УДК 681.3

СИСТЕМА КЛАССИФИКАЦИИ ЭЛЕКТРОННЫХ СООБЩЕНИЙ

Никитин А.П.
Научный руководитель – к.т.н., доцент, Валеев С.С.
УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Рассматривается система распознавания спам-сообщений в потоке электронной почты.

Основные этапы работы системы: получение электронного сообщения, случайным образом выбираем некоторое количество слов, оцениваем принадлежность к спаму каждого из выбранных слов, оцениваем не легитимность всего письма.

Для классификации сообщений используется алгоритм Гари Робинсона на основе метода простой Байесовской классификации.

Из сообщений, поступающих на вход системы, выбираются атрибуты сообщения. Из этих атрибутов отбирается необходимая часть, которая и анализируется. Если сообщение достаточно велико, то атрибуты выбираются случайным образом, в противном случае анализируются все атрибуты. Это позволит достаточно точно и в тоже время быстро проводить классификацию. Для каждого атрибута оценивается вероятность того, что наличие атрибута указывает на спамность сообщения. Затем эта вероятность уточняется с целью уменьшения влияния атрибутов, о которых известно слишком мало. После подсчитывается количество атрибутов, указывающих на легитимность и на не легитимность сообщения, и вновь уточняются вероятности. Данная операция позволяет бороться с преднамеренным добавлением случайных слов. И, наконец, оценивается уровень легитимность сообщения.

Для уменьшения вычислительной нагрузки и вероятности ошибочной классификации сообщений применяются черные и белые списки электронных адресов. В черный список заносятся адреса спамеров, а в белый – адреса клиентов и партнеров. В последующем письма от отправителей из белого списка пропускаются без проверки, а письма от отправителей из белого списка удаляются в корзину. Затем атрибуты, извлеченные из писем пополняют базу знаний для повышения точности распознавания сообщений от неизвестных отправителей.

Для работы системы необходима база знаний, содержащая частоты встречаемости слов в легитимных и не легитимных сообщениях. База пополняется в процессе работы системы, что позволит адаптировать систему к конкретной предметной области. Первоначальное заполнение базы возможно на основе спам - сообщений, публикуемых на тематических сайтах в сети Интернет, и сообщений, самостоятельно классифицированных пользователем.

Система ориентированна на небольшие сети, не обладающие собственным почтовым сервером. Вся работа по классификации сообщений производиться на клиентских компьютерах. Атрибуты, впервые обнаруженные, а также электронные адреса спамеров, отсылаются на локальный сервер, где формируются и распространяются обновления для всех клиентов сети. Также доступно получение статистики, на основании чего возможно активное противодействие в форме блокировки получения писем или судебные иски.

В ходе работы был реализован действующий прототип системы классификации электронных сообщений. Основным фактором, влияющими на точность классификации, является количество атрибутов в базе знаний.