УДК 004.4.056

СПАМ И МЕТОДЫ БОРЬБЫ С НИМ

Белоглазова А.В.
Научный руководитель – ассистент Шапуркина Ю.С.
Сибирский Федеральный Университет, г. Красноярск

Бурное развитие информационных и коммуникационных технологий, несосмненно, привело к положительным результатам развития общества. Однако, существуют и негативные последствия информатизации и компьютеризации, одним из которых является спам – незаконно распространяемая путем массовых рассылок информация рекламного характера, получение которой не согласованно с пользователем.

По данным исследования, проведённого Европейской Комиссией, ежедневный поток спама обходится интернет-пользователям в общей сложности в 10 млрд. евро в год. Цена баз данных по адресам колеблется от 100 долларов за 100 млн. (США) и до 100 долларов за пакет из 100 тысяч электронных адресов (Россия).

Признаки спама:

1. Рассылка носит массовый характер.
2. Не указан источник, из которого взят ваш адрес.
3. Подробная реклама, а также приаттаченные файлы.
4. Примерно следующая фраза: «Если вы не желаете в дальнейшем получать нашу информацию, то пошлите нам письмо».
5. Полное отсутствие извинений.
6. Отсутствующий или неправильный обратный адрес.

Сообщение в зависимости от целей и задач отправителя может содержать коммерческую информацию, а может не иметь отношения к коммерческой деятельности, поэтому выделяют *коммерческий спам* и *некоммерческий*.

В подавляющем большинстве спам используется для рекламы какого-нибудь товара или услуги, иногда для накручивания счетчиков на сайте, реже для засылки вирусов. Но можно выделить общую цель спама - довести свою информацию до максимально возможного числа адресатов при минимальных издержках. Причем авторов не волнует состав аудитории, главное - количество.

Основные цели спама:

1. Реклама товара и услуг. Послания такого рода расхваливают какой-нибудь реальный товар или услуги, и указываются ссылки на сайт, на котором можно подробнее ознакомиться и приобрести товар, или номер телефона, по которому можно сделать заказ.
2. Раскрутка сайта. Информация может быть разнообразной. В основном, рекламируется что-то очень хорошее и/или бесплатное. Ссылка же ведет на сайт, который совершенно не имеет отношения к этой информации. Но рейтинг сайта повышается за счет обманутых посетителей. Иногда послание может быть совершенно пустым, а страница со счетчиком программно открывается в новом окне.
3. Платные звонки. Рекламируется товар и указывается номер телефона, за звонок по которому приходит счет.
4. Маркетинговые исследования. Под видом опроса или заказа предлагают заполнить анкету и отослать данные по указанному адресу.
5. Засылка разрушающего программного обеспечения.
6. Прочие цели.

Технология спама достаточно проста и эффективна. Самым важным является база данных по электронным адресам. Сбор адресов производится с помощью специальных программ, которые путешествуют по интернету и собирают любые данные по шаблону.

Рассылка производится, как правило, с анонимных или собственных почтовых серверов, обратные адреса ставятся либо чужие, либо ложные, но иногда бывают и настоящие.

Каковы же последствия спама?

В данной ситуации выигрывает только спамер (получивший деньги за рассылку) и его заказчик (продавший какое-то количество своих товаров). Все остальные оказываются в проигрыше: причем большее значение играет не финансовая сторона, а моральная: наличие каких-то посторонних писем, идущих непрекращающимся потоком, приводит в состояние ярости и раздражения.

Негативное влияние спам оказывает не только на тех, кто получает его, подобная практика может подорвать уважение и надолго дискредитировать человека или организацию. И именно поэтому ни одна уважающая себя фирма не допускает такой рекламы. Любой маркетолог подтвердит, что даже если фирме и удастся на некоторое время увеличить свою прибыль за счет нее, то на уважение к фирме со стороны клиентов все равно можно не рассчитывать, а значит, не стоит рассчитывать и на будущее фирмы. И действительно, спамом за рубежом обычно пользуются компании-однодневки, задача которых с минимальными затратами в минимальные сроки продать товары и пропасть. Помимо указанных последствий, опишем проблемы провайдеров. Во-первых, спам в больших объёмах загружает сети и коммуникационное оборудование. Во-вторых, при рассылке отправитель обычно не заботится о том, существуют ли реально все получатели, и сервер провайдера загружается ещё. Кроме того, может произойти переполнение почтовых ящиков.

В рамках концепции информационной безопасности применительно к данной проблеме выделим следующие классы мер защиты:

1. Нормативно-правовые или юридические.
2. Организационные или административные.
3. Программно-технические.

Юридические методы.

По эффективности это один из лучших методов защиты от спама – действия спамера носят противозаконный характер, и он подвергается преследованию со стороны закона.

Здесь очень важны следующие аспекты:

- проработка законодательной базы по терминологии, ответственности и механизмам исполнительной власти;
- развитые и отработанные механизмы исполнительной власти;
- координация действий с иностранными службами контроля.

К сожалению, в России до сих пор не создана эффективная законодательная база.

Организационные методы.

Эти методы наиболее просты. Рассмотрим элементарные правила, которые каждый должен соблюдать, чтобы не попасть в спамерские базы электронных адресов:

1. Беречь основной электронный адрес, полученный у провайдера. Сообщать о нем только надежным друзьям и партнерам. При этом напоминать им, чтобы ваш адрес не передавали третьим лицам.
2. При выборе имени почтового ящика придерживаться следующих правил (аналогично созданию стойкого пароля): чем длиннее имя, тем лучше (некоторые программы перебирают адреса по алфавиту - чем больше букв, тем лучше); использовать символы нескольких алфавитов (цифры, английские, знаки).
3. Для второстепенных задач заводить дополнительные адреса на бесплатных почтовых серверах, которые потом будет не жалко ликвидировать. Для сообщений в конференциях, форумах, на досках объявлений пользоваться только второстепенным адресом. С осторожностью относиться к различным розыгрышам, лотереям и призам.

4. Если где-нибудь при регистрации требуют подробные данные: пол, возраст, увлечения, годовой доход и т.п., то с большой вероятностью это сбор данных для последующей продажи спамерам. Дело в том, что такие расширенные базы данных стоят весьма дорого.

5. Для владельцев интернет-ресурсов: не оставляйте свой адрес на главной странице сайта, для контакта с посетителями сделайте отдельную страницу, можно использовать изображение адреса.

Программно-технические методы.

К ним относятся фильтры и электронные марки.

Фильтр – это возможность различать по критериям получаемые письма за счёт настройки почтовых программ и ящиков.

Метод «возвратных электронных почтовых марок» заключается в том, что к каждому сообщению электронной почты от неизвестного для вас адресата прилагается электронная «почтовая марка» как своеобразный залог того, что отправитель не является спамером. Если получатель такого письма считает, что только что полученное им сообщение не является спамом, эта марка возвращается им к отправителю. В противоположном же случае, если, по мнению получателя, сообщение является спамом или другим видом нежелательной корреспонденции, эта марка остается у него.

Представители компьютерной индустрии призывают законодателей активизировать международные усилия по борьбе со спамом – массовой несанкционированной рассылкой электронных писем. По словам Энрике Сейлема, президента компании Brightmail (Brightmail специализируется на средствах фильтрации спама в сетях интернет-провайдеров), спам сегодня составляет 46% в общем объеме трафика электронной почты. (доля спама от общего числа почтовых сообщений в 2001 году составляла всего 7%). По оценке Сейлема, в год спам наносит только американскому бизнесу ущерб в размере 10 млрд. долларов.

В Российской Федерации пока не возникло сбалансированного и адекватного проблеме подхода к разработке специальных норм, регулирующих массовые почтовые рассылки. В ряде предлагаемых за последние два года законопроектов, связанных с регулированием сети интернет и электронной коммерции, существуют различные варианты подходов регулирования рассылок и получения незапрошенной информации.

В России, помимо неопределенности в законодательном регулировании, практически отсутствует и предметная судебная практика, связанная со спамом, и поэтому в текущей ситуации, когда есть реальная необходимость налагать ограничения на спам, по возможности не нарушая прав при этом и спамеров, и пользователей сети, представляется целесообразным, в первую очередь, сосредоточиться на экономических средствах воздействия на явление спама, что должно найти отражение в действиях операторов связи, их экономической политике и договорной базе.

Тем не менее, многие интернет-провайдеры и почтовые сервера имеют достаточно эффективные средства и механизмы анализа, выявления и уничтожения спама.

Подводя итог, отметим, спам является результатом неконтролируемой и непредсказуемо развивающейся глобальной сети.

Эффективные средства со спамом давно известны – необходимо просто сделать его экономически невыгодным и проблема исчезнет. Но проблема заключается именно в том, что нет возможности воплотить это в жизнь – сети стали практически неконтролируемы.

Тем не менее, эта проблема может быть решена в результате контроля сетей, как глобального, так и местного масштаба. Правда, это затронет свободы и права человека, поэтому имеет смысл искать компромисс между контролем и свободой воли.