Н. Г. Ляпичева, О. М. Никонова (Москва, ЦЭМИ РАН, КАМС № 17. **Математико-статистический анализ объемов спама на узле ЦЭМИ РАН.**

«Каков бы ни был ресурс,
он всегда оказывается заполненным».
Закон Паркинсона

Специалисты по безопасности компьютерных сетей традиционно понимают под спамом незапрошенные коммерческие рекламные рассылки, отвечающие требованиям массовости и анонимности. С определенным основанием к спаму можно отнести почтовые сообщения, продуцированные почтовыми вирусами массовой рассылки.

В мире отчетливо прослеживается тенденция к увеличению процентного содержания спама (по отчету компании Barracuda Networks это 95% всей электронной почты в 2007 году). Одновременно с процентным происходит явное нарастание абсолютных величин и почтового трафика в целом, и спама в частности.

На рис. представлена диаграмма, отражающая почтовый трафик узла ЦЭМИ РАН через антивирусный шлюз (входящий в *сотнях писем*, исходящий в *письмах*). Период наблюдений 06.2007–08.2008

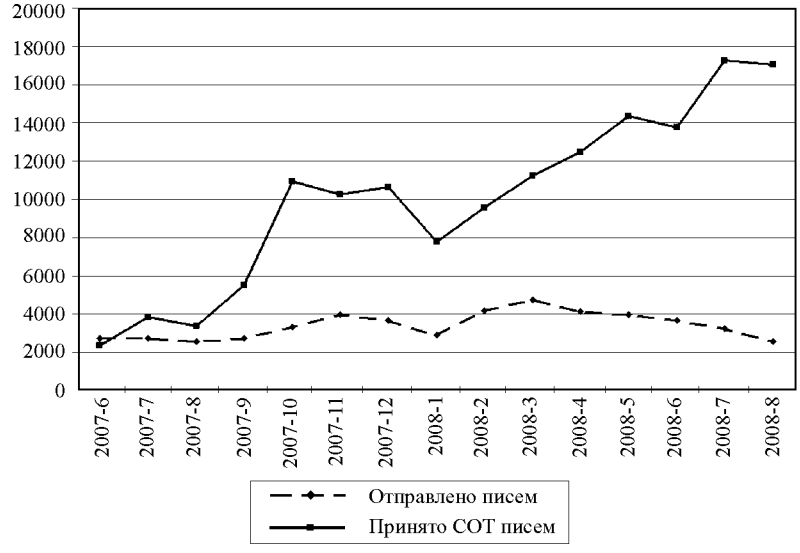

Рис. Входящий и исходящий почтовые трафики в ЦЭМИ РАН

К сожалению, панацеи против спама не существует. Вариативность заголовков и содержания, изменчивость формы, новые методы доставки не позволяют надолго перекрыть этот нарастающий поток. Однако, результат борьбы с почтовыми вирусами, происходящей в масштабах всего Интернета, отраженный в докладе [1] показывает, что при массовом внедрении антиспамовых средств на всех уровнях функционирования электронной почты может существенно уменьшить передаваемые объемы почтового трафика и повысить скорости прохождения почты. Простое возрастание вычислительных ресурсов, использующихся для обслуживания почтового сервиса, обычно приводит к соответствующему увеличению объемов спама.

Комплексные методы борьбы со спамом: антиспамовый шлюз, фильтры спама на клиентских почтовых программах и уничтожение спам-генераторов в ПК-«зомби» [2] позволили снизить объемы спама, исходящие с узла ЦЭМИ РАН.

СПИСОК ЛИТЕРАТУРЫ

1. Анализ вирусной активности в почтовом трафике на узле ЦЭМИ РАН. — Труды Третьей Всероссийской научно-практической конференции «Научное, экспертно-аналитическое и информационное обеспечение стратегического управления, разработки и реализации приоритетных национальных проектов и программ», 31 мая – 1 июня 2007 г. ИНИОН РАН, М.: 2007, с. 538–542. http://www.socionet.ru/publication.xml?h=repec:rus:ualhnv:inion2007-1
2. *Ляпичева Н. Г.* Обнаружение сетевых почтовых атак. — В сб.: Развитие и использование средств сетевого мониторинга и аудита./ Под ред. А. М. Терентьева. М.: ЦЭМИ РАН, 2005, в. 2, с. 28–39. http://www.socionet.ru/publication.xml?h=repec: rus:fmibxo:tom2-03