

СИСТЕМА УЧЕТА И КОНТРОЛЯ ИНТЕРНЕТ-ТРАФИКА В СРЕДЕ LINUX

А.В.Гребенюк, М.С.Бабий

Существует несколько подходов к организации процесса контроля и учета Интернет-трафика. Наиболее популярной является реализация на основе счетчиков файрвола с использованием скриптов, которые заносят данные счетчиков в СУБД и запускают необходимые правила файрвола. Еще одной популярной реализацией является установка прокси-сервера Squid с использованием анализатора, заносящего данные в СУБД в режиме реального времени. Оба решения требуют выполнения большого количества операций на малых интервалах времени и приводят к непропорциональному увеличению затрат времени и ресурсов относительно увеличения количества пользователей.

Цель работы заключалась в построении системы учета Интернет-трафика с более точным учетом количества передаваемой информации и с улучшенными временными характеристиками.

В процессе работы построена подсистема анализа трафика напрямую на основе информации о сетевых пакетах, без необходимости обработки отчетов работы сторонних программ. Для эффективного хранения и поиска информации о пользователях системы в оперативной памяти спроектирована структура данных, представляющая собой AVL-дерево.

Разработанная система обладает низкой латентностью (своевременный отклик и реакция на действие пользователя) и масштабируемостью (адекватное увеличение потребляемых ресурсов при увеличении количества пользователей). Обеспечена возможность хранения резервной копии информации о пользователях в базе данных SQL-сервера MySQL.

Система построена на основе модели клиент-сервер, что дает возможность расширять набор клиентских сервисов.