Санкт-Петербург, ул. Седова, 80, телефон (812) 449-0770, факс (812) 449-0771, E-mail: info@bilim.com

Network Working Group
Request for Comments: 2505
BCP: 30
Category: Best Current Practice

G. Lindberg
Chalmers University of Technology
February 1999

Рекомендации по предотвращению спама для SMTP MTA

Anti-Spam Recommendations for SMTP MTAs

Статус документа

Этот документ относится к категории "Обмен опытом" (Internet Best Current Practic) для сообщества Internet и служит приглашением к дискуссии в целях совершенствования. Документ может распространяться свободно.

Авторские права

Тезисы

В этом документе приводятся рекомендации по реализации SMTP [1] MTA (агентов доставки почты - Mail Transfer Agent, - например, sendmail, [8]), позволяющие затруднить использование почтовых агентов для рассылки спама (spam[1]).

Документ рассчитан на оказание помощи в понимании ситуации со спамом и применим к большинству SMTP MTA в сети Internet, а также может использоваться в качестве руководства при разработке программ MTA. Мы полностью осознаем, что документ не дает решения для всех случаев борьбы со спамом, но использование приведенных здесь рекомендаций на всех SMTP MTA в сети Internet, позволит получить дополнительный опыт и разработать более эффективное решение. Параграф **Продолжение работы** включает некоторые идеи по развитию данного направление. Решение проблемы спама возможно, хотя эта проблема по своей природе в значительной степени является социальной, политической и правовой, нежели технической.

Разработчикам программ следует принимать во внимание, что некоторые из рассмотренных здесь методов могут быть применены для организации атак на службы (denial of service). Например, увеличение числа очередей серверов DNS и размера журнальных файлов может приводить к перегрузке системы и ее краху в результате атаки на службы.

Основные идеи документа:

- Открытая трансляция почты должна быть прекращена.
- Когда спамеры играют в открытую, с ними следует вести переговоры.
- Должна быть разработана почтовая система, которая может работать со спамом.

1. Введение

Этот документ относится к числу BCP (Best Current Practice - обмен накопленным опытом) RFC. Рекомендуется использовать этот документ в качестве руководства при разработке новых программ SMTP MTA для более эффективного предотвращения/обработки спама. Кроме того, документ будет полезен системным и почтовым администраторам, которые хотят реализовать средства предотвращения спама в своих SMTP MTA.

Однако данный документ не содержит общего описания SMTP MTA и не рассматривает опций настройки почтовых агентов. Все содержащиеся в документе рекомендации по настройке указаны явно.

1.1. Предпосылки

Объем нежелательной для получателя электронной почты, часто именуемой спамом (spam), существенно возрос за последнее время и составляет сейчас существенную долю всей электронной почты в сети Internet[2]. Такой рост уровня спама потребовал незамедлительного принятия мер противодействия.

Проблема спама включает несколько аспектов:

- Значительное число нежелательных сообщений, получаемых пользователями электронной почты.
- Спам совершенно тупой - т. е., никак не связан с областью интересов получателя (если не исходить из предположения, что всех пользователей Internet интересуют порнографические картинки, программы для рассылки спама и т. п.).
- Спам стоит его получателю реальных денег, поскольку многие пользователи оплачивают время, затрачиваемое на копирование сообщений из своего почтового ящика у ISP[3] на свой компьютер (например, при подключении по телефонной линии).
- Спам повышает уровень расходов ISP. Предположим, что сообщение размером 10 кбайт отправлено 10 000 адресатов, почтовые ящики которых поддерживаются одним ISP. Суммарный трафик в результате такой рассылки составит 100 Мбайт. Диск размером 4 Гбайт способен принять 40 таких рассылок, после чего на нем уже не останется свободного места. Такие

[1] Spam® - зарегистрированный торговый знак компании Hormel, используемый для мясных консервов. Применение термина spam сообществом Internet берет свое начало от скетча Монти Пайсона (Monty Python), который относится фактически к фольклору Internet. Термин спам обычно трактуется как уничижительный, но этот оттенок не имеет отношения к продукции Hormel.
[2] По оценкам многих аналитиков в 2003 году доля спама превысила 50% суммарного объема электронной почты. *Прим. перев.*
[3] Internet Service Provider – провайдер Internet. *Прим. перев.*

выбросы почтового трафика практически невозможно предусмотреть, поэтому они могут приводить почтовую систему провайдера в состояние полной неработоспособности.

- Многие отправители спама прячутся за подставными адресами отправителя в заголовках почтовых сообщений чтобы спам казался получателю реальным почтовым диалогом или доставленной по ошибке почтой. В полях темы сообщения часто используются фразы типа "material you requested[4]", хотя содержимое такой почты не имеет никакого отношения к интересам и потребностям ее получателей. Тема, указываемая в заголовке таких сообщений зачастую просто служит приманкой для получателя, стимулирующей его к просмотру принятого сообщения.
  Фактически, некоторые программы рассылки спама “почитают за честь” добавлять заголовки, которые заставят ISP “поломать голову".
  Получатели спама, отправляющие в ответ гневные письма протеста или отказывающиеся от получения рассылок в соответствии с включенными в письмо инструкциями, зачастую попадают в дополнительные списки рассылки спама, которые спамеры продают.
- Обычной практикой при рассылке спама является использование сторонних хостов в качестве трансляторов почты (relay), направляющих сообщения адресатам. Такое нелегальное использование почтовых служб является нарушением законодательства большинства – если не всех[5] - стран (по крайней мере, в США спамеров достаточно часто преследуют по закону). Однако, если исходный отправитель находится в США, использованный для рассылки спама почтовый транслятор – в Швеции, а получатели спама в США[6], юридические проблемы существенно осложняются[7].

1.2. Рамки документа

В данном документе не содержится окончательного решения проблемы спама.

Однако при реализации предложенных здесь методов и правил (особенно правил Non-Relay) на достаточном числе MTA в сети Internet деятельность спамеров значительно усложнится. Если правовых методов предотвращения спама окажется недостаточно, спам можно блокировать техническими мерами с использованием описанных ниже правил (поскольку правила Non-Relay сейчас можно использовать открыто, можно создать различные фильтры против спама). Очевидно, что наилучшие результаты могут быть достигнуты при использовании правовых и технических мер предотвращения спама.

Такой подход существенно снизит остроту проблемы спама и позволит сообществу Internet разработать и реализовать эффективное и долговременное решение этой проблемы.

Однако следует понимать, что одних правил Non-Relay недостаточно для предотвращения спама. Даже если настанет день, когда 99% SMTP MTA будут использовать такие правила, спамеры продолжат использовать оставшийся 1%. В крайнем случае, они смогут напрямую соединяться с хостом каждого адресата – это приведет к лишь к некоторому повышению затрат на рассылку спама.

Реализация IPv6 представляется достаточно скорым событием, но бороться со спамом приходится уже сейчас, поэтому в данном документе рассматривается только IPv4.

1.3. Терминология

В данном документе использование глаголов долженствования соответствует RFC2119 [4]:

- **Должно** (MUST)
  Это слово используется для обозначения обязательных к исполнению требований.
- **Следует** (SHOULD)
  Этот термин означает рекомендацию и используется в тех случаях, когда те или иные обстоятельства позволяют отказаться от выполнения указанных требований. Все случаи отказа от выполнения таких требований должны быть основаны на взвешенном решении.
- **Возможно (**MAY)
  Это слово используется для обозначения необязательных требований. Одни производители могут использовать такие опции, а другие – отказываться от их реализации по собственному усмотрению.

1.4. Использование данных DNS

В документе используются термины “имя хоста” (host name) и “доменное имя” (domain name) которые следует трактовать как полные доменные имена хостов – FQDN[8], т. е., имена, возвращаемые DNS в ответ на запрос PTR (.IN-ADDR.ARPA) для преобразования IP-адреса в доменное имя, или имена, указываемые в записях MX для домена (RFC1034 [5], RFC1035 [6]).

Использование FQDN вместо адресов IP в этом документе обусловлено исключительно удобством восприятия. Однако такое использование жестко связано в DNS и записями .IN-ADDR.ARPA (PTR). Поскольку эти сведения легко подменить путем подстановки записей в кэш серверов DNS или использования спамерами собственных серверов имен, работать с доменными именами следует осторожно, проверяя соответствие прямого и обратного преобразования. Использование Secure DNS (RFC2065, [7]) упрощает ситуацию, делая невозможной подставку .IN-ADDR.ARPA.

Одна из рекомендаций связана с проверкой поля "MAIL From:" (envelope originator) с помощью DNS (исходя из предположения о существовании данных DNS для домена отправителя). При использовании такой проверки следует принимать во внимание ряд обстоятельств:

1) Такая проверка может привести к значительному росту числа DNS-запросов и связанному с этим увеличению нагрузки на серверы DNS. Кроме того, использование такой проверки дает злоумышленникам возможность организации DoS-атаки на сервер DNS путем простой генерации многочисленных сообщений.

2) Следует отметить, что при негативном кэшировании в DNS можно использовать подставные отклики DNS для организации атак на службы (denial of service – DoS). Например, если известно, что сайт использует проверку FQDN для SMTP-команд "MAIL From:", атакующий может использовать негативные отклики DNS для эффективной блокировки приема почты из одного или многих источников. Учет этого обстоятельства требует осторожности при выборе сервера DNS, используемого для проверки адреса отправителя, с целью минимизации риска получения подставных откликов.

[4] Запрошенные Вами материалы. *Прим. перев.*
[5] Увы, далеко не всех. *Прим. перев.*
[6] Или любой другой стране. *Прим. перев.*
[7] В настоящее время во многих странах предпринимаются серьезные попытки законодательного подавления спама и создания интернациональных служб для решения связанных со спамом юридических и иных проблем. *Прим. перев.*
[8] Fully Qualified Domain Name – полное доменное имя.

3) Для ранних версий программ рассылки спама проверки FQDN может оказаться вполне достаточно, поскольку такие программы используют совершенно произвольные значения в командах "MAIL From:" и сообщения от таких программ практически полностью блокируются, благодаря проверке с использованием DNS. Такая проверка может использоваться и сегодня, но уровень эффективности существенно понизился за счет использования программами рассылки реальных или правдоподобных имен в командах "MAIL From:".

С другой стороны, сайты, не имеющие достаточно хорошего соединения с DNS, могут сталкиваться с проблемами при получении легитимной почты из-за тайм-аутов при обращении к серверу DNS во время проверки поля "MAIL From:". Однако данные DNS обслуживаются в асинхронном режиме и могут кэшироваться, поэтому достаточно высока вероятность получения запрошенной информации даже при возникновении тайм-аута.

В более современных версиях программ рассылки спама проверка "MAIL From:" может не дать столь очевидного результата, поскольку программы спамеров также совершенствуются и зачастую используют реальные адреса (легитимность такого использования выходит за пределы рассмотрения данного документа).

1.5. Где блокировать спам – в SMTP, в RFC822 или в UA

Нашим основным предположением является то, что решение о приеме или отбрасывании сообщения должно приниматься на уровне SMTP и агент MTA должен принимать решение об отказе в процессе диалога SMTP. Такой подход позволяет избавиться от приема ненужных сообщений. Кроме того, при таком подходе ответственность за принятие окончательного решения передается отправителю сообщения – он получает соответствующий код возврата от SMTP и может обрабатывать его с учетом своих задач.

1.6. Коды возврата SMTP

Протокол SMTP поддерживает несколько классов кодов возврата (Return Code), описанных в работе [1]:

- **5xx**
  Постоянный отказ (Permanent Negative Completion) – критическая ошибка (Fatal Error) – почтовая транзакция прерывается и сообщение возвращается отправителю.
- **4xx**
  Временный отказ (Transient Negative Completion) – временная ошибка (Temporary Error) – почтовая транзакция возвращается в очередь для повторения попытки по истечении некоторого времени.
- **2xx**
  Позитивный результат (Positive Completion) – показывает, что агент MTA принял на себя ответственность за дальнейшую доставку сообщения.

При использовании описанных в этом документе опций и методов следует принимать во внимание ряд аспектов:

Для некоторых событий типа "Denied - you're on the spammer's list[9]" возврат кода 5xx может быть корректным действием, поскольку при этом почтовая сессия прерывается (если спамер не играет по правилам SMTP, он может поместить сообщение обратно в очередь на отправку или перебросить на другой хост в зависимости от возвращенного кода). Однако возврат кода 5xx в результате конфигурационной ошибки может приводить к отказу в приеме легитимной почты.

Следовательно, мы предлагаем в большинстве случаев возвращать коды 4xx. Поскольку такой код говорит о исправимой ошибке, почта заново помещается в очередь на стороне отправителя и мы получаем некоторое время на обнаружение и исправление конфигурационных ошибок и не отказываемся категорически от приема сообщения (например, отказ в трансляции почты для домена, в котором MX-запись указывает на данный транслятор).

Возврат кода 4xx спамеру также приводит к сохранению сообщения в почтовой очереди и, если спамер использует свой хост, может заставить этого спамера образумиться – ведь размеры диска не бесконечны. С другой стороны, если спамер пользуется открытым транслятором, переполнение очереди может послужить владельцам хоста сигналом о непорядке в их системе.

Однако при возврате кодов 4xx может возникать нетривиальный случай взаимодействия с записями MX. Если домен адресата имеет несколько MX-записей и хост с наиболее предпочтительным[10] значением MX возвращает код 451, передающий сообщение хост может (и часто делает это реально) попытаться использовать хост со следующим значением MX.

Если второй хост не использует в точности такой же список для отказа в приеме почты, он может принять сообщение и далее будет пересылать его транслятору с минимальным значением MX, который ранее отказался принимать сообщение на основе анализа "MAIL From:". В результате будет заполняться почтовая очередь на дружественном хосте, обеспечивающем адресату дополнительную запись MXt.

Наконец, можно возвратить код 2xx, не предпринимая усилий по дальнейшей доставке спама (например, отправив сообщение в /dev/null). Очевидно, что это является нарушением RFC821 и таким способом не следует пользоваться без аккуратного рассмотрения всех аспектов. Вместо отбрасывания почты вслепую можно заново помещать ее в очередь и вручную (или автоматически) проверять является она спамом или легитимной почтой, после чего отбрасывать или пересылать дальше.

1.7. Списки рассылок

Агент MTA может также поддерживать списки рассылок (mailing list) и отправлять по этим спискам сообщения множеству адресатов. Требуется обеспечить проверку отправителя и предотвращение возможности рассылки спама по таким спискам. Механизмы в данном случае могут существенно отличаться от тех, которые применяются для отдельных сообщений и отдельных пользователей. Рассмотрение этих механизмов выходит за пределы данного документа.

2. Рекомендации

Сначала мы приведем краткий список рекомендаций, а потом более детально рассмотрим каждую из них. Будут также даны рекомендации по тому, что **не** следует делать – что-то может казаться совершенно естественным с точки зрения борьбы со спамом (и может даже помочь в ней), но может приводить к вредным последствиям для почтовой системы и отрицательный эффект может оказаться больше положительного.

1) **Должна** обеспечиваться возможность ограничения несанкционированного использования почтовых трансляторов.

[9] Почта отвергнута – вы в списке спамеров.
[10] Минимальным из имеющихся. *Прим. перев.*

2) **Должна** обеспечиваться возможность обеспечения строк "Received:" с достаточно информацией для трассировки пути доставки почты независимо от использования спамерами обманных имен хостов в командах HELO и т. п.

3) **Должна** обеспечиваться возможность доступа к локальным системным журналам для последующей трассировки событий.

4) **Следует** обеспечивать возможность записи в системные журналы информации о всех действиях anti-relay/anti-spam.

5) **Следует** обеспечивать возможность отказа от приема почты для хоста или группы хостов.

6a) **Недопустимо** отвергать "MAIL From: <>".

6b) **Недопустимо** отвергать "MAIL From: <user@my.local.dom.ain>".

7a) **Следует** обеспечивать возможность отвергать почту от конкретного пользователя "MAIL From:" user, <foo@domain.example>.

7b) **Следует** обеспечивать возможность отвергать почту из домена в целом "MAIL From:" domain <.*@domain.example>.

8) **Следует** обеспечивать возможность отвергать почту для ограничения скорости приема почты ("Контроль скорости").

9) **Следует** обеспечивать возможность проверки домена "MAIL From:" domain (с использованием DNS или иных способов).

10) **Следует** обеспечивать возможность проверки <local-part> для исходящей почты.

11) **Следует** обеспечивать возможность контроля для команд SMTP VRFY и EXPN.

12) **Следует** обеспечивать возможность контроля для команды SMTP ETRN.

13) **Должна** обеспечиваться возможность настройки параметров для возврата разных значений Return Code по различным правилам (например, 451 Temp Fail, а не 550 Fatal Error).

Приведенное ниже обсуждение рекомендаций зачастую заканчивается необходимостью проверки соответствия для имен хостов/доменов и адресов/подсетей IP. **Рекомендуется** обеспечивать возможность представления данных/шаблонов для проверки соответствия извне по отношению к MTA (например, правила проверки соответствия включаются в MTA, но данные, с которыми проводится сравнение могут храниться в отдельном файле). **Рекомендуется** также обеспечивать возможность включения в данные для проверки соответствия (внешний файл) регулярных выражений для обеспечения максимальной гибкости.

Естественно, что при проверке соответствия имен доменов и/или хостов **недопустимо** принимать во внимание регистр символов. Поскольку локальная часть адреса (<local-part>) может быть регистрозависимой, для ее проверки разумно учитывать регистр символов. Однако, поскольку <sPAmMeR@domain.example> и <spammer@domain.example> скорей всего указывают на одного пользователя и поскольку в результате сравнения принимается решение об отбрасывании сообщения мы предлагаем при сравнении <local-part> также не учитывать регистр символов.

Интерпретация применения всех этих рекомендаций является достаточно гибкой – в зависимости от того, как вы реализуете фильтрацию спама сегодня, спамеры будут завтра искать обходные пути и качественные реализации MTA должны обеспечивать достаточную гибкость для предотвращения новых уловок и хитростей спамеров.

2.1. Ограничения на использование почтовых трансляторов

Несанкционированное использование хоста в качестве почтового транслятора (Mail Relay) означает кражу ресурсов транслятора и подвергает риску репутацию владельцев такого транслятора. Может также оказаться невозможным отфильтровать или заблокировать спам без одновременного блокирования легитимной почты.

Следовательно, агент MTA **должен** обеспечивать контроль за использованием транслятора и возможность отказа в доступе к нему.

В сессии SMTP мы имеем 4 элемента с разным уровнем доверия к каждому из них:

1) "HELO Hostname" легко и часто подменяется.

2) "MAIL From:" легко и часто подменяется.

3) "RCPT To:" корректное или, по крайней мере, намеренно заданное значение.

4) SMTP_Caller (хост) IP-адрес отправителя (нормально), FQDN (может быть нормально).

Поскольку 1) и 2) легко подменить и это часто происходит, мы не может полагаться на эти параметры для проверки полномочий (авторизации) при использовании нашего хоста в качестве почтового транслятора.

Агент MTA **должен** быть способен контролировать доступ к функциям почтового транслятора на основе комбинации:

- "RCPT To:" адрес (домен).
- SMTP_Caller FQDN-имя хоста.
- SMTP_Caller IP-адрес.

Предлагается следующий алгоритм проверки:

a) Если "RCPT To:" содержит один из “наших” доменов, локальное доменное имя или имя домена, для которого мы обеспечиваем пересылку почты (дополнительный MX), доступ к транслятору разрешается (Relay).

b) Если SMTP_Caller проверен по IP-адресу отправителя или FQDN (зависит от уровня доверия к DNS), доступ к транслятору разрешается (Relay).

c) Доступ к транслятору не разрешается.

При выполнении п. a) нужно быть уверенным, что все типы SMTP source routing[11] (официальные [@a,@b:u@c], с помощью '%' и пути uucp '!') полностью удалены до выполнения проверки или, по крайней мере, принимаются во внимание при проверке.

[11]Заданная отправителем маршрутизация.

Сайт, реализующий такую проверку, должен осознавать, что он может блокировать корректно адресованные сообщения, особенно в тех случаях, когда они исходят от систем, работающих по отличному от SMTP протоколу, или направлены в такие системы. До реализации такого правила следует аккуратно убедиться в том, что приняты во внимание все используемые алгоритмы маршрутизации почты, другие почтовые системы и иные специальные случаи. Каждая из таких систем может потребовать выполнения специальных мер.

Примером подобной почтовой системы может служить X.400 с ее адресами типа:

```
"/c=us/admd= /prmd=xyz/dd.rfc-822=user(a)final/"@x400-gateway
```

Другим примером является DECnet MAIL-11, которая использует адреса в форме:

```
"gateway::smtp%\"user@final\""@mail-11-gateway
```

Во всех случаях конфигурация **должна** поддерживать шаблоны для FQDN и классы адресов IP, **следует** также поддерживать форму "адрес/маска" для бесклассовых адресов IP. Примерами могут служить domain.example и *.domain.example; 10.11.*.*, 192.168.1.*, 192.168.2.*, 10.0.0.0/13, 192.168.1.0/23.

Конфигурации **следует** позволять получение шаблонов и данных для принятия решений из внешних источников (например, из текстового файла или базы данных). **Следует** поддерживать возможность включения в эти данные регулярных выражений.

2.2. Строки Received:

Агент MTA **должен** добавлять информацию о себе в начало (prepend) строки "Received:" почтового заголовка (как описано в RFC822 [2] и требуется в RFC1123 [3]). Добавляемый в строку "Received:" текст **должен** содержать информацию, достаточную для обеспечения возможности трассировки пути доставки почты в направлении ее отправителя. Здесь возможны два случая, описанных ниже.

2.2.1. Прямые соединения между MTA

Почтовая система Internet разрабатывалась с учетом того, что хост-отправитель соединяется непосредственно с получателем, указанным в записи MX (при наличии множества MX они упорядочиваются по уровню приоритета). Для обеспечения возможности трассировки в направлении хоста-отправителя (который может быть МСЭ[12] или шлюзом, как описано ниже) каждый агент MTA на пути доставки, включая конечный MTA, **должен** помещать информацию о себе в начало (prepend) строки "Received:". Добавляемая строка "Received:" должна включать:

- IP-адрес передающего хоста;
- Дату и время в соответствии с RFC822 [2] (стр. 18).

Следует также включать в это строку:

- Имя FQDN, соответствующее IP-адресу передающего хоста;
- Аргумент, переданный в команде HELO;
- Аутентификационные данные, если для передачи или подачи почты используется аутентификация.

Предполагается, что большинство остальных полей "Received:", описанных в RFC822, будет включено в строки "Received:".

В большинстве случаев любую информацию, которая может помочь в трассировке пути сообщения, можно и следует добавлять в строку "Received:". Это верно даже в тех случаях, когда исходное сообщение подается не через SMTP. Например, подача сообщения через web-интерфейс осуществляется с использованием между клиентом и сервером протокола HTTP; строка "Received:" в таких случаях может быть использована для идентификации IP-адреса, использованного при соединении с сервером HTTP, на котором было создано почтовое сообщение.

Эти рекомендации обдуманно жестче, нежели RFC1123 [3], и это сделано для того, чтобы можно было отслеживать почту, переданную спамером непосредственно со своего хоста. Типичным случаем является использование спамерами коммутируемых соединений – в такой ситуации ISP нужно знать адрес IP, дату и время отправки, чтобы принять меры по отношению к спамеру.

2.2.2. МСЭ и шлюзы

Организациям, применяющим политику сокрытия структуры своей внутренней сети, должна обеспечиваться возможность сохранения такой политики. Такие организации обычно используют внутренние агенты MTA, которые включают в строки "Received:" минимум информации или не добавляют таких строк совсем. После этого почта передается наружу через тот или иной МСЭ или шлюз, который может даже удалить все добавленные внутренними агентами MTA строки "Received:" прежде, чем включить в заголовок свою строку "Received:" (в соответствии с требованиями RFC1123 [3]).

Поступая таким образом, организация полностью принимает ответственность за трассировку и обнаружение спамеров, рассылающих почту из сети этой организации, или просто берет на себя ответственность за действия этих спамеров. В заголовках исходящей из организации почты **требуется** обеспечить информацию, которой будет достаточно для них, чтобы выполнить любую необходимую трассировку.

Для входящей в организацию почты строки "Received:" **должны** сохраняться неизменными, чтобы обеспечить получившему почту внутреннему пользователю возможность трассировки отправителя информации.

В общем случае шлюзам **не следует** менять строк "Received:", если этого не требует политика безопасности. Изменение содержимого существующих строк "Received:" зачастую приводит к повреждению и удалению информации, требуемой для трассировки сообщений. Следует принимать меры по сохранению информации из строк "Received:" в самом сообщении, которое получит адресат, или, если это возможно, в системных журналах.

2.3. Журналы событий

Агент MTA **должен** записывать в локальный системный журнал достаточное для трассировки событий количество информации. Сюда входит большая часть информации, помещаемой в строки "Received:".

[12]Межсетевой экран. *Прим. перев.*

2.4. Протоколирование anti-relay/anti-spam

Агенту MTA **следует** записывать в системный журнал операции anti-relay/anti-spam. В записи журнального файла следует включать как минимум:

- дату и время события;
- информацию о причинах отказа ("Mail From", "Relaying Denied", "Spam User", "Spam Host" и т. п.);
- адреса (домены) "RCPT To:" (если соединение было запрещено на раннем этапе, например, при проверке адреса SMTP_Caller, адрес "RCPT To:" не будет известен и не может быть сохранен в журнале);
- IP-адрес подключающегося хоста;
- имя FQDN подключающегося хоста;
- другие относящиеся к делу сведения (например, информацию, переданную в диалоге SMTP, до того, как запрос был отвергнут).

Следует отметить, что протоколирование лишних событий (особенно отказов в приеме почты) открывает возможность для DoS-атаки (например, путем заполнения журнальных файлов огромным количеством записей о командах "RCPT To:"). Реализации, поддерживающие описанное здесь протоколирование, должны принимать во внимание увеличение размера журнальных файлов (особенно во время атак).

2.5. Отказ на основе адреса SMTP_Caller

Агенту MTA **следует** обеспечивать возможность восприятия или отказа в приеме почты от конкретного хоста или группы хостов. Здесь имеется в виду адрес IP.src или имя FQDN, которое преобразуется в адрес .IN-ADDR.ARPA (в зависимости от того, доверяете ли вы серверу DNS). Функционально это может быть реализовано в МСЭ, но поскольку MTA следует уметь защитить себя, мы рекомендуем реализовать такую функцию.

Рекомендуется обеспечивать агенту MTA возможность принятия решения на основе имен FQDN (host.domain.example), шаблонов имен (*.domain.example), отдельных адресов IP (10.11.12.13) или префиксов IP (10.0.0.0/8, 192.168.1.0/24).

Рекомендуется также обеспечивать возможность объединения правил принятия решений для формирования гибких списков accept/refuse/accept/refuse, как показано ниже:

```
accept   host.domain.example
refuse   *.domain.example
accept   10.11.12.13
accept   192.168.1.0/24
refuse   10.0.0.0/8
```

Список просматривается от начала до первого соответствия, которое определяет действие accept/refuse (принять или отвергнуть).

Рекомендуется поддерживать префиксы в формате IP-address/length. Однако реализации поддержки шаблонов адресов (например, 10.11.12.*) также может оказаться вполне достаточно.

Для дополнительного повышения эффективности фильтрации MTA **может** поддерживать использование регулярных выражения для имен хостов, а возможно и для адресов IP.

2.6. "MAIL From: <>" и "MAIL From: <user@my.local.dom.ain>"

Хотя борьба со спамерами имеет достаточно важную роль, она никогда не должна нарушать существующие стандарты работы с электронной почтой. Поскольку спамеры часто используют обманные адреса "MAIL From:", возникает соблазн начисто запретить прием почты с таких адресов (особенно с тех, которые используются наиболее часто). Такой подход, однако, принесет больше вреда, чем это делает спам.

Когда существует необходимость отвергнуть почту с конкретного хоста или сайта мы рекомендуем использовать другие методы, упомянутые в этом документе (например, отвергать почту по адресу или имени SMTP_Caller, независимо от значения "MAIL From:").

2.6.1. "MAIL From: <>"

Недопустим отказ от приема почты с адресом "MAIL From: <>".

Адрес "MAIL From: <>" используется в сообщениях об ошибках от самой почтовой системы (например, когда используется легитимный транслятор и сообщение об ошибке возвращается пользователю). Отказ от приема таких сообщений означает, что пользователи не узнают об ошибках, возникших при доставке отправленной ими почты (например, сообщений "User unknown"), что будет приносить больше вреда, нежели спам.

Наиболее распространенным вариантом для сообщений, направленных с адреса адресу "MAIL From: <>", является их передача одному получателю (т. е., все сообщения об ошибках возвращаются одному лицу). Поскольку спамеры могут использовать "MAIL From: <>" для почты, адресованной множеству получателей, возникает соблазн отвергнуть такую почту совсем или отказаться от ее приема для всех адресатов, кроме первого. Однако существуют легитимные ситуации, когда сообщения об ошибках направляются множеству получателей (например, список рассылки с несколькими владельцами, расположенными на одном удаленном сайте), следовательно для агента MTA **недопустим** отказ от приема почты на основании адреса "MAIL From: <>" даже в таких случаях.

Однако MTA **может** снизить скорость соединения TCP (частоту вызова функции read()) при наличии множества адресов в поле "RCPT To:" и, таким образом, осложнить спамерам отправку почты с адресом "MAIL From: <>".

2.6.2. "MAIL From: <user@my.local.dom.ain>"

Недопустим отказ от приема почты с адресом "MAIL From: <user@my.local.dom.ain>".

С помощью "my.local.dom.ain" указывается, что имена трактуются как локальные и почта доставляется локально. На первый взгляд может показаться, что нет никого, кому требуется использовать адрес "MAIL From: <user@my.local.dom.ain>" и ограничения на использование этого адреса могут снизить риск обмана и таким образом уменьшить объем спама. Хотя это может быть верно для некоторых ситуаций, это ограничение будет препятствовать двум перечисленным ниже случаям легитимного использования:

- **псевдонимы** (файлы .forward).

  <user1@my.local.dom.ain> шлет письмо <user2@external.example> и эта почта пересылается обратно <user2@my.local.dom.ain> (например, в результате того, что <user2> был перемещен в my.local.dom.ain и его файл .forward находится в external.example.

- **списки рассылок**

  RFC1123 [3] указывает явное требование что адрес "MAIL From:" в почте из списка рассылок должен показывать владельца этого списка (list owner), а не конкретного отправителя. С учетом этого факта и того, что отправитель сообщения может находиться в другом домене по отношению к списку рассылки, почта может приходить в домен владельца списка из чужого домена с адресом владельца списка из локального домена в команде "Mail From:".

Если сообщения с "MAIL From: <user@my.local.dom.ain>" будут отвергаться, в обоих перечисленных случаях станет невозможной доставка легитимной почты.

2.7. Отказ по значению "MAIL From:"

Агентам MTA **следует** поддерживать возможность отказа от приема почты с конкретных адресов "MAIL From:" user (foo@domain.example) или целых доменов "MAIL From:" domain (domain.example). В общем случае спамеры легко обходят такие правила, часто меняя значения "MAIL From:". Однако возможность блокирования почты от отдельных пользователей или целых доменов может быть полезна в тех случаях, когда атака обнаружена до ее завершения.

Отметим еще раз, что почту с адресов

```
"MAIL From: <>"
```

и

```
"MAIL From: <user@my.local.dom.ain>"
```

недопустимо отвергать (см. выше) за исключением тех случаев, когда она должна отвергаться на основе других правил (например, когда адрес SMTP_Caller относится к сети, почта из которой не принимается совсем.

2.8. Контроль скорости

Агентам MTA **следует** предоставлять почтовому хосту средства для контроля за скоростью, с которой почта передается или принимается. Смысл использования контроля скорости описан ниже.

1) Если легитимный пользователь с существующей для него учетной записью начинает рассылать спам, возникает естественно желание ограничить скорость отправки. Такой подход может показаться спорным и пользоваться им следует с большой осторожностью, но он поможет защитить пользователей Internet от спама.

2) Если вас атакуют спамеры, этот метод позволит вам снизить скорость приема почты для данного пользователя или хоста.

При передаче почты контроль скорости осуществляется за счет снижения скорости соединения TCP (например, путем снижения частоты вызовов функции write()).

Для случая приема мы можем использовать такой же подход (например, снизить частоту вызовов функции read()) или передавать сигнал с кодом 4xx о невозможности приема почты. **Рекомендуется** принимать решение о выполнении таких операций на основании пользователя или домена в "MAIL From:", имени или адреса SMTP_Caller, адреса получателя "RCPT TO:" или комбинации этих параметров.

2.9. Проверка "MAIL From:"

Агенту MTA **следует** поддерживать возможность простой проверки корректности домена "MAIL From:" и отказа от приема почты из несуществующих доменов (т. е., доменов, для которых не удалось получить запись типа MX или A). Если сервер DNS сообщает о временной ошибке (TempFail), агент MTA **должен** возвращать код 4xx (Temporary Error). Если сервер DNS возвращает ошибку Authoritative NXdomain (неизвестный хост или домен), агенту MTA **следует** возвращать код 4xx (поскольку причиной может быть отсутствие синхронизации между первичным и вторичным DNS), но он **может** возвращать код 5xx (в зависимости от конфигурации).

2.10. Проверка <local-part>

Агенту MTA **следует** разрешать проверку локальной части адреса (<local-part>) в исходящей почте на предмет соответствия реальным именам пользователей и имеющимся в системе псевдонимам. Это предназначено прежде всего для защиты пользователей Internet от различных “опечаток”

```
MAIL From: <fo0bar@domain.example>
```

и/или недобросовестных отправителей

```
MAIL From: <I.am.unknown.to.you.he.he@domain.example>
```

Как обычно, такая защита достаточно легко обходится спамерами, он с ужесточением правил трансляции почты сделать это становится все сложнее. Фактически перехват “опечаток” на первом (и официальном) почтовом трансляторе уже является достаточной мотивацией для такой проверки.

2.11. SMTP-команды VRFY и EXPN

Обе команды SMTP VRFY и EXPN позволяют потенциальным спамерам проверить корректность адресов в своем списке (VRFY) и даже получить новые адреса (EXPN). Поэтому агенту MTA **следует** контролировать доступ к этим командам. Использование этих команд может быть разрешено или запрещено для всех (on/off) а также ограничено с помощью списков управления доступом, подобным упомянутым выше.

Отметим, что поддержка команды VRFY требуется спецификацией RFC821 [1]. Если вы отключили возможность реального использования этой команды или используете для нее списки управления доступом, можно просто возвращать "252 Argument not checked". Так следует поступать по умолчанию.

Команду EXPN по умолчанию следует отключать (off).

2.12. SMTP ETRN

Команда SMTP ETRN заставляет MTA заново обрабатывать свою почтовую очередь, что может оказаться достаточно дорогим делом и потенциально может использоваться для организации DoS-атак. Поэтому агентам MTA **следует** контролировать доступ к этой команде. Можно разрешить или запретить (on/off) использование этой команды для всех или разрешать доступ к ней на основе списков, подобных упомянутым выше. По умолчанию следует отключать команду (off).

2.13. Коды возврата

Основным критерием здесь должна быть гибкость. В рамках одного документа просто невозможно определить различия между возвратом кода 5xx при однократном отказе от приема легитимной почты вследствие конфигурационной ошибки и возвратом кода 4xx для обеспечения возможности записи сведений об ошибке в журнальный файл для ее последующего устранения.

Следовательно, агент MTA **должен** обеспечивать возможность настройки на возврат "Success[13]" (2xx), "Temporary Failure[14]" (4xx) или "Permanent Failure[15]" (5xx) для различных наборов правил. Точные значения кодов возврата кроме первых цифр (2, 4 или 5) не следует делать настраиваемыми через параметры конфигурации. Это обусловлено тем, что при настройке конфигурации легко допустить ошибки, а также тем фактом, что выбор точного кода возврата является весьма тонким делом, а многие реализации проверяют в кодах возврата не только первую цифру.

Однако, когда отклик обусловлен обращением к DNS, при котором был получен код TempFail (временная ошибка), агент MTA **должен** отразить это и возвратить код 4xx. Если отклик DNS был Authoritative NXdomain (хост или домен неизвестен), MTA **может** отразить это путем возврата кода 5xx.

Дополнительную информацию вы можете найти выше в обсуждении кодов возврата SMTP.

2.13.1. Важность обеспечения гибкости – простой пример

Сервер имен в Chalmers University of Technology содержит записи

```
cdg.chalmers.se.  IN  MX    0   mail.cdg.chalmers.se.
                  IN  MX  100   mail.chalmers.se.
```

Имеются также подобные записи для множества субдоменов. Второй хост используется для хранения почты в те периоды, когда основной сервер недоступен. Это означает, что хост mail.chalmers.se должен быть готов для использования в качестве почтового транслятора для субдоменов ("RCPT To:"), которые он обслуживает и почтовые хосты этих субдоменов принимают соединения SMTP от mail.chalmers.se. Свежие версии используемых для рассылки спама программ могут воспользоваться этим фактом, всегда обращаясь к хосту mail.chalmers.se для доставки почты в субдомены и почтовые хосты принимают эту почту, поскольку она приходит от легитимного транслятора, не имея возможности проверить реальный адрес или имя FQDN передающего спам хоста.

Пока сохраняется вторая запись MX на хосте mail.chalmers.se нет возможности запретить трансляцию почты по крайней мере с возвратом кодов 5xx. Однако этот хост может напрямую идентифицировать хосты, домены или сети и отвергать использование в качестве почтового транслятора для них (и только для них), возвращая код 4xx. Легитимная почта от них может быть задержана, если хост конечного получателя недоступен, но она в конце концов будет доставлена, когда хост заработает (код возврата 4xx) и это будет работать даже при смене записей MX. Спам получает отклик "Denied" при подключении к каждому из получателей, кто может отвергать соединения SMTP.

Использование второй строки (резервный сервер) возможно по двум причинам: 1) достаточная гибкость кода Relay Authorization и 2) достаточная гибкость выбора кодов возврата (MTA с кодом возврата делает такое использование абсолютно невозможным).

3. Продолжение работы

3.1. Влияние на пользовательские агенты SMTP и конечных пользователей

Хотя этот документ посвящен агентам доставки почты MTA и содержит рекомендации для них, он оказывает некоторое влияние на работу пользовательских агентов UA (User Agents – обычные почтовые программы).

Агенты UA:

1) Читают сообщения из почтовых ящиков и выводят их на экран. Для доступа к почте обычно используются протоколы POP, IMAP или NFS.

2) Читает пользовательский ввод с клавиатуры и передает его агенту MTA для доставки в качестве почтового сообщения. Для этого обычно используется протокол SMTP (т. е., тот же протокол, который применяется для обмена почтой между MTA).

Когда агенты MTA начали использовать различные антиспамовые фильтры, как описано выше, агенты UA на переносных компьютерах стали получать сообщения типа "Relaying Denied"[16] просто потому, что они использовали адреса IP из неизвестного диапазона или эти адреса преобразовывались в неизвестные имена FQDN.

Типичным случаем получения отказа от трансляции является использование переносного компьютера в менеджером по продажам, находящимся в командировке или даже делегатом на конференции IETF. Менеджер вероятно подключается к ближайшему ISP и получает адрес IP из пула этого провайдера, а делегат IETF будет использовать адрес IP из выделенного для таких подключений блока. В обоих случаях будут возникать проблемы при работе почтовой программы (UA – например, pine, Netscape, Eudora), которая будет пытаться отправить почту через “домашний” агент MTA (например, SMTP-SERVER=mail.home.example), но пока mail.home.example не будет обновлен для приема почты с этого (временного) адреса IP, он будет возвращать код "Relaying Denied" и отказывать в приеме почты.

[13]Успешное выполнение.
[14]Временный отказ.
[15]Постоянный отказ.
[16]Отказ в трансляции почты.

Для решения проблемы можно просто добавить временные адреса IP в список сетей, из которых принимается почта для трансляции, на mail.home.example. Это создает некоторый незначительный риск использования добавленных адресов спамерами, подключающимися к сети с адресами из добавленных блоков (например, через того же ISP во время нахождения менеджера в командировке). Однако риск достаточно мал, если не открывать постоянную трансляцию со всего мира и вести наблюдение за журнальными файлами транслятора с целью прекращения доступа из временного блока после того, как в этом отпадет необходимость.

Другим вариантом будет использование менеджером почтового транслятора местного провайдера, если такой транслятор предоставляется. Для использования этого метода нужно изменить SMTP-SERVER= в UA на переносном компьютере, что может оказаться слишком сложной задачей для менеджера.

Корректным способом решения проблемы было бы использование другого протокола между UA и MTA.

Хотя отдельного протокола подачи почтовых сообщений не существует, недавно был определено профиль SMTP для решения этой задачи - "Message Submission" [9].

Возможно также при использовании SMTP Authentication [10] применять Authenticated SMTP в качестве протокола для обмена между UA и домашним агентом MTA (не имеет значения рассматривать этот протокол как новый или тот же самый SMTP).

Это добавляет один элемент в алгоритм трансляции, предложенный в параграфе 2.1:

+ **If "SMTP Authenticated" then accept to Relay[17].**

3.2. Персональные фильтры спама

Пользователями электронной почты являются конкретные люди и мало надежды на то, что то или иное централизованное средство борьбы со спамом будет удовлетворять всех и каждого. На практике люди могут и будут говорить о нарушении свободы слова, если то или иное централизованное правило борьбы со спамом будет использоваться без одобрения пользователей. Кто-то может сказать, что от спама никому нет пользы, но в любом случае каждый волен принимать решение сам а не зависеть вынужденно от централизованных правил.

Следовательно, единственным приемлемым решением является разрешение на использование персональных антиспамовых фильтров. Такие фильтры подобны описанным выше, но применяются и настраиваются каждым пользователем независимо. Поскольку большинство пользователей не имеет четкого представления о том, что следует делать (за исключением единодушного желания избавиться от спама), почтовой системе следует обеспечивать принятый по умолчанию набор правил и предоставлять каждому пользователю возможность изменения этих правил для себя. В среда типа UNIX это может выглядеть примерно так:

```
/etc/mail/rc.spam
~/.spamrc
```

К этому добавляются правила взаимодействия между первой и второй конфигурацией.

Все это создает достаточное количество нерешенных проблем. Например, следует ли разрешать пользователям самим задавать коды возврата SMTP, как описать эти коды для несведущего пользователя и как существующие почтовые системы будут разбираться с возвращаемыми от пользователей кодами, особенно в тех случаях, когда вперемешку возвращаются коды 5xx и 4xx, как показано ниже:

```
C  MAIL From: <usr@spam.example>
S  250 <usr@spam.example>... Sender ok
C  RCPT To: <usr@domain.example>
S  250 <usr@domain.example>... Recipient ok
C  RCPT To: <foo@domain.example>
S  451 <foo@domain.example>... Denied due to spam list
C  RCPT To: <bar@domain.example>
S  550 <bar@domain.example>... Denied due to spam list
```

Естественно, что можно ограничиться кодами "250 OK" или "550 Denied", не предоставляя пользователям других вариантов, но и в этом случае возникает вопрос, как объяснить рядовому пользователю значение "Refuse 'MAIL From: <.*@spam.example>'" и то, что это может привести к отказу от приема ожидаемого сообщения.

3.3. Аутентификация SMTP

Аутентификация SMTP [10] уже была предложена в качестве проверки полномочий при трансляции почты, однако этим преимущества данного метода не ограничиваются. При полной реализации SMTP Authentication спамерам будет значительно сложнее использовать подставные адреса и прятаться за чужими хостами.

3.4. Спам и NAT

По мере расширения использования систем трансляции адресов (NAT[18]) может возникнуть необходимость записи в системные журналы дополнительной информации. При использовании взаимно-однозначного (1:1) отображения между внешними и внутренними адресами проблем не возникает, но если NAT транслирует также номера портов (для объединения множества внутренних хостов на одном доступном извне адресе[19]), потребуется записывать не только IP-адреса связанных со спамом хостов, но и номера портов. Иначе не будет возможности идентификации конкретного хоста, использующего NAT.

4. Вопросы безопасности

Подобное лесному пожару распространение спама показало наличие некоторых проблем безопасности, которые, по сути, создают риск для всех пользователей электронной почты Internet:

- Люди могут не найти нужную почту в своих заполненных спамом ящиках или удалить нужное сообщение вместе со спамом.

[17]Если используется SMTP Authenticated, принимать соединения и выполнять трансляцию.
[18]Network Address Translators – трансляция сетевых адресов.
[19]Существуют и другие варианты трансляции адресов, которые не используют взаимно-однозначного отображения между внутренними и внешними адресами. См., например, RFC 3022. *Прим. перев.*

- Почтовые системы ISP и особенно дисковые подсистемы с почтовыми ящиками перегружены. Расчистка пользовательских почтовых ящиков требует значительных людских ресурсов. Фактически почтовые серверы ISP рушатся под лавиной почты.
- Когда диски становятся недоступными в результате переполнения или исчерпания почтовых квот, важные сообщения могут задерживаться или теряться совсем. Обычно этого не происходит без уведомления, но если переполнены диски как на стороне получателя, так и на стороне отправителя, невозможность доставки может остаться незамеченной. Таким образом, уровень доверия к почтовой системе существенно снижается.
- На хостах, используемых в качестве почтовых трансляторов без проверки полномочий, возникают перегрузки. Кроме возникновения технических проблем это требует значительных людских ресурсов для очистки очередей и работы с внешними пользователями, рассылающими спам через этот транслятор.
- Принимаемые против спамеров меры включают блокирование их хостов, как описано в этом документе. Однако существует значительный риск ошибочного блокирования почтовых трансляторов, несмотря на то, что они сами являются жертвами спама. В долгосрочной перспективе это может привести к разрушению почтовой системы Internet.
- Широкое использование подставных адресов "MAIL From:" и "From:" наносит ущерб репутации невинных людей, хостов и организации. Это может оказывать существенное влияние на бизнес в целом.

Некоторые из описанных здесь методов увеличивают нагрузку на некоторые системы поддержки и саму систему электронной почты. К системам поддержки относятся DNS, системные журналы, базы данных со списками локальных пользователей, механизмы аутентификации и т. п. реализация описанных в документе методов будет повышать риск атак на соответствующие службы поддержки путем передачи на сайт больших объемов спама. Средства ведения системных журналов, например, должны обслуживать большее количество записей (что произойдет, когда журнальные файлы заполнят диск?). серверы DNS и механизмы аутентификации также должны справляться с растущей нагрузкой.

Функционирование систем поддержки при высокой нагрузке следует внимательно изучить до реализации описанных в этом документе методов.

Следует внимательно изучить поведение почтовой системы (например, ее реакцию на отказ одной или нескольких служб поддержки). Для почтового сервера **недопустим** возврат кодов "Permanent Failure" (5xx) при возникновении временных проблем в используемых им системах поддержки.

5. Благодарности

Этот документ является результатом дискуссий в специальной группе шведских ISP и университетов. Мы не будем перечислять здесь конкретных людей, ограничившись указанием доменных имен - algonet.se, global-ip.net, pi.se, swip.net, telia.net, udac.se, chalmers.se, sunet.se, umu.se, and uu.se.

Мы хотим поблагодарить за полезные замечания и предложения Andras Salamon, John Myers, Bob Flandrena, Dave Presotto, Dave Kristol, Donald Eastlake, Ned Freed, Keith Moore и Paul Hoffman.

Большое спасибо Harald Alvestrand и Patrik Faltstrom за их полезные комментарии, а также поддержку и руководство при контактах с IETF.

6. Литература

[1] Postel, J., "Simple Mail Transfer Protocol", STD 10, RFC 821[20], August 1982.

[2] Crocker, D., "Standard for the format of ARPA Internet text messages", STD 11, RFC 822, August 1982.

[3] Braden, R., "Requirements for Internet hosts - application and support", STD 3, RFC 1123[21], October 1989.

[4] Bradner, S., "Key words for use in RFCs to Indicate Requirement Level", BCP 14, RFC 2119[21], March 1997.

[5] Mockapetris, P., "Domain Names - Concepts and Facilities", STD 13, RFC 1034, November 1987.

[6] Mockapetris, P., "Domain Names - Implementation and Specifications", STD 13, RFC 1035, November 1987.

[7] Eastlake, D. and C. Kaufman, "Domain Name System Security Extensions", RFC 2065, January 1997.

[8] Сайт sendmail http://www.sendmail.org

[9] Gellens, R. and J. Klensin "Message Submission", RFC 2476[21], September 1998.

[10] Myers, J., "SMTP Service Extension for Authentication", Work in Progress[22].

Адрес редактора

Gunnar Lindberg

Computer Communications Group

Chalmers University of Technology

SE-412 96 Gothenburg, SWEDEN,

Phone: +46 31 772 5913

FAX: +46 31 772 5922

EMail: lindberg@cdg.chalmers.se

[20] На сайте http://www.protocols.ru имеется перевод на русский язык более современного варианта спецификации протокола – RFC 2821. *Прим. перев.*

[21] На сайте http://www.protocols.ru имеется перевод этого документа на русский язык. *Прим. перев.*

[22] К настоящему времени работа завершена и документ опубликован как RGC2554. Перевод имеется на сайте http://www.protocols.ru. *Прим. перев.*

Перевод на русский язык
Николай Малых

BiLiM Systems

nmalykh@bilim.com

тел. (812) 4490770

Полное заявление авторских прав