БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра математического моделирования и анализа данных

Аннотация к магистерской диссертации

«Обнаружение аномалий в сетевом трафике с помощью методов машинного обучения»

Сафиуллин Тулеубай Тулеубаевич

Научный руководитель – кандидат физ.-мат. наук,
доцент Абрамович М. С.

Минск, 2024

Реферат

Магистерская диссертация, 64 стр., 7 рис., 6 табл., 14 источников, 1 приложение.

Ключевые слова: ВЫЯВЛЕНИЕ АНОМАЛИЙ, СЕТЕВОЙ ТРАФИК, МАШИННОЕ ОБУЧЕНИЕ, НЕЙРОННЫЕ СЕТИ.

Объект исследования – Сетевой трафик.

Цель работы – Выявление аномалий в сетевом трафике с использованием методов машинного обучения и нейронных сетей.

Методы проведения работы – Использовались нейронные сети с прямой связью, рекуррентные нейронные сети, длинные цепи элементов краткосрочной памяти, классические методы машинного обучения и методы ансамблей моделей.

Результаты – Обнаружено, что нейронные сети проявляют высокую эффективность в выявлении аномалий. Также выявлено, что методы ансамблей моделей способны дополнить и улучшить результаты отдельных моделей.

Область применения – Результаты могут быть использованы для разработки надежных систем обнаружения и предотвращения кибератак, использоваться в учебном процессе при преподавании учебных дисциплин, связанных с машинным обучением и компьютерными сетями.

Abstract

Master thesis, 64 p., 7 figures, 6 tables, 14 sources, 1 appendix.

Keywords: ANOMALY DETECTION, NETWORK TRAFFIC, MACHINE LEARNING, NEURAL NETWORKS.

Object of research – The self-similarity of network traffic. In particular, the possibility of modeling network traffic using stable distribution is being investigated.

Purpose of the work - Identification of anomalies in network traffic using machine learning and neural networks.

Methods – Feedforward neural networks, recurrent neural networks, long short-term memory network, classical machine learning methods and model ensemble methods were used.

Results – It is found that neural networks exhibit high efficiency in anomaly detection. It is also found that model ensemble methods can complement and improve the results of individual models.