

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Факультет прикладной математики и информатики
Кафедра математического моделирования и анализа данных

Аннотация к дипломной работе

“Методы машинного обучения для обнаружения аномального сетевого трафика”

Кахановский Максим Викторович

Научный руководитель — кандидат физико-математических наук, доцент
кафедры математического моделирования и анализа данных Абрамович М. С.

Минск, 2024

РЕФЕРАТ

Дипломная работа: 30 страниц, 2 рисунка, 14 таблиц, 21 формула, 14 источников.

Ключевые слова: МАШИННОЕ ОБУЧЕНИЕ, ЗАДАЧА КЛАССИФИКАЦИИ, СЕТЕВОЙ ТРАФИК, ОБУЧЕНИЕ С УЧИТЕЛЕМ, IDS.

Объект исследования: методы машинного обучения, применяемые для выявления аномалий в сетевом трафике, алгоритмы, используемые для анализа и классификации сетевых данных.

Цель работы: разработка системы, способной автоматически выявлять аномалии в сетевом трафике с использованием методов машинного обучения.

Методы исследования: а) теоретические: изучение литературы, посвящённой методам классификации, способы оценки результатов.

б) практические: применение изученных алгоритмов на данных NSL-KDD, написание программы для классификации данных на основе предложенных методов.

Результат: разработана программа, которая по данным NSL-KDD классифицирует записи на аномальный и нормальный трафик, используя рассмотренные методы.

Область применения: системы обнаружения вторжений (IDS), мониторинг сетевой безопасности в корпоративных сетях, выявление мошеннической активности в банковских системах.

ABSTRACT

Diploma thesis: 30 pages, 2 images, 14 tables, 21 formulas, 14 sources

Keywords: MACHINE LEARNING, CLASSIFICATION TASK, NETWORK TRAFFIC, SUPERVISED LEARNING, IDS.

Object of study: machine learning methods applied to anomaly detection in network traffic, algorithms used for analysis and classification of network data.

Purpose of work: development of a system capable of automatically detecting anomalies in network traffic using machine learning methods.

Research methods: a) theoretical: literature review on classification methods and result evaluation techniques.

b) practical: application of studied algorithms on NSL-KDD data, writing a program for data classification based on proposed methods.

Result: a program that classifies records into anomalous and normal traffic using the NSL-KDD data and the studied methods was developed.

Scope: intrusion detection systems (IDS), network security monitoring in corporate networks, detecting fraudulent activity in banking systems.