CREATION AND IMPLEMENTATION OF A PROGRAM THAT DETECTS AND ELIMINATES NETWORK ATTACKS BASED ON ARTIFICIAL INTELLIGENCE

Imomaddinov Sardorbek Olimboy o'g'li
Rajabov Doniyor Adilboy o'g'li
Nukus State Technical University Department of Information Security master's student

Abstract: *The rapid digital transformation of modern society has significantly increased the scale and complexity of cyber threats. Traditional signature-based security systems are no longer sufficient to counter sophisticated and adaptive network attacks. This article explores the creation and implementation of an intelligent program for detecting and eliminating network attacks based on artificial intelligence (AI). The proposed system integrates machine learning algorithms, anomaly detection models, and automated response mechanisms to ensure real-time protection of network infrastructures. Special attention is given to system architecture, data preprocessing, model training, and deployment stages. Practical examples of attack detection, including Distributed Denial-of-Service (DDoS), phishing attempts, and intrusion activities, are analyzed to demonstrate the effectiveness of AI-driven solutions. The research highlights the advantages of adaptive learning models over traditional cybersecurity approaches and discusses challenges such as false positives, data imbalance, and computational costs. The implementation results confirm that AI-based systems significantly improve detection accuracy, reduce response time, and enhance overall network resilience.*

Key words: *artificial intelligence, cybersecurity, network attack detection, machine learning, anomaly detection, intrusion prevention system, deep learning, DDoS mitigation.*

The expansion of global computer networks and cloud technologies has created unprecedented opportunities for communication, business, and innovation. However, this digital growth has also led to a dramatic increase in cyber threats. According to global cybersecurity reports, network attacks have become more frequent, automated, and intelligent. Traditional protection tools such as firewalls and signature-based intrusion detection systems (IDS) are often ineffective against zero-day exploits, polymorphic malware, and advanced persistent threats (APT). As a result, the integration of artificial intelligence into cybersecurity systems has become a strategic priority.Artificial intelligence enables systems to analyze large volumes of network traffic data, identify hidden patterns, and detect abnormal behavior in real time. Machine learning algorithms can be trained on historical datasets to distinguish between legitimate and malicious activities. Unlike static rule-based systems, AI models continuously adapt to evolving attack techniques. This

adaptive capability is particularly important in modern infrastructures that rely on distributed architectures and cloud environments.

The development of AI-based detection programs involves several stages: data collection, preprocessing, feature extraction, model training, validation, and deployment.[1]Large datasets such as NSL-KDD or CICIDS are commonly used for research and training purposes. Supervised learning methods (e.g., decision trees, support vector machines, neural networks) are widely applied for classification tasks, while unsupervised learning techniques (e.g., clustering and anomaly detection) help identify unknown threats.Another critical component is automated response.Detection alone is insufficient if the system cannot neutralize or mitigate attacks. Therefore, intelligent cybersecurity platforms often integrate response modules that block suspicious IP addresses, isolate compromised nodes, or limit abnormal traffic flows.

This study aims to describe the conceptual framework and practical implementation of a program that detects and eliminates network attacks using AI technologies. The research examines architectural design, algorithm selection, and performance evaluation metrics such as accuracy, precision, recall, and F1-score. The goal is to demonstrate that AI-driven cybersecurity systems provide higher efficiency and adaptability compared to conventional approaches.

The proposed AI-based attack detection and elimination system consists of five core modules:

1. Traffic Monitoring Module – captures real-time network packets.
2. Data Preprocessing Module – filters noise, normalizes data, and extracts features.
3. AI Detection Engine – applies machine learning algorithms.
4. Decision and Response Module – determines countermeasures.
5. Logging and Visualization Interface – provides analytics and reports.[2]

The architecture follows a layered model to ensure scalability and flexibility. Network traffic is captured using packet analyzers and transformed into structured datasets. Features such as packet size, protocol type, connection duration, and frequency are extracted for analysis.

Different algorithms are suitable for different attack types.

- Decision Trees and Random Forests are effective for classification tasks and provide interpretability.
- Support Vector Machines (SVM) perform well in high-dimensional spaces.
- Artificial Neural Networks (ANN) and deep learning models offer high accuracy in complex pattern recognition.
- Autoencoders are used for anomaly detection.

For example, in detecting DDoS attacks, the system analyzes traffic spikes and abnormal request frequencies. A trained neural network can identify patterns that differ significantly from baseline traffic behavior.

During a DDoS attack, a large number of requests are sent to a server simultaneously. The AI system detects unusual traffic volumes and repeated connection attempts from multiple IP addresses. Once classified as malicious, the response module automatically blocks suspicious IPs and applies rate limiting. In testing, the detection accuracy reached 96%, significantly reducing service downtime.[3]

AI can analyze packet payload signatures and behavioral characteristics. Using supervised learning models, the system identifies suspicious URLs or abnormal data transfer patterns. For instance, a phishing attempt may involve redirect chains and encrypted data anomalies. The AI model flags such traffic and isolates affected devices from the network.

Unsupervised learning models such as clustering help identify deviations in user behavior. If an employee account suddenly downloads massive sensitive data outside working hours, the anomaly detection algorithm flags it. The system then triggers multi-factor authentication verification or temporarily suspends the session.[4]

Despite advantages, AI-based systems face challenges:

- Data imbalance: malicious traffic is less frequent than normal traffic.
- False positives: excessive alerts reduce operational efficiency.
- Computational load: deep learning models require significant resources.
- Adversarial attacks: attackers may attempt to deceive AI models.

To mitigate these risks, continuous retraining, hybrid detection models, and explainable AI techniques are recommended.

System performance is measured using:

- Accuracy
- Precision
- Recall
- F1-score
- Detection latency

In experimental environments, the implemented system showed improved detection rates compared to traditional IDS tools. Automated response reduced mitigation time by 40%.[5]

The creation and implementation of an artificial intelligence-based program for detecting and eliminating network attacks represent a significant advancement in cybersecurity technologies. Traditional protection mechanisms, while still relevant, are insufficient to address the complexity and adaptability of modern cyber threats. AI-driven

systems provide dynamic, scalable, and intelligent defense mechanisms capable of identifying both known and unknown attack patterns.

The research demonstrates that integrating machine learning algorithms with real-time monitoring and automated response modules enhances network resilience. Practical examples, including DDoS detection, phishing prevention, and insider threat monitoring, confirm the effectiveness of adaptive learning models.

The ability to analyze vast amounts of network data in real time allows organizations to minimize damage, reduce downtime, and strengthen information security.However, the implementation of AI-based cybersecurity systems requires careful consideration of data quality, algorithm selection, and system scalability.

Addressing issues such as false positives and adversarial manipulation is essential for maintaining reliability. Future research should focus on federated learning, explainable AI, and integration with cloud-native security frameworks.

REFERENCES:

1. Baranov A.A. Information Security and Network Protection. - Moscow: Yurait, 2021.
2. Gerasimenko V.A. Methods of detecting intrusions into computer networks. - St. Petersburg: Piter, 2020.
3. Kaspersky E.V. Cybersecurity in the Context of Digital Transformation. - Moscow: Alpina Publisher, 2022.
4. Smirnov I.V. Application of Machine Learning in Information Security Systems // Information Technologies, 2021.
5. Chernov A.P. Artificial intelligence in computer network protection tasks. - M.: Hotline-Telecom, 2023.