

А.И. Афонин  
ВРЕД КАК ОДНО ИЗ ПОСЛЕДСТВИЙ СПАМИНГА

Одной из специфических характеристик спаминага является распространение незапрошенной адресатом информации. Это может сопровождаться наступлением ряда негативных последствий в виде вреда, причиненного имущественным, информационным, личным и др. правам субъектов сервиса электронной почты. В общем случае можно выделить: материальный (прямой и косвенный) и нематериальный вред.

Для описания материального вреда удобно воспользоваться понятием совокупной стоимости владения (*Total Cost of Ownership, TCO*) информационных систем. Согласно определению консалтинговой корпорации Gartner Group - признанного мирового лидера в области независимой аналитики информационных технологий, *совокупная стоимость владения* - это полностью учтенные ежегодные расходы предприятия, связанные с приобретением и, что особенно важно, использованием информационных технологий в предметной деятельности.

В структуре затрат можно выделить прямые и косвенные затраты на противодействие спаминагу и устранение последствий его воздействия. Эти затраты можно рассматривать как вред (ущерб), наносимый спаминагом. В свою очередь, в структуре ущерба можно выделить прямой и косвенный материальный ущерб.

На этапе создания информационной системы (сервиса электронной почты) прямой ущерб может быть понесен в связи с необходимостью осуществления фиксированных затрат:

1. На привлечение внешних консультантов в рамках разработки проекта информационной системы. Расходы в данном случае производятся на этапе решения задачи создания защищенного от спама сервиса электронной почты.

2. На закупку аппаратного и лицензионного антиспамингового программного обеспечения.

3. На внедрение проекта.

На этапе эксплуатации сервиса электронной почты адресаты несут текущие прямые и косвенные затраты. Прямой ущерб включает затраты на обновление и модернизацию системы информационной безопасности (антиспаминговый модуль) и непосредственные убытки денежных средств (вынужденные затраты на оплату операторам связи времени, требуемого для приема спама). К этой же категории ущерба можно отнести редко учитываемые расходы на: управление системой, обучение персонала и техническую поддержку пользователей.

Значительная часть расходов приходится на долю так называемых

косвенных расходов. Ежедневные поступления сотен спам-сообщений вынуждают адресатов электронной почты тратить значительное время на чтение и удаление спама. Так, по оценке MessageLabs, эти процедуры требуют до 10 % рабочего времени пользователей.

Относительно небольшие потери, причиняемые спамом отдельному получателю, в масштабе крупной организации становятся достаточно высокими и составляют от \$50 до \$200 в год в расчете на одного офисного сотрудника.

Кроме того, в контексте приема и обработки спама методика Gartner Group учитывает следующие составные части этого вклада:

- время, затрачиваемое IT-персоналом на решение проблем пользователей, связанных с получением спама;
- время, затрачиваемое пользователями на самообразование и взаимопомощь вместо обращения в службу поддержки;
- время, затрачиваемое пользователями в связи с неоптимальными приемами работы;
- расходы, связанные с утратой критически важных данных (в связи с вирусной атакой, аппаратным или программным сбоем или случайно удаленные);
- расход времени на запланированные простои (модернизация оборудования, сети, обновление программного обеспечения);
- расход времени на незапланированные простои (по техническим причинам, из-за вирусных атак, в связи с использованием устаревшей техники и программного обеспечения).

Одна из самых серьезных проблем, связанных со спамингом, состоит в том, электронная почта представляет собой практически идеальную среду для переноса различного рода "опасных" вложений, а именно компьютерных вирусов, вредоносных программ, "троянских" программ и т.п. Вирусы, распространяемые путем спаминга, могут реализовывать весь спектр угроз информационной безопасности, а именно: угрозы нарушения целостности, конфиденциальности, доступа.

Спаминг, сопряженный с "засорением" почтовой системы, представляет пересылку в качестве вложений в электронных сообщениях файлов больших объемов или многократно заархивированных файлов. "Открытие" таких файлов или попытка "развернуть" архив может привести к "зависанию" системы. Следует отметить, что в этом случае получателю может быть нанесен ущерб даже одиночным спам-сообщением (не массовая рассылка).

Спаминг также, как правило, приводит к нарушению *личных немущественных прав* адресатов электронной почты.

1. Право на беспрепятственное получение информации. Данное пра-

во нарушается в результате переполнения почтовых ящиков спамом, и как следствие - потери оператором связи технической возможности принимать новые, в том числе полезные для пользователя ящика сообщения. Такого рода эффекты в сфере обеспечения информационной безопасности трактуются как реализация угрозы нарушения доступа (блокирование) к информации. В некоторых случаях блокирование информации ведет к такому виду ущерба, как упущенная выгода.

Здесь же следует отметить высокую вероятность случайного удаления релевантной информации, которое может произойти при разборе электронной почты. Угроза потери обусловлена естественными ошибками получателя, допускаемыми при семантическом анализе пакета поступивших сообщений, в котором спам может составлять до 90-95 %. Релевантное сообщение "теряется" и удаляется вместе со спамом.

2. Право на получение качественной информации. Иногда возможно поступление спама, который содержит релевантную для получателя, но не качественную (недобросовестную, недостоверную, заведомо ложную) информацию. Распространение такого рода информации: вводит адресатов в заблуждение; может нанести вред имущественным и неимущественным (например, здоровью) интересам получателей сообщений; как правило, служит для осуществления недобросовестных или незаконных целей создателя информации. Видимо, в таком контексте в некоторых случаях спаминг можно рассматривать как способ совершения мошенничества (в соответствии со ст. 159 УК РФ) .

3. Нарушение права получателей электронных сообщений на частную жизнь. Нарушение этого права возникает при поступлении незапрошенных сообщений: в виде политической рекламы; религиозного (например, привлечение к участию в сектах, фондах) и порнографического содержания; содержащих различного рода обращения и призывы (например, об оказании помощи, пожертвованиях, принятии участия в акциях и пр.). Такие спам-сообщения могут также посягать на общественные интересы, принципы гуманности и морали.

4. Нарушение права третьих лиц на личную тайну, честь, достоинство, деловую репутацию и пр. Перечисленные права субъектов информационных отношений нарушаются при распространении персональных данных третьих лиц, а также данных о них, не соответствующих действительности, в том числе задевающих честь, достоинство или порочащих деловую репутацию.

В результате спаминга может быть нарушено право операторов связи (ресурсы которых используются для рассылки спама) на свободное использование имущества (систем связи) для предпринимательской деятельности (ст. 34 Конституции РФ). Дело в том, что в 2003 году доля спама в

трафике электронных сообщений превысила 50 %. По сведениям ведущих провайдеров России, на начало 2004 года спам составил около 75-80 % всей входящей корреспонденции в публичных почтовых службах Рунета.

С точки зрения операторов связи, массовые отправления спам-сообщений создают бесполезную нагрузку на почтовые сервера, затрудняя тем самым работу информационных систем. Это, в свою очередь, влечет неоправданное увеличение затрат на модернизацию инфраструктуры сетей, а также увеличение численности обслуживающего персонала, рост нагрузки системных администраторов.