# Эта назойливая муха СПАМ

**ПОТОК НЕЖЕЛАТЕЛЬНОЙ ПОЧТЫ
РЕКЛАМНОГО ХАРАКТЕРА — СПАМА-
УГРОЖАЕТ ЦЕЛОСТНОСТИ ИНТЕРНЕТА.
ПРОГРАММИСТЫ ПОСТОЯННО ИЩУТ
НОВЫЕ СПОСОБЫ БОРЬБЫ С НИМ,
А СПАМЕРЫ — ПУТИ ОБХОДА ЛОВУШЕК.**

Первое спамовое сообщение с рекламой компьютера DECsystem20, разосланное отделом маркетинга корпорации DEC, 400 пользователей сети Arpanet получили в 1978 г. Сегодня нежелательная корреспонденция рекламного характера — это две трети всех передаваемых через Интернет сообщений. В почтовом ящике каждого третьего пользователя электронной почты около 80% писем оказываются спамом. Еще опаснее он стал с появлением так называемого фишинга: мошенники рассылают письма от имени банков или крупных компаний и получают доступ к номерам кредитных карт и другой конфиденциальной информации. Согласно исследованиям, проведенным компанией Gartner Research, в 2004 г. ущерб от фишинговых атак только в США составил $1,2 млрд. Снам встречается не только в электронной почте. Например, в чатах специальные программы-роботы выдают себя за людей и заманивают простаков на порносайты. Так называемые ссылочные спамеры нарушают работу поисковых систем, добавляя гиперссылки, искажающие поисковый рейтинг веб-ресурсов.

Для того чтобы в один непрекрасный день поддерживающие Интернет системы не захлебнулись в потоке бесполезной информации, программисты разрабатывают методики борьбы с различными проявлениями спама. Ни одну из них нельзя считать универсальной, однако эффект от совместного применения разных подходов множеством пользователей может превзойти все ожидания. И пользователи вправе надеяться, что когда-нибудь их почтовые ящики будут полностью очищены от назойливой рекламы

**Письма, которых никто не ждет**

Быстрый рост количества нежелательных сообщений объясняется исключительной дешевизной их распространения. По оценкам американских исследователей Д. Гудмана, Д. Хеккермана и Р. Раунвейта, одно сообщение стоит меньше 0,01 цента. При таких демпинговых ценах спамер не в накладе, даже если прибыль с продажи единицы рекламируемого товара составляет лишь $11, а коэффициент отклика на рекламу не превышает 1/100 тыс. Таким образом, получатели спама страдают по вине тех, кто покупает эти товары.

Самое неприятное, что каждый раз, когда программисты находят очередное противоядие, спамеры изобретают обходной путь. В результате противоборствующие стороны невероятно усовершенствовали и усложнили свой арсенал. Особую сложность представляет правовая идентификация спама. В законодательстве большинства развитых стран (Украины это не касается. У нас вообще нет никаких его юридических определений) под спамом подразумевается самовольная рассылка коммерческого сообщения без установления деловых отношений. Такое описание весьма размыто. Допустим, автор получил предложение о съемке фильма по мотивам опубликованной им в Интернете истории. Все признаки совпадают с юридическим определением: самовольное, коммерческое, от неизвестного отправителя. Но вряд ли кто-то назовет это нежелательным сообщением. Можно уточнить формулировку и добавить фразу о том, что спам рассылается массово. Однако если сообщение, например, об организации будущей выставки или конференции, рассылается массово (а в противном случае мероприятие не имеет смысла), оно тут же попадает под определение спама. Возможно, самым явным его признаком является неопределенность целевой аудитории и ненужность для адресатов. Абсолютно точно определить снам крайне сложно, при этом, как и порнографию, пользователь без труда выделяет его среди других электронных писем.

**Как борются с потоком коварных почтовых сообщений**

В 1997 г. Дэвид Хеккерман предложил для эффективной борьбы с нежелательной корреспонденцией разработать самообучающуюся программу. С тех пор было создано множество программных средств для предотвращения спама. Первой методикой стала так называемая техника сравнения отпечатков. Вначале нужно найти ряд спамовых сообщений, и занести их характерные отпечатки в базу данных программы.Отпечаток — это номер, который присваивается письму исходя из его содержания. Под содержанием подразумевается, конечно, не смысл письма. Сделать это можно примерно так: к энному количеству букв «а» прибавляется количество букв «в», умноженное на 10, затем количество ~ ' букв «в», умноженное на 100, и т.д. Когда придет новое письмо, программа рассчитает его отпечаток и при совпадении с любым из имеющихся в базе удалит сообщение или отправит в архив. Спамеры быстро нашли способ защиты от столь прямолинейных методов борьбы и стали помещать в свою корреспонденцию случайные символы. Борцы с почтовой рекламой ответили усложнением техники расчета отпечатков и научились выявлять бессмысленные наборы символов. Тогда спамеры начали добавлять более информативные вставки, например прогнозы погоды или биржевые сводки. Кроме того, изменяли написание слов. Скажем, в слове «доход» вместо буквы «о» вставляется ноль. Некоторые фильтры анализируют имеющиеся в сообщениях ссылки, однако спамеры постоянно регистрируют новые веб-адреса, указывают фальшивый адрес отправителя, который вводит получателя в заблуждение. А новое доменное имя, создаваемое для обмана систем, ведущих списки запрещенных URL (uniform resource locator— унифицированный указатель информационных ресурсов), вообще может регистрироваться каждые несколько минут. Разбивка слов на части, фиктивный IP-адрес компьютера-«зомби», зараженного вирусом и рассылающего сообщения, — чего только не придумали спамеры для достижения своей цели! Короче говоря, создание систем, основанных на вычислении отпечатков, превратилось в кошмар.

**Самообучающиеся системы**

Придя к выводу о малоперспективности подобных методов борьбы со спамом, ученые занялись разработкой самообучающихся систем. Такие программы постепенно учатся выбирать из потока корреспонденции письма со спамом, и их уже нелегко обмануть простым добавлением случайной информации. Первым был опробован алгоритм Байеса, ставший наиболее распространенным методом обучения систем. Этот алгоритм заключается в определении вероятности появления слов в письме. Например, слова «нажми», «здесь» и «отписаться» в спамовых сообщениях появляются с вероятностью 0,9, а в обычных — с вероятностью 0,2. Перемножив вероятности появления всех слов сообщения и применив определенные статистические правила, можно оценить вероятность того, что данное письмо является спамом. Этот алгоритм быстро учится правильно отличать полезные сообщения от спама и хорошо противостоит простым спамерским уловкам. Однако слова в письме не являются независимыми друг от друга. Так, слова «нажми» и «здесь» часто встречаются вместе, поэтому результаты анализа зачастую искажаются. Далее работа сосредоточилась на моделях, в которых используется весовая оценка признаков (слова и свойства письма, например, количество адресатов, которым оно отослано). Такие алгоритмы способны в некотором смысле изучать взаимосвязь различных признаков. При обычном анализе Байеса сообщение со словами «нажми», «здесь» и «отписаться» программа может удалить как спам. Но одновременно уничтожит и полезные сообщения. Более сложная модель примет во внимание, что в нежелательных письмах названные слова обычно находятся рядом, и назначит им меньший «вес». Со временем система поймет, что слово «здесь» встречается довольно часто, и перестанет учитывать его. В результате обучения программа усвоит, что некоторые слова нейтрализуют друг друга. Преимущество простых систем в том, что их легко обучать. Определение «веса» намного сложнее: программист должен перепробовать множество комбинаций слов и признаков, чтобы определить оптимальный набор, характерный для спамового сообщения. К счастью, исследователи достигли значительного прогресса в данной области. Ряд разработанных методов работают в десятки и сотни раз быстрее своих предшественников. А когда для обучения системы приходится обрабатывать миллионы сообщений и рассчитывать сотни тысяч весовых коэффициентов, скорость алгоритма становится важнейшим параметром.

**<Веселые картинки>**

Иногда спамеры прячут рекламу в рисунках, содержание которых невозможно проанализировать с помощью обычного обучаемого алгоритма. В этом случае наиболее перспективный подход — распознавание изображения (как при обработке отсканированного текста) и передача результатов обучаемому фильтру. Одно из самых неприятных свойств спама — периодическое появление в почтовых ящиках пи-сем с порнографическим содержанием. Сегодня программы распознавания таких материалов широко применяются для ограничения доступа детей к сомнительным веб-ресурсам и борьбы с размещением откровенных картинок на серверах бесплатного хостинга. И все же анализ изображений занимает слишком много времени, а его качество зачастую оставляет желать лучшего: обычные фотографии, на которых изображены большие участки кожи, нередко отфильтровываются как спам.

**Кто там**

Хотя методы фильтрации хорошо зарекомендовали себя, спамеры всегда будут стараться обойти их. Поэтому вместо того чтобы пытаться выиграть бесконечное соревнование, лучше изменить правила игры. Для этого можно использовать системы подтверждения, которые будут требовать от спамеров больше, чем те смогут себе позволить. Первое спамовое письмо было направлено по 400 адресам, набранным вручную. Сегодня снам рассылается автоматически. Если отправитель сможет доказать, что он не робот, значит, скорее всего, он не спамер. Мони Наор из Израильского института им. Вейцмана предложил различные способы интерактивного подтверждения человека (HIP — human interactive proofs) и несколько тестов, позволяющих отличить компьютеры от людей (тесты Тьюринга). Речь идет о задачах, которые слишком сложны для вычислительных машин, но без труда решаются любым человеком. Например, люди, в отличие от машин, легко распознают искаженные алфавитно-цифровые символы. HIP входит в состав системы опознавания, определяющей, что отправитель — человек. Если адрес отправителя содержится в «белом списке» получателя, письмо доставляется сразу, если нет, то отправителю направляется запрос с предложением распознать HIP. Такая система очень надоедлива. Мало кто согласится разгадывать HIP. Автоматическая система подтверждения, разработанная Мони Наором и его коллегой Синтией Дворк, предлагает компьютеру отправителя перед отсылкой письма решить вычислительную задачу. Идея в том, чтобы заставить спамера тратить на отправку сообщения больше времени, чем он может себе позволить. Эти вычислительные задачи чем-то похожи на составные картинки-головоломки: сложно решить, но легко проверить. Чтобы быстро справляться с такими задачами, спамерам придется покупать множество компьютеров, что сделает массовую рассылку просто невыгодной.

В другой системе подтверждения используются деньги. Отправители прикрепляют к сообщению электронный чек на небольшую сумму, предположим на 1 цент. Если сообщение легитимно, пользователь игнорирует чек, но если это спам, механизм компенсации позволяет получателю обналичить его. Система запрещает отсылку писем при нулевом балансе на счету абонента. Для обычных пользователей электронная почта бесплатна, но для спамеров цена сообщения вырастает примерно в 100 раз, и рассылка становится им не по карману. Клиентам интернет-провайдеров выставляется виртуальный счет с небольшой суммой, так что им отправка писем ничего не стоит.

**Как сообщает NetNews, Россия сейчас генерирует 27,9% от общего количества червей, вирусов, троянов, шпионских модулей и прочих опасных спамерских программ. Китай, который еще недавно удерживал лидирующие позиции по объемам выпускаемых вредоносных программ, теперь отступил на вторую позицию с показателем 26,5%. Замыкают тройку крупнейших стран-е вирусораспространителей США (10%)**

С виду концепция проста, но ее практическая реализация сопряжена с некоторыми сложностями. Системы электронных переводов требуют определенного управления и поэтому не бесплатны. Чтобы проводить электронные платежи, нужно решить ряд вопросов. В частности, откуда возьмутся деньги для платежей, кто будет осуществлять транзакции и получать прибыль, как система может противостоять мошенничеству

**Сборная корзинка**

Лучшая стратегия борьбы со спамом — сочетание фильтрации с механизмами подтверждения: HIP, вычислительными задачами и микроплатежами. В таком случае, если адрес отправителя не содержится в разрешенном списке, письмо направляется на обучаемый спамовый фильтр для максимально агрессивного поведения системы. Если сообщение вызывает малейшее подозрение, отправитель проверяется. Таким образом, легитимность большинства обычных писем проверяться не будет, так что нагрузка невелика. Затем отправителю предлагается либо решить HIP или вычислительную задачу, либо совершить микроплатеж. Если на компьютере пользователя установлено новейшее ПО, оно решит вычислительную задачу автоматически. В противном случае отправитель решит HIP либо предпочтет микроплатеж.

**Будущее без спама**

Компьютерная промышленность, независимые разработчики и научное сообщество продолжают искать способы борьбы со спамом. Инженеры из IBM показали, как использовать для фильтрации спама технологии биоинформатики, изначально созданные для нахождения генов по шаблону. Другие исследователи продемонстрировали, что эффективность систем, работающих по отпечаткам, возрастает при добавлении нескольких словарей. Сотрудники Калифорнийского университета выяснили, почему добавление нескольких одинаковых слов позволяет обойти антиспамовые фильтры и как обучить их (фильтры) противостоять этому.

Есть веские основания сомневаться в том, что системы борьбы со спамом когда-нибудь его остановят. Всегда найдутся люди, стремящиеся доставить нам свои сообщения. Но поток нежелательной корреспонденции все же можно превратить в тоненькую струйку.