# АЛГОРИТМ ОБНАРУЖЕНИЯ DDOS-АТАК НА ОСНОВЕ СТАТИСТИЧЕСКОГО АНАЛИЗА ТРАФИКА

Д.Н. Одинец, В.В. Носков

*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Республика Беларусь*

Алгоритм анализирует информацию о характеристиках заголовка трафика [1], чтобы обнаружить вредоносное ПО DDoS-атаки с подменой IP. Его этапами являются извлечение, анализ и обнаружение аномальных пакетов. На первом этапе на основе анализа пакетов коммутатора уровня 3 создается таблица T1 путем извлечения информации о функциях, включая IP-адрес и MAC-адрес заголовков Ethernet, текущее время, временной интервал.

На втором этапе вычисляются статистические характеристики (частоты встречаемости). для обнаружения вредоносных программ DDoS-атак с подменой IP. На третьем этапе извлеченные IP-адреса и MAC-адреса из заголовков Ethernet трафика в режиме реального времени сравниваются с атрибутивной информацией, представленной в таблице T1, чтобы определить, произошло ли заражение DDoS-атак с подменой IP-адресов вредоносным ПО. Если есть совпадение между IP-адресами и MAC-адресами трафика в реальном времени со значениями свойств в T1, делается вывод о вероятном заражении DDoS-атаки с подменой IP-адресов вредоносными программами. В результате исследований получены графические зависимости времени обнаружения DDoS-атаки с подменой IP от входных параметров.

**Список литературы**

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. СПб: Питер, 2006. 957 с.