УДК 004.7

ДЕТЕКТИРОВАНИЕ DOS АТАК НА ПРИКЛАДНОМ УРОВНЕ В МОДЕЛИ "ИЗДАТЕЛЬ-ПОДПИСЧИК"

Дикий Д.И. (Университет ИТМО)
Научный руководитель – д.т.н., доцент Гришенцев А.Ю.
(Университет ИТО)

Аннотация

Новые информационные технологии порождают новые риски и угрозы информационной безопасности. Одной из таких технологий является информационно-центрические сети и частная их реализация в виде модели «издатель-подписчик». В данном исследовании рассмотрены проблемы детектирования DoS атак в таких сетях.

Введение. Новые информационные технологии порождают новые риски и угрозы информационной безопасности. Одной из таких технологий является информационно-центрические сети и частная их реализация в виде модели «издатель-подписчик». Цель применения данной модели заключается в сокращении объемов передаваемой информации, рассылаемой одновременно группе получателей.

Основная часть. Был произведен анализ модели «издатель-подписчик», в ходе которого было выявлена предрасположенность к реализации атаки вида отказ в обслуживании. Для подтверждения опасности угрозы была собрана экспериментальная установка, на которой удалось успешно провести атаку при выполнении некоторых условий. Для детектирования данного типа атак с учетом специфики модели «издатель-подписчик» предложен алгоритм, с применением методов машинного обучения, который способен установить источник атаки: участок сети, скомпроментированная учетная запись или взломанное устройство.

Выводы. В ходе проведения исследования установлен наиболее успешно справляющийся с задачей обнаружения атаки метод классификации сетевого трафика методами машинного обучения. Использование этого метода классификации в структуре разработанного алгоритма позволило достичь значений F1-меры более 0.95.