Н. Г. Ляпичева, **О. М. Никонова** (Москва, ЦЭМИ РАН). **Проблемы DNS-сервиса и их роль в борьбе со спамом.**

Атаки на DNS-сервис являются неотъемлемой частью успешной массированной рассылки спама. Варианты развития массированной рассылки зависят от возможностей спам-агента, внедренного в действующую сеть. Это может быть DoS-атака (Denial of Service) на DNS-сервер с последующей подменой поддельными пакетами ответов на запросы почтового сервера, либо отравление кэша (cache poisoning) фальшивыми записями, с той же целью повышения легитимности источников спама. Современный уровень индустрии спама включает в себя не только бот-сети распространения, но и поддельный DNS-сервис, обслуживающий эти цели.

Основные методы повышения надежности DNS-сервиса широко известны [1]: функциональное разделение на общедоступные и внутренние; ограничение передачи зон; защита от внешнего воздействия. И в дополнение — мониторинг сетевой обстановки и целостности хостов, содержащих DNS-серверы.

Отдельной проблемой Рунет обзавелся в прошлом, 2010 г. — Рунет получил новый домен в кириллическом отображении: «.рф». Итоги годичного развития данного домена сильно разнятся для существующих групп участников использования этого сетевого достижения. Не касаясь процессов коммерческих и организационных, которые были разработаны довольно удобно, можно обсудить вопрос реального использования этого (и подобных) многоязычных доменных имен, входящих в систему IDN (International Domain Names).

DNS-сервис Интернета в основном готов к использованию многоязычных доменных имен, уже 8-я версия сервера BIND поддерживает использование нелатинских имен, оформленных в символьной кодировке Punycode (например, кириллическое имя цэми-ран.рф отображается в виде XN----8SBWPIQ2B6C.XN--P1AI). Преобразование реализовано в 9-й версии в виде отдельного приложения (10-я версия в процессе разработки, пробный вариант ожидается в 2012 г. [2]).

Основная проблема состоит в неготовности части интернет-приложений работать с кириллическими именами, конкретно — отображать исходный облик доменного имени. Веб-браузеры (последних версий) давно справляются с соответствующим отображением [3]. Почтовый сервис в транспортной части использует закодированные адреса, что не вызывает проблем. Клиентские приложения в основном испытывают трудность использования кириллических почтовых адресов и их преобразования в Punycode (даже такой сервис, как mail.ru, не воспринимает кириллические адреса).

Широта использования кириллических почтовых адресов будет зависеть от насыщения почтовых клиентов расширениями (add-on), предназначенными для преобразования и отображения доменных имен. Одновременно следует ожидать появления уязвимостей и их использования для рассылки нелегитимной почты.

СПИСОК ЛИТЕРАТУРЫ

1. *Барнетт М.* Защищайте серверы DNS. http://cpi-it.ru/zaschischayte-serveryi-dns.html.
2. BIND 10. http://bind10.isc.org/wiki.
3. *Сидоров В.* Ну, здравствуй, кириллический домен .РФ! http://netler.ru/ikt/domain-rf.htm.