АДАПТИВНЫЙ АЛГОРИТМ ОБНАРУЖЕНИЯ СЕТЕВЫХ КИБЕРАТАК

к.т.н., доц. Н.А. Маслова, магистр С.А. Жаданов, Донецкий национальный технический университет, Институт информатики и искусственного интеллекта, г. Донецк

Одной из самых сложных задач в сфере защиты компьютерных систем является предотвращение DDoS-атак. В настоящее время способов, гарантирующих полную защиту от DDoS-атак не существует и основная причина этого – развитие компьютерных систем, увеличение количества пользователей сети интернет, постоянное совершенствование методов, которыми пользуются киберпреступники. Поэтому алгоритмы и методы диагностики и предотвращения кибератак указанного типа являются актуальными.

Целью работы является исследование алгоритмов и методов диагностики сетевых атак на основе анализа сетевого трафика и данных о состоянии информационной среды; разработка требований к построению адаптивного алгоритма обнаружения атак.

Наиболее эффективное средство предотвращения ущерба, наносимого DDoS-атаками – их своевременное обнаружение. Предпринимаемые меры безопасности должны работать в режиме реального времени, учитывать состояние компьютерной системы, оперативно реагировать на постоянно меняющиеся схемы проведения атак. Одним из путей решения этой задачи является применение адаптивных алгоритмов.

Адаптивный алгоритм основывается на мониторинге получаемых пакетов, анализе трафика сети и контроле информационной среды. Он обладает комбинированной настройкой, основанной на данных мониторинга загрузки конкретного сервиса с учетом его нагрузок в штатном режиме работы.

Использование принципов адаптации и совместный анализ состояния информационной среды и поступающего трафика характеризуют новизну работы. Разработка может быть использована организациями, чьи сотрудники имеют доступ к сети Интернет, фирмами, предоставляющими услуги хостинга, владельцами сайтов и облачных сервисов.