УДК 004.85:004.852

ИССЛЕДОВАНИЕ МЕТОДОВ КЛАССИФИКАЦИИ И РАЗРАБОТКА МОДЕЛИ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ФИЛЬТРАЦИИ СЕТЕВОГО ТРАФИКА.

Автор - **Галанцев Олег Евгеньевич (Университет ИТМО)**

Научный руководитель - к.т.н. **Грудинин Владимир Алексеевич**

Введение. В настоящие время задача классификации сетевого трафика играет ключевую роль в области сетевой безопасности, поскольку позволяет определить тип и структуру приложения, которое является его источником. Системы классификации сетевого трафика используются в множестве сетевых функций: управление сетью, обеспечению качества связи (QoS, QoE), выполнение политик информационной безопасности и разработке систем мониторинга, обеспечивающих контроль, диагностику состояния сети, выявления сетевых проблем и аномалий. При решении задач классификации сетевого трафика существует широкий спектр традиционных методов классификации (например, по номерам портов, на основе полезной нагрузки DPI, Deep Packet Inspection), однако они обладают рядом существенных недостатков, именно с этим связан активный рост исследований в этом направлении. На данный момент наиболее перспективным подходом является применение технологии машинного обучения (МО, англ.ML, Machine Learning), используемых в различных исследованиях и получивших эффективные результаты точности.

Цель работы. Целью данной работы является исследование применения различных классификаторов машинного обучения для выполнения сравнительного анализа при решении задач классификации сетевого трафика и разработка собственной модели МО для решения задачи фильтрации сетевого трафика с целью безопасности.

Основной результат. В работе произведён обзор использования средств МО для классификации сетевого трафика и определены основные тенденции развития такого подхода. На основе построенной модели МО произведен экспериментальный сравнительный анализ различных классификаторов машинного обучения: метод опорных векторов (SVM), дерево принятия решений (Decision tree cl.), наивный Байесовский (Naïve Bayes) классификатор и классификатор на основе логистической регрессии (LR cl.).

Автор _____ О.Е. Галанцев

Научный руководитель _____ В. А. Грудинин