

ABSTRACT

The explanatory note consists of 119 pages, includes 11 illustrations, 11 tables, 6 appendices, and 22 references.

Relevance of the topic. With the increasing volume of network traffic and the growing number of cyber threats, it is crucial to employ modern approaches for data analysis. Decision Support Systems (DSS) are particularly effective in accelerating data processing and enabling well-informed decisions. The use of machine learning algorithms and neural networks allows for the detection of hidden patterns and anomalies in traffic in real time, significantly aiding rapid responses to cyber threats.

Objective of the research. The main goal is to improve the efficiency of anomaly detection in network traffic through the development of software utilizing machine learning algorithms and neural networks.

Object of research: analysis of anomalies in network traffic.

Subject of research: methods, algorithms, and neural networks for detecting anomalies in network traffic.

To achieve this goal, the following tasks were formulated:

- Analysis of anomaly detection tools;
- Development of anomaly detection tools;
- Design of the software;
- Development of the software;
- Testing the solution.

Scientific novelty. The scientific novelty of the master's thesis lies in improving methods for detecting anomalies in network traffic.

Practical significance. The practical significance of the obtained results is that the anomaly detection software for network traffic can assist system administrators in making appropriate decisions.

Connection with scientific programs, plans, and topics. The work was carried out at the Department of Informatics and Software Engineering of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute."

Keywords: NETWORK TRAFFIC, NEURAL NETWORKS.