**По обе стороны спама**

Никита Пасынков

Спам раздражает. Спамеров ненавидят все интернет-пользователи, которым приходит в день по 20-80 писем с предложением купить пилюли, вызвать грузчиков или пройти курс английского языка. Про спамеров сочиняют анекдоты, в которых прочат им самые страшные страдания в аду, куда они, без всяких сомнений, обязательно попадут после долгой, мучительной смерти от рук несчастных пользователей интернета. Но если отбросить лирику, спам - это и серьезные деньги, и серьезные проблемы. Для всех участников процесса.

В феврале 2005 года Rockbridge Associates совместно с Center for Excellence in Service выпустили отчет, согласно которому ежегодные убытки американских компаний от спама оцениваются в $22 млрд. При этом исследователи брали в расчет только рабочее время, которое американцы тратят на удаление и просмотр спама, и не учитывали затраты на оплату интернет-трафика, поскольку в США наиболее распространены безлимитные подключения. В России же большая часть людей платит или за время доступа в сеть, или за объем скачиваемой информации. Поэтому каждое новое письмо с предложением купить ручку с исчезающими чернилами или вечный фонарик приносит пусть копеечный, но убыток конкретному человеку. Когда этих писем миллионы, общая сумма получается весьма внушительной. Александр Иванов, президент Ассоциации документальной электросвязи, в марте 2004 года оценил ущерб российских операторов и пользователей интернета от рассылки несанкционированных рекламных сообщений в $55 млн в год. Компания "Ашманов и партнеры" считает эту цифру сильно заниженной и в аналитическом отчете "Спам 2004" оценивает убытки от спама в 250 млн евро.

**Разделение труда**

На спамерской стороне баррикад деньги зарабатываются тремя способами. Во-первых, разработка и продажа технологий для рассылки спама. Это программы, рассылающие миллионы писем в течение пары часов, обходящие антиспам-фильтры, заражающие компьютеры вирусами для дальнейшего сбора контактов или прямой рассылки писем. Во-вторых, работает бизнес по сбору и продаже баз данных e-mail адресов. В-третьих, на спаме наживаются компании, непосредственно рассылающие непрошенные письма. Зачастую по всем трем направлениям работает одна компания, однако в последние годы в среде спамеров происходит более четкое разделение труда.

Сколько зарабатывают разработчики технологий, оценить невозможно. Это наиболее закрытый сектор спамового бизнеса. С базами e-mail адресов картина более прозрачная: в России они продаются в среднем по $30-60 в зависимости от количества адресов и уровня их упорядоченности. Но четкую оценку объемов этого рынка дать нельзя, поскольку даже точное количество работающих в этом направлении компаний и частных лиц неизвестно.

Наибольшие же прибыли получают люди, рассылающие спам в промышленных масштабах.

**"Серые" и "черные"**

В зависимости от целей, которые они преследуют, спамеров делят на "серых" и "черных". "Серый" спам - это реклама легальных услуг или стимулирование продаж каких-то товаров, но посредством незапрошенной рассылки коммерческой информации. Грузчики, курсы английского языка, обогреватели и тренажеры - все это "серый" спам. Его используют преимущественно представители малого бизнеса, у которых нет денег на традиционную солидную рекламу. Спам остается феноменально дешевым рекламным инструментом: стоимость 1 тыс. контактов составляет порядка $0.01. И как бы люди ни проклинали надоедливые письма, в 2004 году 14% получателей спама признались, что постоянно просматривают эти сообщения, а 4% - воспользовались предложением, полученным столь ненавистным, казалось бы, способом (данные National Technology Readiness Survey). Спам работает, и именно поэтому им пользовались, пользуются и будут пользоваться дальше. Конечно, когда компания подрастет и заработает денег для размещения объявления в газете или ролика на радио, она откажется от спама, чтобы не портить себе имидж. Но ее место тут же займет маленькая фирма, у которой нет ни имиджа, чтобы о нем заботиться, ни денег, чтобы их потратить на рекламный блок в журнале.

"Серый" спам условно легален. Конечно, он нарушает антиспамовое законодательство, но ведь и не во всех странах таковое существует. Другое дело "черный" спам, под которым понимают в первую очередь мошенничество, прибегающее к массовым рассылкам как каналу распространения информации. В русскоязычном интернете это направление еще уступает позиции "серым" рассылкам, но в США и Европе спам гораздо более криминализирован. Он используется преимущественно для продажи самой разной контрафактной продукции, детской порнографии, нелицензированных лекарств. Отдельное направление электронного мошенничества - "фишинг", активно развивавшийся в прошлом году. Злоумышленники рассылают письма, например, от лица банка или платежной системы, с просьбой под тем или иным поводом (получение дополнительных возможностей, восстановление работы системы после сбоя в базе данных и т. д.) сообщить пароль к электронному счету или номер кредитки. Некоторые доверчивые люди передают все эти данные: ведь в поле "отправитель" написано Citibank или PayPal - компании, которые они знают, которым они верят. В результате все деньги со счета беспечного пользователя исчезают в тот же день.

Не менее активно спам используется для "черного" пиара. Во время последних парламентских выборов в русскоязычном интернете были разосланы письма якобы от "Единой России", обращенные к руководителям компаний, с "убедительной просьбой" организовать партийные ячейки ЕР среди своих работников. На следующий же день партия заявила, что не имеет никакого отношения к этой рассылке.

**Охотники за привидениями**

Кроме криминальности и навязчивости, спам имеет еще одно неприятное свойство, касающееся всех пользователей интернета: огромный (75-85% от всего объема электронной почты) поток писем, рассылаемых с несуществующих адресов, перегружает сервера провайдеров, что в конечном счете негативно сказывается на работе интернета в целом.

Впрочем, даже если бы технически спам никому не мешал, с ним бы все равно активно боролись. И эта борьба - тоже прибыльный бизнес. По оценкам IDC, рынок продаж антиспам-фильтров в 2004 году составил порядка $500 млн. Частные лица покупают средства для борьбы со спамом в пакете с другими программами для обеспечения безопасности компьютера. Крупными заказчиками антиспам-технологий являются публичные почтовые сервисы, для которых защита ящиков своих пользователей от нежелательных писем - ключевой момент удержания аудитории.

Крупные корпорации, такие, как Microsoft, объявляют войну против спамеров, возбуждают против них судебные иски и разрабатывают технологии защиты от спама. Для корпораций эта борьба - в первую очередь PR, увеличение лояльности к своему брэнду. Люди так ненавидят спам, что готовы полюбить кого угодно, лишь бы он защитил их от лавины назойливых писем.

Ожидать победы над спамом в ближайшее время не стоит. Одновременно с развитием фильтров появляются новые технологии рассылки спама, которые умеют эти ограничения обходить. Постоянные "догонялки", в которые играют спамеры и борцы с ними, всего лишь сдерживают бесконтрольный рост нежелательных рассылок, но не решают проблему. На данный момент не существует ни одного проекта, на который можно было бы возложить большие надежды и ждать, когда придет самое-самое последнее письмо с предложением купить вечный фонарик.

**Электронное письмо является спамом**

Если персоналия получателя не связана с контекстом письма, поскольку последнее равно может быть обращено ко многим другим потенциальным получателям.

Если получатель не выразил в форме, допускающей проверку, намеренное, явное и действующее на момент посылки разрешение на посылку данного письма.

Если акт пересылки и получения письма с точки зрения получателя приносит непропорциональную выгоду отправителю.