альтернатива "доставить или сообщить" является основным принципом работы электронной почты, однако от него, по-видимому, придется отказаться, из-за большого количества сообщений электронной почты, которые подразумеваются направленными пользователем, не имеющим к этому никакого отношения.

В идеальном варианте, следовало бы вести реестр, в котором хранилась бы уничтоженная таким образом электронная почта, что позволяло бы использовать такие методы, как отслеживание сообщений, например, путем развертывания [b-IETF RFC 3885] с описанием протокола отслеживания сообщений, что позволяет пользователям узнавать, что произошло с их сообщениями (наподобие систем отслеживания посылок, как это делают обычные компании по доставке посылок).

7.17 Отказ путем направления DSN (уведомление о статусе доставки или "сбой")

Этот метод традиционно используется в электронной почте. Однако из-за присутствия сообщений от того, кто скрывается "под чужой личиной", существует опасность того, что могут пострадать законные отправители, как это можно видеть на примере антивирусных программ, ошибочно направляющих DSN.

7.18 Доставка в почтовый ящик для спама

Если на входе в платформу блокируется слишком мало сообщений, то в почтовом ящике для спама может оказаться очень большое количество сообщений, что может отбить у пользователей всякое желание их читать. Сообщение не уничтожается, однако пользователю предоставляется возможность устранить случаи ложного распознавания.

7.19 Маркировка

Сервер не принимает решения, а лишь ставит отметку на электронном сообщении. Этот метод оставляет пользователю полный контроль, но вместе с тем вынудит его загружать почту, содержащую спам.

Следует отметить, что поставщик услуг интернета мог бы предложить пользователю сделать выбор между простой маркировкой электронной почты и доставкой ее в ящик для спама. Организовать это относительно несложно.

Дополнение I

Деятельность по противодействию спаму, рассылаемому по электронной почте

(Это Дополнение не является неотъемлемой частью настоящей Рекомендации)

I.1 Введение

В настоящем Дополнении содержится описание новых видов деятельности в различных организациях, включая МСЭ-Т, технические спецификации, промышленные объединения и инициативы по вопросам противодействия спаму, рассылаемому по электронной почте. Организации, которые перечислены ниже, представлены для того, чтобы отразить их активную работу в области противодействия спаму, рассылаемому по электронной почте, которая была проведена в период подготовки настоящей Рекомендации. Поэтому диапазон и достоверность технических спецификаций, а также статус перечисленных организаций в будущем могут претерпеть определенные изменения.

I.2 Международная деятельность в области противодействия спаму

I.2.1 МСЭ

В Декларации принципов, принятой в рамках первого этапа Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО), состоявшейся в Женеве в декабре 2003 года [b-WSIS-2003], спам был определен как потенциальная угроза полному использованию интернета и услуг электронной почты. Поэтому участники ВВУИО признали, что спам представляет "для пользователей, сетей и в целом для интернета серьезную проблему, масштабы которой возрастают", и чтобы обеспечить доверие и безопасность при использовании ИКТ, необходимо "принять на национальном и международном уровнях надлежащие меры".

Интерес Государств-Членов к вопросам, касающимся спама, был особо подчеркнут в ходе Всемирной ассамблеи по стандартизации электросвязи (ВАСЭ) МСЭ, которая состоялась во Флорианополисе, Бразилия, в октябре 2004 года. На этой Ассамблее Члены МСЭ утвердили две резолюции, касающиеся деятельности МСЭ в области борьбы со спамом.

Первая резолюция, Резолюция 51 о противодействии спаму, поручает Директорам трех Секторов МСЭ и Генеральному секретарю безотлагательно подготовить Совету 2005 года отчет о соответствующих инициативах МСЭ и других международных инициативах по противодействию распространению спама и предложить, с учетом вкладов Государств-Членов и Членов Секторов, возможные последующие меры для рассмотрения Советом. Резолюция далее предлагает Государствам – Членам Союза принимать надлежащие меры в рамках своих национальных правовых систем для обеспечения принятия соответствующих эффективных мер по борьбе со спамом.

Вторая резолюция, Резолюция 52 о противодействии распространению спама техническими средствами, утверждает, что "спам создает проблемы для безопасности сетей электросвязи, в том числе являясь средством распространения вирусов, "червей" и т. д." В Резолюции признается наличие соответствующих Рекомендаций МСЭ-Т, которые могли бы обеспечить руководящие указания в отношении будущего развития в этой области, и в связи с этим поручается соответствующим исследовательским комиссиям МСЭ-Т в сотрудничестве с Целевой группой по инженерным проблемам интернета (IETF) и другими соответствующими группами в неотложном порядке разработать надлежащие технические Рекомендации по противодействию распространению спама, включая необходимые определения, и регулярно представлять Консультативной группе по стандартизации электросвязи отчеты о своей работе. Эти усилия должны получить всю необходимую помощь со стороны Директора Бюро стандартизации электросвязи, который будет представлять Совету МСЭ отчеты об этой деятельности.

I.2.2 ОЭСР

Спам оказывает негативное влияние на цифровую экономику и приводит к большим социально-экономическим затратам в странах как входящих в ОЭСР, и не входящих в эту организацию. С учетом возможных дальнейших проблем в результате конвергенции в области коммуникационных технологий, возникновения повсеместной связи и мобильного интернета, страны – члены ОЭСР сталкиваются с необходимостью поиска эффективных путей борьбы со

спамом. Для того чтобы решить эту проблему, Комитет по информационной, компьютерной и коммуникационной политике (ИККП) ОЭСР поддержал работу по этой важной теме во время собрания 3–4 марта 2003 года, просил ускорить ее и подчеркнул глобальный характер проблемы. Комитет по политике в области охраны прав потребителей (КПОПП) также выразил заинтересованность в продолжении работы ОЭСР по данной теме. Первые исследования по вопросам, связанным со спамом, нашли отражение в одном базовом документе, а также были предприняты в ходе семинара-практикума по проблемам спама, организованного Европейской комиссией в Брюсселе.

Проблема спама носит многосторонний характер, оказывая влияние на использование сетей, ведет к перегрузкам в сети, влияет на сеть на основе протокола Интернет; спам ставит проблемы, связанные с защитой конфиденциальности информации и безопасности сети, а также с защитой прав потребителей. Для того чтобы более эффективно координировать работу в отношении спама и содействовать скорейшему достижению консенсуса по вопросу об основах политики для решения проблем, создаваемых спамом, Совет ОЭСР принял в июле 2004 года решение о создании горизонтальной "Целевой группы по спаму". Целевой группе было предложено представить отчет КПОПП и ИККП к июлю 2006 года.

Основная задача Целевой группы заключалась в том, чтобы объединить назначенных координаторов по разработке политики в области борьбы со спамом и предусмотреть максимально эффективную разработку срочно требующихся инструментов политики по борьбе со спамом, опираясь при этом на широкий подход и используя специальные знания ОЭСР, накопленные в различных областях.

Целевую группу просили изучить, документально подтвердить и продвигать существующие и разрабатываемые стратегии по борьбе со спамом во всех отраслях. Признавая факт отсутствия простого решения проблемы спама, Целевая группа разработала в апреле 2006 года инструментарий по борьбе со спамом ("Инструментарий"). Этот инструментарий основывается на предпосылке, состоящей в том, что необходимо задействовать целый ряд различных согласованных между собой элементов, с тем чтобы воздействовать на проблему спама и помочь разработать и расширить стратегии и решения по борьбе со спамом в технической, регламентарной и правоприменительной областях, а также содействовать развитию международного сотрудничества. Инструментарий ОЭСР предназначен для того, чтобы объединить ряд согласованных и взаимодополняющих инициатив в области стратегии и других областях (например, правоприменительной области). При разработке и внедрении инструментария значительный упор делался на вкладе заинтересованных сторон в различных рассматриваемых областях. Инструментарий состоит из восьми взаимосвязанных элементов:

- нормативно-правовое регулирование в области борьбы со спамом;
- международное сотрудничество в области обеспечения выполнения законов;
- решения в области борьбы со спамом, реализуемые отраслью;
- существующие и появляющиеся технологии в области борьбы со спамом;
- обучение и ознакомительная деятельность;
- совместное партнерство в борьбе со спамом;
- система показателей в области спама;
- глобальное сотрудничество (пропагандистская деятельность).

По некоторым элементам инструментария для Целевой группы были подготовлены аналитические отчеты. В данном Дополнении обобщается работа, проделанная Целевой группой, и содержатся ее выводы. Настоящее Дополнение добавляет Рекомендация Совета ОЭСР о международном сотрудничестве в области обеспечения выполнения законов о борьбе со спамом, а также веб-сайт ОЭСР, касающийся борьбы со спамом (www.oecd-antispam.org).

1.2.3 АТЭС

В организации Азиатско-Тихоокеанского экономического сотрудничества (АТЭС) вопросы, касающиеся спама, рассматриваются в Рабочей группе по электросвязи и информации (TEL WG). TEL WG поручено заниматься улучшением инфраструктуры электросвязи и информации в регионе, содействовать развитию эффективного сотрудничества, свободной торговли и притоку инвестиций, а также устойчивому развитию.

В области безопасности сетей и инфраструктуры TEL ведет совместную с другими организациями работу по вопросам безопасности и усиливает деятельность по созданию безопасной среды для

работы в реальном времени в информационном обществе, занимаясь такими вопросами, как спам, с тем чтобы противодействовать угрозам сетям, включая последующую деятельность в связи с принципами АТЭС, относящимися к мерам по борьбе со спамом, к осуществлению руководящих принципов АТЭС, касающихся мер по борьбе со спамом, а также активизирует сотрудничество с международными и региональными организациями, такими как МСЭ, ОЭСР и Ассоциация стран Юго-Восточной Азии (АСЕАН). С соответствующей информацией можно ознакомиться на веб-сайте TEL WG АТЭС (<http://www.apectelwg.org/>).

I.3 Разработка технических спецификаций для противодействия спаму

I.3.1 МСЭ-Т

Всемирная ассамблея по стандартизации электросвязи (Флорианополис, 2004 г.) в Резолюции 52 поручила соответствующим исследовательским комиссиям в сотрудничестве с IETF и другими соответствующими группами разработать технические Рекомендации по противодействию распространению спама, включая необходимые определения, и регулярно представлять Консультативной группе по стандартизации электросвязи отчеты о своей работе.

17-я Исследовательская комиссия как ведущая исследовательская комиссия по безопасности электросвязи, поддерживающая деятельность по Резолюциям 50, 51 и 52, весьма подходит для изучения разнообразных потенциальных технических мер по противодействию распространению спама, затрагивающего стабильность и надежность сетей электросвязи. ИК17 МСЭ-Т создала специализированную Группу Докладчика по Вопросу 17/17 для подготовки технических решений по противодействию спаму. В самом начале работа была сосредоточена на разработке технических спецификаций, касающихся противодействия спаму, рассылаемому по электронной почте. Впоследствии работа включила разработку технических решений по противодействию спаму для мультимедийных IP-приложений, таких как IP-телефония, мгновенная передача сообщениями и т. д. В технические спецификации включены или планируется включить руководящие указания, требования, техническую основу и технические средства для противодействия различным видам спама.

I.3.2 IETF

IETF разработала несколько RFC по противодействию спаму, рассылаемому по электронной почте, начиная от руководящих указаний до технических спецификаций, таких как:

- [b-IETF RFC 2505] "Рекомендации по борьбе со спамом для МТА SMTP":

Этот RFC содержит ряд внедренческих рекомендаций для SMTP, МТА (агенты передачи сообщений электронной почты), для того чтобы они могли более эффективно ослаблять воздействие спама. Их смысл заключается в том, что эти рекомендации помогут улучшить ситуацию со спамом, если они будут распространены на достаточно большое число МТА SMTP в интернете, и что они должны использоваться как руководящие указания для различных производителей МТА. Это решение не является окончательным, однако если эти рекомендации будут включены и будут использоваться на всех МТА SMTP интернета, то ситуация значительно улучшится, что позволит выиграть время для разработки более долгосрочного решения. В разделе, посвященном будущей работе, высказываются некоторые соображения, которые могут стать частью долгосрочного решения. Хотя вполне может случиться и так, что конечное решение будет носить социальный, политический или юридический, а не технический характер. Разработчик должен сознавать возрастание рисков, связанных с воздействием вызывающим отказ в обслуживании законных пользователей, к которым может привести внедрение некоторых из предлагаемых методов. Так, например, как рост числа запросов на серверы DNS, так и увеличение размера файла регистрации могут привести к перегрузкам систем и их полному отказу в результате одного из таких воздействий.

- [b-IETF RFC 2635] "НЕ ПРЕНЕБРЕГАЙ – Набор руководящих указаний для массовых случаев незапрашиваемой почты и сообщений (спама*)":

Этот RFC объясняет, почему массовые незапрашиваемые электронные сообщения оказывают вредное влияние на интернет-сообщество. В нем содержится набор руководящих указаний о том, как поступать с незапрашиваемой почтой, предназначенных для пользователей, системных администраторов, новых администраторов, а также кураторов рассылочного списка. В нем также содержатся предложения, которым могли бы следовать поставщики услуг интернета.

- [b-IETF RFC 3685] "Компоненты ситового теста на спам и теста на вирус (система фильтрации электронной почты SIEVE)":
Компоненты ситового "теста на спам" и "теста на вирус" позволяют пользователям использовать простые, портативные командные устройства для тестирования электронных сообщений на наличие в них спама и вируса. Каждый компонент обеспечивает новый тест, использующий совпадения в противовес бальной оценке. Внедрение базовой системы SIEVE должно привести к проведению фактических проверок, результатом которых является образование возвращаемых тестами значений.
- [b-IETF RFC 4686] "Анализ угроз, служащих причиной для идентификации почты с использованием доменных ключей (DKIM)":
Этот RFC содержит анализ некоторых угроз для почты интернета, которые планируется устранять путем аутентификации почты на основе подписи, в частности посредством идентификации почты с использованием доменных ключей. В нем рассматривается характер и место расположения злоумышленников, их возможности, а также цели, которые они намереваются достичь своими атаками.

Помимо этого, разрабатывается ряд проектов с описанием аутентификации на уровне домена, которые можно применять для противодействия спаму, рассылаемому по электронной почте.

I.4 Перечень промышленных альянсов и инициатив в области противодействия спаму

Ниже приводится перечень промышленных инициатив со всего мира. Этот перечень не является исчерпывающим и его следует рассматривать как попытку наглядно проиллюстрировать широкое разнообразие проектов, реализуемых различными организациями, для того чтобы бороться со спамом более скоординированным и эффективным образом.

I.4.1 Рабочая группа по вопросам борьбы с "фишингом"

Рабочая группа по вопросам борьбы с "фишингом" (APWG) [b-APWG] является всемирной, всеотраслевой и правоприменительной ассоциацией, основное внимание которой направлено на ликвидацию мошенничества и хищений персональных данных, являющихся результатом обостряющейся проблемы, связанной с фишингом, фармингом и спуфингом. Организация представляет собой форум, на котором обсуждаются вопросы, касающиеся фишинга, определяются масштабы проблемы с точки зрения фиксированных и не фиксированных затрат, происходит обмен информацией и передовым опытом в целях устранения данной проблемы. Когда это целесообразно, APWG будет стремиться обмениваться информацией с органами правопорядка.

I.4.2 Союз по проблемам аутентификации и доверия при работе в онлайн-режиме

Основанная в октябре 2004 года Email Authentication.org превратилась в Союз по проблемам аутентификации и доверия при работе в онлайн-режиме (AOTA Inc.). Миссия AOTA заключается в содействии укреплению доверия при электронной передаче сообщений всех видов, при электронной торговле, электронных банковских операциях, а также в интернете, что помогает повысить безопасность и улучшить защиту предприятий, равно как и потребителей, работающих в онлайн-режиме. Цели Союза включают содействие распространению передового опыта, обмену информацией, а также введению и использованию процедур аутентификации электронной почты и интернета, введению стандартов и решений, касающихся опознавания и оценки репутации, развитию стратегий защиты доменов, предоставление предписывающих рекомендаций по защите экосистемы и дающих основания для дальнейших действий в нейтральной среде в отношении производителей. В AOTA входят ведущие промышленные, отраслевые и некоммерческие организации, работающие над тем, чтобы укрепить доверие при обмене электронными сообщениями, при работе в интернете и при электронной торговле. В условиях фишинговых атак и фальшивых электронных сообщений такое сотрудничество имеет критически важное значение для оказания помощи в обеспечении безопасности и доставки электронной почты, для укрепления доверия при работе в онлайн-режиме и защиты фирменных знаков и доменов коммерческих предприятий во всем мире.

В начале 2004 года группа представителей бизнеса, отрасли и маркетинга во главе с компаниями Bigfoot Interactive, Email Sender and Provider Coalition (ESPC), Microsoft и Sendmail организовали встречу в целях выработки решений для аутентификации электронных сообщений и укрепления доверия пользователей. После Встречи на высшем уровне по проблемам аутентификации в рамках Федеральной торговой комиссии США в ноябре 2004 года, организованной совместно с национальным институтом стандартов и технологий министерства торговли, было принято решение о

необходимости решительных действий по продвижению работы в области аутентификации электронной почты и создан сайт www.emailauthentication.org. В условиях продолжающегося натиска фишинга и мошеннических электронных сообщений, подрывающих доверие со стороны пользователей и коммерческих предприятий, в сентябре 2006 года emailauthentication.org был зарегистрирован как АОТА (Союз по проблемам аутентификации и доверия при работе в онлайн-режиме).

Хотя АОТА по-прежнему уделяет основное внимание проблемам аутентификации электронных сообщений и остается лидером в этой области с технической точки зрения, он расширил сферу своей деятельности, с тем чтобы оказывать помощь в решении вопросов более широкого характера и преодолении угроз, влияющих на доверие при работе в онлайн-режиме.

1.4.3 Контактная сеть органов по борьбе со спамом (CNSA)

По инициативе Европейской комиссии была создана неофициальная группа, в которую вошли национальные органы власти, занимающиеся применением Статьи 13 директивы о конфиденциальности и электронной связи 2002/58/ЕС, и которая получила название "контактная сеть органов власти, занимающихся проблемами спама (CNSA)".

В рамках CNSA национальные органы власти обмениваются информацией о текущей практике по борьбе со спамом, в том числе передовым опытом, касающимся получения и обработки информации по жалобам, разведывательной информации, а также проведения расследований и противодействия спаму. Комиссия выполняет функции секретариата CNSA. Кроме того, работе CNSA помогает координатор. Координатор содействует обмену информацией между членами CNSA и оказывает поддержку секретариату Комиссии. В настоящее время координатором выступает канцелярия премьер-министра Франции. CNSA проводит регулярные заседания (3-4 раза в год) в Брюсселе. CNSA проводит также ежегодные совместные заседания с участниками Лондонского плана действий.

CNSA разработала процедуру сотрудничества с целью облегчения обмена информацией по жалобам или соответствующей разведывательной информацией между национальными органами власти.

1.4.4 Digital PhishNet

Digital PhishNet (DPN) создана 8 декабря 2004 года как совместная акция, имеющая своей целью объединить лидеров отрасли в области оказания технических, банковских и финансовых услуг и аукционных онлайн-продаж с органами правопорядка для борьбы с "фишингом", представляющим собой пагубную и растущую форму хищения персональных данных в онлайн-режиме.

Фишинг представляет собой развивающуюся, особо опасную и вводящую в заблуждение онлайн-угрозу, основанную на направлении потребителей на фальшивые веб-сайты, обычно с использованием фальшивых или "поддельных" электронных спам-сообщений, для получения личной финансовой информации, например номеров кредитных карт и секретных кодов. В то время как другие отраслевые группы сосредотачивают основное внимание на выявлении фишинговых веб-сайтов и обмене передовым опытом и информацией по конкретным случаям, DPN является первой в своем роде группой, сосредоточившей свою деятельность на оказании содействия в применении уголовного законодательства и помощи в задержании и преследовании лиц, ответственных за совершение преступлений в отношении потребителей посредством фишинга. DPN устанавливает единую линию связи между отраслью и органами правопорядка, с тем чтобы можно было в реальном времени собирать и предоставлять органам правопорядка данные, имеющие важнейшее значение в борьбе с фишингом.

1.4.5 Объединение отправителей и провайдеров электронной почты

Объединение отправителей и провайдеров электронной почты (ESPC) – это коллективная группа лидеров отрасли, работающих над созданием решений в связи с продолжающимся распространением спама и зарождающейся проблемой возможности доставки. Члены ESPC признали необходимость разработки кардинальных решений по спаму, которые обеспечивали бы доставку законных электронных сообщений и были бы весьма эффективными в борьбе со спамом. ESPC работает над решениями по спаму и проблемами доставки путем сочетания правовой защиты, технических разработок и отраслевых стандартов.

ESPC состоит из четырех подкомитетов:

- По законодательству – направляет усилия ESPC по лоббированию разработки федерального законодательства и законодательства штатов.

- По связям с получателями – создан для того, чтобы способствовать лучшему пониманию и ведению диалога между сообществом отправителей и создаваемым сообществом получателей.
- По технологиям – проводит оценку и разрабатывает технические решения, которые позволят более адекватно реагировать на спам (и уменьшить количество случаев ложного распознавания). В рамках этой группы создана техническая рабочая группа для проведения исследований и подготовки таких решений. Группа проводит заседания по мере необходимости, периодически планируя личные встречи.
- По связям с общественностью – готовит для объединения общую стратегию по связям с общественностью.

I.4.6 Институт по проблемам спама и государственной политики в отношении интернета (ISIPP)

Институт по проблемам спама и государственной политики в отношении интернета (ISIPP) ориентирован на проведение анализа, предоставление информации, а также консультирование по отраслевым вопросам, касающимся государственной политики и процессов в отношении спама, электронной почты, возможности доставки электронной почты, а также интернета. ISIPP предоставляет также широко используемые услуги по сертификации отправителей электронных сообщений, SuretyMail, организует отраслевые форумы и выступает в качестве их спонсора, например совещания круглого стола по вопросам управления электронной почтой, совещания на высшем уровне по вопросам доставки электронной почты, а также конференции по вопросам, касающимся спама и права.

I.4.7 Лондонский план действий

Лондонский план действий (LAP) представляет собой глобальную сеть органов правопорядка и представителей отрасли, участвующих в борьбе против спама, фишинга и связанных с ними онлайн-угроз. Инициаторами создания Лондонского плана действий в 2004 году стали Федеральная торговая комиссия США и Управление добросовестной конкуренции Соединенного Королевства. Членами Лондонского плана действий сегодня являются представители свыше 20 стран. С момента своего создания Лондонский план действий содействовал налаживанию двусторонних и многосторонних связей между органами правопорядка, способствуя тем самым международному сотрудничеству в расследовании нескольких дел, связанных со спамом. В 2005 году Лондонский план действий сотрудничал с некоторыми другими правительственными учреждениями при проведении "операции зомби спам", – инициативы, во время которой органы правопорядка во всем мире направили письма поставщикам услуг интернета с настоятельным призывом использовать защитные меры для предотвращения захвата компьютеров потребителей с целью рассылки спама.

Как уже упоминалось выше, Лондонский план действий ежегодно проводит совместные собрания с CNSA. Так, например, совсем недавно, 9–11 октября 2007 года, Лондонский план действий провел третий совместный семинар-практикум с CNSA в Вашингтоне, О.К. Семинар-практикум LAP-CNSA проводился совместно с 11-м общим собранием MAAWG. LAP и CNSA провели несколько совместных заседаний с MAAWG, на которых было рассмотрено большое количество соответствующих тем.

Во время семинара-практикума 2007 года Лондонский план действий провел также занятия по профессиональной подготовке для органов правопорядка, проанализировал полезный эффект от инициатив в области сотрудничества между государственным и частным секторами и рассмотрел пути активизации международного сотрудничества органов правопорядка. В работе совместного семинара-практикума приняли участие представители органов правопорядка и частного сектора более чем из 20 стран.

I.4.8 Рабочая группа против злоупотребления рассылкой сообщений (MAAWG)

Рабочая группа против злоупотребления рассылкой сообщений (MAAWG) является всемирной организацией, занимающейся в основном вопросами предотвращения злоупотреблений при обмене электронными сообщениями в онлайн-режиме, цель которой заключается в том, чтобы укреплять доверие со стороны пользователей, при обеспечении доставки законных сообщений. Имея широкую базу поставщиков услуг интернета (ISP) и сетевых операторов, представляющих свыше 600 миллионов почтовых ящиков, основных поставщиков технологий и отправителей, MAAWG занимается решением проблемы злоупотреблений рассылкой сообщений с упором на инициативы в области технологий, отраслевого сотрудничества и государственной политики.

Цель МААВГ состоит в том, чтобы объединить отрасль обмена сообщениями для совместной работы и успешного решения проблем, связанных со злоупотреблениями, такими как спам, содержащийся в электронных сообщениях, вирусные атаки, атаки типа отказ в обслуживании и другие виды злоупотреблений. Для этого МААВГ разрабатывает инициативы в трех следующих областях, необходимых для того чтобы решить проблему злоупотреблений при рассылке электронных сообщений: сотрудничество, технологии и государственная политика.

I.4.9 Проект Spamhaus

Проект Spamhaus является международной некоммерческой организацией, задача которой состоит в том, чтобы отслеживать спамеров, группы спамеров и услуги, относящиеся к спаму, для обеспечения надежной защиты от спама сетей на основе протокола Интернет в реальном времени, работать совместно с органами правопорядка в целях выявления и преследования спамеров во всем мире, и лоббировать в правительствах принятие эффективных законов по борьбе со спамом. Основанная в 1998 году организация Spamhaus базируется в Женеве, Швейцария, и Лондоне, Соединенное Королевство, и управляется специальной группой, состоящей из 25 следователей, находящихся в девяти странах.

Spamhaus публикует список известных спамовых операций (ROKSO), т. е. базу данных, содержащую информацию и факты по "200" наиболее известным спамерам во всем мире, которая используется поставщиками услуг интернета, для того чтобы не допускать найма на работу известных спамеров, которые будут не надлежащим образом использовать их сети, а также органами правопорядка, для того чтобы обнаруживать профессиональных спамеров и возбуждать в отношении них дела.

Spamhaus публикует несколько баз данных в реальном времени для блокирования спамеров, включая список Spamhaus для блокирования (SBL), список злоумышленников, подлежащих блокированию (XBL) и политический список для блокирования (PBL). Трансляция из сети, включающей 40 серверов DNS в 17 странах, и списки для блокирования Spamhaus используются многими сетями крупных поставщиков услуг интернета, сетями корпораций, университетов, правительственных учреждений, а также военными сетями связи.

Финансирование операций осуществляется за счет спонсорских взносов и пожертвований. Средства для финансирования международной инфраструктуры поступают за счет предоставления услуг достоверной вычислительной базы списков для блокирования ("передача данных Spamhaus"), оказываемых самостоятельной организацией материально-технического обеспечения крупным сетям на основе протокола Интернет, а также коммерческим компаниям, занимающимся фильтрацией спама.

I.4.10 Объединение "остановить спам"

Объединение "остановить спам" является совместной инициативой для сбора информации и ресурсов по борьбе со спамом. Эта инициатива была предпринята АТЭС, CNSA ЕС, МСЭ, Лондонским планом действий, ОЭСР и группой по борьбе со спамом Сеул–Мельбурн.

В соответствии с Тунисской программой ВВУИО [b-WSIS-2005], в которой содержится просьба к членам "принять эффективные меры для решения существенной и все возрастающей проблемы, связанной со спамом" и призыв ко всем заинтересованным сторонам принять многосторонний подход к противодействию спаму, объединение "остановить спам" осуществляет связь с инициативами в области законодательства по борьбе со спамом и правоприменительной деятельности, обучения потребителей и бизнесменов, передового опыта и международного сотрудничества.

"Общая программа мероприятий", показ международных мероприятий, касающихся спама и связанных с ним угроз, организуемых соответствующими организациями, также доступны на веб-сайте <http://stopspamalliance.org/>.

I.4.11 Форум по надежным средствам электронной связи (ТЕСФ)

Форум по надежным средствам электронной связи (ТЕСФ) является ассоциацией представителей всех отраслей и географических регионов, занимающейся вопросами стандартизации технологий, методов и передового опыта в борьбе против фишинга, спуфинга и хищения личных данных. Основной упор в деятельности ТЕСФ делается на эффективное и действенное создание, внедрение и поддержку решений проблем, предоставляемых научными исследованиями, аналитиками и его членами. Создаются рабочие группы и комитеты для разработки и/или проверки методов и инструментария, специально предназначенных для устранения опасных угроз, обозначенных ТЕСФ.

Библиография

- [b-WSIS-2003] Первый этап ВВУИО (2003 г.), *Декларация принципов*.
<http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160>
- [b-WSIS-2005] Второй этап ВВУИО (2005 г.), *Туниская программа для информационного общества*.
<http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2266|2267>
- [b-APWG] Anti-Phishing Working Group, <<http://www.antiphishing.org/>>.
- [b-IETF RFC 2505] IETF RFC 2505 (1999), *Anti-Spam Recommendations for SMTP MTAs*.
<<http://www.ietf.org/rfc/rfc2505.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 2822] IETF RFC 2822 (2001), *Internet Message Format*.
<<http://www.ietf.org/rfc/rfc2822.txt>>
- [b-IETF RFC 3461] IETF RFC 3461 (2003), *Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)*.
<<http://www.ietf.org/rfc/rfc3461.txt>>
- [b-IETF RFC 3685] IETF RFC 3685 (2004), *SIEVE Email Filtering: Spamtest and VirusTest Extensions*.
<<http://www.ietf.org/rfc/rfc3685.txt>>
- [b-IETF RFC 3885] IETF RFC 3885 (2004), *SMTP Service Extension for Message Tracking*.
<<http://www.ietf.org/rfc/rfc3885.txt>>
- [b-IETF RFC 4686] IETF RFC 4686 (2006), *Analysis of Threats Motivating DomainKeys Identified Mail (DKIM)*.
<<http://www.ietf.org/rfc/rfc4686.txt>>
- [b-FTC] United States Federal Trade Commission, *Email Address Harvesting and the Effectiveness of Anti-Spam Filters*, November, 2005.
<<http://www.ftc.gov/opa/2005/11/spamharvest.pdf>>
- [b-Lyris] Lyris Technologies, Inc., *Email Advisor: ISP Email Deliverability Report Card*, 2nd quarter, 2007.
<http://www.lyris.com/resources/reports/deliverability_report_Q22007.pdf>
- [b-OECD TF] OECD Task Force on Spam (2006), *Report of the OECD Task Force on Spam: Anti-Spam Toolkit of Recommended Policies and Measures*.
<<http://www.oecd.org/dataoecd/63/28/36494147.pdf>>

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия А	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных, взаимосвязь открытых систем и безопасность
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи