ОБЗОР МЕТОДОВ ФИЛЬТРАЦИИ СПАМА ЭЛЕКТРОННОЙ КОРРЕСПОНДЕНЦИИ

Варешнюк І. В.
Национальный технический университет "Харьковский политехнический институт",
г. Харьков, ул. Пушкинская, 79/2, тел. 707–63–60,
e-mail: *innominatus_tru@mail.ru*

Сейчас, в эпоху современных компьютерных технологий, спам является одной из основных проблем, с которой пользователям сети Интернет ежедневно сталкиваются, потому что они уже не в силах отказаться от возможностей, которые открыла для них всемирная паутина.

Под спамом в наиболее общем смысле понимают незапрашиваемую информацию, то есть, все, что Вы получаете, вне зависимости от Вашего желания.

Не зависимо от наличия коммерческих или рекламных целей спам всегда преследует одну цель – довести свою информацию до максимально возможного числа адресатов при минимальных издержках. Причем "авторов" не волнует состав аудитории, главное – количество [1].

Существует несколько основных видов спама, имеющих много общего и в то же время отличающихся друг от друга. Самым большим потоком спама является почтовый спам, который распространяется через электронную почту. В настоящее время доля вирусов и спама в общем трафике электронной почты составляет по разным оценкам от 70 до 95 процентов [2].

Поэтому в дальнейшем будем рассматривать именно этот вид спама [3].

Рассмотрим методы, используемые для фильтрации спама:

1. Статистические метода фильтрации спама. Программы автоматической фильтрации используют статистический анализ содержания письма для принятия решения, является ли оно спамом. На практике пользуются популярностью методы байесовской фильтрации спама или различные ее вариации.
2. Черные списки – списки IP-адресов компьютеров, о которых известно, что с них ведётся рассылка спама.
3. Авторизация почтовых серверов – различные способы для подтверждения того, что компьютер, отправляющий письмо, действительно имеет на это право (Sender ID, SPF, Caller ID, Yahoo DomainKeys, MessageLevel).
4. Серые списки. Метод серых списков основан на том, что «поведение» программного обеспечения, предназначенного для рассылки спама, отличается от поведения обычных почтовых серверов, а именно, спамерские программы не пытаются повторно отправить письмо при возникновении временной ошибки, как того требует протокол SMTP.
5. Проверка соблюдения требований протокола SMTP.
6. Общие ужесточения требований к письмам и отправителям, например –

отказ в приеме писем с неправильным обратным адресом (письма из несуществующих доменов), проверка доменного имени по IP-адресу компьютера, с которого идет письмо, и т. п.

7. Сортировка писем по содержанию полей заголовка письма даёт возможность избавиться от некоторого количества спама.

8. Системы типа «вызов-ответ» позволяют убедиться, что отправитель – человек, а не программа-робот. Использование этого метода требует от отправителя выполнения определённых дополнительных действий, часто это может быть нежелательно, так как многие реализации таких систем создают дополнительную нагрузку на почтовые системы.

9. Системы определения признаков массовости сообщения, такие как Razor и Distributed Checksum Clearinghouse.

10. Общее изменение идеологии работы электронной почты, при которой для принятия сервером получателя каждого сообщения система отправителя должна выполнить определенное «затратное» действие. Для обычных пользователей, отправляющих десятки писем, это не составит затруднения, тогда как затраты спамера умножаются на количество отправляемых им писем, обычно измеряемое миллионами [2].

В заключение, необходимо отметить, что каждый из вышеперечисленным методов, используемый по отдельности, является недостаточно эффективным.

Поэтому большинство коммерческих и свободно распространяемых спам-фильтров, используют одновременно несколько методов фильтрации, выстраивая их в цепочки, в которых команды SMTP и электронное письмо будет передаваться каждому фильтру по очереди. В случае отрицательного ответа хотя бы одного фильтра письмо будет отвергаться [4].

Список литературы

1. http://antispam.rin.ru/mytest2.htm
2. http://ru.wikipedia.org/wiki/Спам
3. http://www.securelist.com/ru/threats/spam?chapter=151
4. http://gate.udec.ntu-kpi.kiev.ua/~bat/exp/about-spam.html