УДК 004.056.53

AI-Based Solutions for Enhancing Corporate Network Security

Мусса Х.И. (ИТМО)
Научный руководитель – кандидат технических наук, доцент Заколдаев Д. А.
(ИТМО)

Introduction. In today's interconnected world, corporate networks are under constant threat from sophisticated cyberattacks targeting sensitive user data. Traditional security measures often fail to detect novel attack vectors, highlighting the need for advanced solutions. AI-based systems, leveraging machine learning (ML) and deep learning (DL), offer real-time threat detection and adaptive defense mechanisms. These technologies have gained significant attention in recent years, with numerous studies demonstrating their potential to enhance cybersecurity. For instance,[1] showcased the effectiveness of unsupervised ML for anomaly detection in network traffic, achieving 92% accuracy. Similarly,[2]proposed a machine learning approach to anomaly detection based on traffic monitoring for secure blockchain networking, highlighting the potential of ML in enhancing network security. This study evaluates AI models for securing corporate networks, focusing on their accuracy, efficiency, and practical implementation.

Main Part. The study proposes hybrid AI models to detect cyber threats effectively. Supervised methods, such as Support Vector Machines (SVM) and Random Forest (RF), classify network traffic as benign or malicious with high accuracy, up to 95.2%. These models are highly effective but require labeled data for training. Unsupervised methods, including K-means clustering and autoencoders, detect anomalies without labeled data, achieving accuracies of 89.5% and 90.3%, respectively. However, they have higher false positive rates (11%). An optimal solution is a hybrid approach, combining SVM with autoencoders, to reduce dependency on labeled data while maintaining accuracy. The research emphasizes the importance of using modern datasets, such as CICIDS2017, to adapt models to new attack types and improve their effectiveness in real-world scenarios. Additionally, the study explores the application of deep learning architectures, such as Convolutional Neural Networks (CNNs) and transformers, to further enhance threat detection capabilities. The integration of explainable AI (XAI) techniques, such as SHAP and LIME, is also proposed to provide interpretable decisions and improve model transparency.

Conclusions. The study confirms the potential of AI to significantly enhance corporate network security. Practical implementation involves integrating these AI models with Security Information and Event Management (SIEM) systems, such as Splunk, and ensuring compliance with regulations like GDPR. Testing on edge devices is recommended to achieve low-latency threat detection. Future work should focus on incorporating deep learning architectures, such as Convolutional Neural Networks (CNNs) and transformers, and developing explainable AI (XAI) techniques to provide interpretable decisions and improve model transparency.

References

1. Vikram A., Mohana. Anomaly detection in Network Traffic Using Unsupervised Machine learning Approach // 2020 5th International Conference on Communication and Electronics Systems (ICCES). IEEE, 2020. P. 476–479.
2. Kim J. et al. A Machine Learning Approach to Anomaly Detection Based on Traffic Monitoring for Secure Blockchain Networking // IEEE Transactions on Network and Service Management. 2022. Vol. 19, № 3. P. 3619–3632.