УДК 681.3:621.391

А.И. Баранчиков, Е.А. Баранчикова

НЕГАТИВНОЕ ВЛИЯНИЕ «СПАМА» НА РАБОТУ МАЛЫХ ИНФОРМАЦИОННЫХ СИСТЕМ И ОСНОВНЫЕ МЕТОДЫ БОРЬБЫ С НИМ

Рассматривается негативное влияние «спама» на современные информационные системы в условиях малых предприятий, связанное с их особенностями и ограниченными ресурсами, выделяемыми на борьбу с ним. Проведена оценка потерь предприятия, вызванных получением «спама». Кратко охарактеризованы и предложены основные методы борьбы со «спамом», позволяющие снизить потери предприятия. Показан выигрыш, связанный с реализацией предложенных мер.

Стабильное функционирование современных информационных систем (ИС) на предприятиях различных форм и назначений является одним их необходимых условий успешной работы данного предприятия. Поэтому присущая для всех ИС проблема – уязвимость – заставляет уделять особое внимание их защите от различного рода воздействий, способных привести к нарушениям конфиденциальности, целостности или доступности информации, а также работы самой ИС или к финансовым потерям предприятия [1]. Данное обстоятельство наиболее актуально для малых предприятий, т.к. даже самые небольшие финансовые потери в условиях жесткого ограничения денежных ресурсов могут привести к негативным последствиям.

В данной статье рассмотрим актуальную на сегодняшний день для многих предприятий малого бизнеса, работа которых тесно связана с сетью Internet и электронной почтой, угрозу информационной безопасности и финансовой стабильности предприятия – «спам».

Само это понятие можно определить следующим образом: «спам» – любая информация, полученная предприятием без явного на то запроса и приводящая к увеличению трафика и уменьшению пропускной способности каналов, а также увеличивающая время обработки корреспонденции и поиска нужной информации.

Основными неблагоприятными факторами при большом количестве «спама» являются:

1) оплата лишнего трафика;

2) уменьшение производительности труда вследствие следующих причин:

– увеличивается время, необходимое на обработку пользователем корреспонденции, объем которой возрастает (дополнительно к основному требуется время на просмотр и удаление «спама»);

– увеличивается вероятность того, что нужная информация может быть не найдена, т.к. на обработку корреспонденции отводится определенное время, а часть его будет затрачена на отсев «спама»;

– уменьшается быстродействие работы почтового клиента. Так, время отклика почтового клиента The Bat 3.8 на действия пользователя при достижении файла, содержащего письма, размера в 1 Гб увеличивается практически в 2 – 3 раза в зависимости от аппаратного обеспечения. При дальнейшем увеличении файла возможны сбои в работе почтового клиента, вплоть до зависания всей системы и невозможности открытия почтовой программой файла с письмами.

3) потери нужной информации из-за переполнения почтового ящика не сервере, происходящие из-за того, что новые письма не могут быть получены в связи с недостатком дискового пространства, в результате чего сервер выдает отправителю сообщение об ошибке;

4) получение вирусов, часто содержащихся в теле «спам»-писем, приводящее к сбоям в информационной системе и потерям нужной информации.

Зависимость времени обработки «спама» от его количества носит нелинейный характер и при большем количестве «спама» и малых аппаратных ресурсах может носить лавинообразный характер. Данная функция имеет следующий вид:

$$T(n) = k_1 n + \frac{k_1 k_2 n}{100} = k_1 n\left(1 + \frac{k_2}{100}\right), \qquad (1)$$

где n - количество писем «спама»;

k_1 - количество времени, затрачиваемого на обработку одного письма, примем $k_1 = 0{,}015$ часа;

k_2 - показывает на сколько % увеличивается время, затраченное на обработку одного письма, из-за увеличения времени отклика почтового клиента при увеличении количества писем.

Коэффициент k_2 определяется следующим образом.

Так как время отклика программы зависит от количества обрабатываемых писем, предположим, что в самом простом виде имеется линейная зависимость $k_2 = k_3 n$, где k_3 - коэффициент, подбираемый экспериментальным путем, в зависимости от почтового клиента, операционной системы (ОС) и аппаратной части. Примем $k_3 = 0{,}01$ (для почтового клиента The Bat 3.8, ОС Windows 2000, компьютер: процессор 1000 MHz, оперативная память 256 Мб).

Окончательно получим:

$$T(n) = k_1 n + \frac{k_1 k_3 n^2}{100} = \\ = k_1\left(n + \frac{k_3}{100} n^2\right) = 0{,}015\left(n + 10^{-4} n^2\right). \quad (2)$$

Так как при определенном уровне потерь дальнейшее функционирование системы будет нерентабельным, произведем суммарную оценку потерь предприятия из-за наличия «спама», при этом будем учитывать следующие наиболее вероятные потери:

1) оплата лишнего трафика;

2) уменьшение производительности труда за счет времени, потраченного на обработку «спама», и за счет уменьшения быстродействия почтового клиента.

$$P(n_1) = (k_1 n_1 z + k_1 \frac{k_3}{100} n_1 (n_1 + n_2) z + \\ + k_4 c n_1) * 20, \quad (3)$$

где $P(n_1)$ - потери предприятия, связанные с получением «спама», в течение календарного месяца;

n_1 - среднее количество писем «спама», получаемое за сутки;

n_2 - среднее количество писем, содержащих полезную информацию, получаемое за сутки;

k_4 - средний размер письма «спама», примем k_4 =0,1 Мб (данные получены на основе выборки о 1000 писем со «спамом»);

c - стоимость трафика за 1 Мб данных, примем с=3 руб (на основе данных о средней стоимости 1 Мб по г. Рязани);

z - зарплата сотрудника, занимающегося обработкой корреспонденции (руб/час).

Примем z=37 р/час, n_2 =700 и построим график функции $P(n_1)$ (см. рисунок 1).

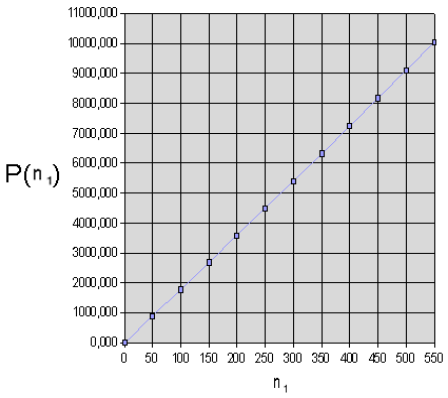

Рисунок 1 – Потери предприятия за месяц, при получении n_1 писем «спама» ежедневно

Исходя из экспериментально полученных данных, на примере работы туристической фирмы имеем число писем «спама» n_1 =550 шт. без применения какой-либо фильтрации. В итоге ежемесячные потери предприятия, связанные только с получением «спама», $P(n_1) = 10350$ руб.

Данная ситуация усугубляется еще и тем фактом, что поток «спама» растет с каждым днем за счет того, что с течением времени почтовый адрес предприятия становится известным все большему числу людей в результате распространения рекламной информации. Также людьми, рассылающими «спам» (далее – «спамерами»), постоянно производятся сканирование электронных страниц, обмен адресами между самими «спамерами». В итоге, если не принять своевременных мер, то убытки от получения «спама» могут быть весьма существенными для малого предприятия и, как крайний случай, может возникнуть вопрос о его рентабельности.

За последние годы было изобретено немало способов борьбы. К сожалению, «спамеры» отслеживают действия фильтров и изобретают все новые приемы для их обхода. К тому же нередко фильтрация спама приносит больше вреда, чем пользы: вместе с назойливой рекламой не доходят до адресата и важные деловые или личные сообщения[2].

Опишем наиболее известные и часто применяющиеся методы борьбы с нежелательными почтовыми сообщениями. В основном они базируются на стандартах ISO, касающихся электронной почты [3]:

1) проверка домена, с которого направлена почта, на существование. Почтовый сервер производит проверку, существует ли сервер, с которого пришло письмо, или нет. Если такой сервер не существует, пришедшие с него письма классифицируются как СПАМ;

2) проверка соответствия сетевого узла, который передал почту на соответствие MX-записям DNS;

3) проверка адреса назначения электронного письма. В случае, если адрес получателя электронного письма отсутствует в соответствующем поле, письмо классифицируется как СПАМ.

Этих мер часто бывает недостаточно. Фактически идет интеллектуальная борьба администраторов почтовых серверов и злоумышленников.

Проведенные эксперименты показывают, что таким образом отсеивается порядка 40 % «спама». На нашем примере – это приблизительно 215 писем в день удаляется автоматически сервером при попытке доставки. В итоге получаем выигрыш в размере 4100 рублей.

Среди дополнительных методов, находящихся в распоряжении системных администраторов, нужно отметить следующие:

1) использование открытых интернет-серверов черных списков доменов недоброжелателей;

2) использование локальных черных списков доменов;

3) использование численных СИИ (spamAssassin и пр.);

4) использование символьных СИИ (sendmail).

Методы, использующие черные списки, хороши тем, что отсекают определенный список доменов или адресов, однако эти методы недостаточно гибки.

Использование численных СИИ является эффективным методом, однако обладает следующим недостатком: существует (хотя и малая) вероятность «ложного срабатывания», в результате которого ожидаемая почта может быть не доставлена, а отфильтрована как «спам».

Наиболее перспективным методом является использование символьных (дедуктивных) СИИ. Этот процесс представляет собой сложную задачу, но в то же время вероятность «ложной тревоги» зависит только от мастерства администратора и может быть сведена к минимуму.

В итоге комплексное поэтапное использование всех вышеперечисленных методов позволяет значительно уменьшить потери предприятия, связанные с получением «спама», и повысить его рентабельность.

Библиографический список

1. *Якубайтис Э.А.* Открытые информационные сети. – М.: Радио и связь, 1991. – 197 с.

2. *Гуров В.В.* Интернет для бизнеса. – М.: Электроинформ, 1997. – 224 с.

3. *Альбитц П., Ли К.* – DNS и BIND. 4-е издание. – Спб:Символ-Плюс, 2002. – 696 с.