М. М. Гишкелюк
(*ГрГУ им. Я. Купалы, Гродно*)

ИССЛЕДОВАНИЕ СОВРЕМЕННЫХ ПРОГРАММ ДЛЯ АНАЛИЗА СЕТЕВОГО ТРАФИКА

В связи с развитием новых сетевых технологий, их внедрением и эксплуатацией, а также появлением внушительного количества новых сетевых протоколов прикладного уровня, все большую актуальность получает анализ сетевого трафика.

Целью работы было провести исследование и классификацию инструментов анализа трафика и выяснить, какие задачи анализа сетевого трафика способны решать такие инструменты, выявить их возможности, достоинства и недостатки с точки зрения функциональности и удобства использования.

Традиционным методом решения описанной выше задачи является проведение ряда испытаний для каждого из инструментов, при обеспечении одинакового потока трафика на сетевом интерфейсе.
На основании проведенных исследований были сделаны выводы, что оптимальным инструментом среди свободно распространяемых стал Wireshark. Он является кроссплатформенным, поддерживает анализ и идентификацию более 1000 сетевых протоколов, предоставляет пользователю графический интерфейс.

При рассмотрении коммерческих инструментов лидером стал ClearSight Analyzer. Основные его преимущества перед конкурентами: поддержка большего количества сетевых протоколов, гибкая си-

стема уведомлений с возможностью запуска собственных скриптов, поддержка высокоскоростных сетей, удобный графический интерфейс. В то же время цена продукта ClearSight Analyzer – около 6000 Евро. Ни один из рассмотренных инструментов не предоставляет удобного интерфейса для работы с результатами анализа туннелированного трафика.

На основе полученных данных, целью дальнейшей работы является разработка авторского программного обеспечения для анализа сетевого трафика, сочетающего в себе все преимущества рассмотренных инструментов, распространяемого по демократичной цене.