УДК 004.048

ИЗВЛЕЧЕНИЕ ИНФОРМАТИВНЫХ ПРИЗНАКОВ СЕТЕВОГО ТРАФИКА ПРИ ЕГО ОБРАБОТКЕ С ПОМОЩЬЮ МИКРОСХЕМ ПРОГРАММИРУЕМОЙ ЛОГИКИ

Горошков В.А. (Национальный исследовательский университет ИТМО),
Научный руководитель – к.т.н., доцент Кузнецов А.Ю.
(Национальный исследовательский университет ИТМО)

В работе проведено определение набора информативных признаков сетевого трафика и алгоритмов их извлечения, реализация которых возможна с применением ресурсов микросхем программируемой логики.

Обнаружение вредоносной активности в современных вычислительных сетях требует проведения анализа сетевого трафика, передаваемого с помощью современных высокоскоростных интерфейсов. Обработка значительного потока сетевого трафика связана со значительным ростом вычислительной нагрузки на хост-систему, что может привести к снижению ее производительности при выполнении целевых приложений.

В работе предложен способ извлечения информативных признаков пакетов сетевого трафика, реализацию которого возможно включить в состав процесса обработки сетевого трафика с использованием ресурсов микросхем программируемой логики. Определен набор информативных признаков, дополняющий базовые поля пакета сетевого уровня информацией о поведенческих особенностях потоков сетевого трафика и углубленным разбором маркеров известных сетевых протоколов.

Реализация предложенного решения позволит включить сбор информативных признаков пакетов сетевого трафика в состав операций, выполняемых средствами сетевого адаптера с минимальным задействованием ресурсов хост-системы.

Горошков В.А. (автор) Подпись

Кузнецов А.Ю. (научный руководитель) Подпись