ИСПОЛЬЗОВАНИЕ ОБФУСКАЦИИ ПАКЕТОВ ДЛЯ СОКРЫТИЯ МЕТАДАННЫХ ТРАФИКА

П.С. Федорцов

Обфускация типа трафика – сокрытие сетевого протокола, используемого при обмене между двумя или более конечными узлами. Интерес к технологии маскировки метаданных трафика при помощи обфускации стал проявляться в ответ на широкое распространение технологии глубокого анализа пакетов (DPI) для активного мониторинга трафика, отправляемого приложениями. DPI, в отличие от традиционных брандмауэров, позволяет анализировать не только заголовки, но и содержимое пакетов. Также для фильтрации трафика при помощи DPI учитываются косвенные признаки, присущие каким-то определенным сетевым программам и протоколам. Для этого может использоваться статистический анализ (например, статистический анализ частоты встречи определенных символов, длины пакета и т. д.).

Обфускация направлена на разрушение этих статистических характеристик. Известны два подхода к обфускации: рандомизация характеристик и маскировка под известные сетевые протоколы. Рандомизация характеристик обычно заключается разбиении данных на пакеты случайного размера и отправки их со случайными интервалами. Такой подход проще в реализации и требует меньше вычислительных ресурсов. В результате невозможно установить принадлежность соединения какому-либо известному протоколу. При маскировке под известный сетевой протокол передаваемая информация таким образом, что ее сложно отличить от той, что обычно передается с использованием выбранного протокола. Также имитируются его статистические характеристики. Такой подход требует больших вычислительных ресурсов, но при этом сложнее обнаружить факт использования обфускации.