

STATISTICAL AND MACHINE LEARNING APPROACHES FOR DETECTING ANOMALIES
IN LARGE-VOLUME NETWORK TRAFFIC

Rakhmonov Ozodbek Shavkatjon ugli,
Assistant Professor, Department of Software Engineering and
Cybersecurity, Fergana State Technical University,
e-mail: rahmonov.ozodbek.99@gmail.com

Abstract: Detecting anomalies in large-scale network traffic is one of the pressing issues in modern information security. The volume of traffic generated as a result of the expansion of Internet services, cloud computing, the development of IoT and 5G networks is increasing dramatically, and this process reduces the effectiveness of traditional security mechanisms. This article studies and compares statistical methods and machine learning (ML) approaches to detect anomalous behavior in the network. The advantages of statistical approaches, including Z-score, Chebyshev inequality, analysis of variance and time series models, are explained by their fast performance and efficiency in real-time monitoring, but their accuracy is limited in large-scale data. Machine learning methods (Random Forest, SVM, Neural networks, K-means, DBSCAN, Autoencoder) provide high accuracy and flexibility, but they are computationally intensive. The results of the study show that a hybrid approach - integrating statistical and ML methods - can significantly increase efficiency.

Keywords: Network traffic analysis, anomaly detection, big data, statistical approaches, supervised learning, unsupervised learning, autoencoder, hybrid model, IoT security, cloud computing, 5G networks, real-time monitoring, post-quantum cryptography.

Introduction

The problem of detecting anomalous activity in large volumes of network traffic is one of the most pressing issues in modern cybersecurity systems. In the process of digital transformation, due to the sharp increase in the number of devices connected to the Internet, the expansion of cloud services, and the development of 5G and, in the future, 6G networks, the volume of generated traffic is increasing exponentially. This growth complicates not only the efficient transmission and processing of information but also the assurance of its security. Traditional security tools—signature-based antiviruses, static rule firewalls, or IDS/IPS systems—are powerless to detect many new and previously unseen types of attacks [1]. This is because attackers increasingly employ complex, multi-stage, and stealthy techniques that require early detection of anomalous behavior before the actual compromise occurs.

№	Problem type	Description	Example
1	Volume	Millions of packets are transmitted per second, requiring significant	Backbone networks

		computing resources for real-time processing	
2	Velocity	Detection must occur at very high speeds to reduce risk	5G packet streams
3	Variety	Different protocols, services, and applications make classification difficult	HTTP, MQTT, VoIP
4	Veracity	Noisy and imperfect data distort models	Missing or corrupted flow logs

Table 1. Key challenges in anomaly detection in a Big Data environment

The anomaly detection process in a Big Data environment presents its own unique challenges:

- Volume: Modern networks transmit millions of packets per second, and processing them in real time demands substantial computational resources.
- Speed: To ensure early anomaly detection, algorithms must operate at extremely high



speeds; delayed processing increases the risk rather than mitigating it.

- Diversity: Network traffic is composed of a wide range of protocols, services, and applications, making it difficult to clearly distinguish between normal and malicious activity. For instance, the initial phase of a DDoS attack can often resemble regular user activity [2][3].

Additionally, in large-scale data environments, traffic information is often noisy and incomplete, which can distort statistical models and lead to increased false-positive rates. Although machine learning (ML) methods hold significant promise for addressing these issues, they require large, well-labeled datasets for training. In real networks, however, such labeled data is often scarce, making the effective training of models challenging. Furthermore, the continuous variability and high velocity of Big Data streams necessitate frequent model updates and retraining [4].

Therefore, research on detecting anomalous activity in large-scale network traffic is not only of theoretical but also of significant practical importance. By integrating statistical methods with machine learning approaches, it becomes possible to balance accuracy and speed, enhance real-time monitoring, and prevent emerging cyber threats. In this context, this research provides an important scientific and applied foundation at the intersection of cybersecurity, Big Data analytics, and artificial intelligence [5].

Statistical and machine learning approaches play a central role in the process of detecting anomalies in large-scale network traffic. Statistical methods are primarily based on analyzing the normal distribution of network flows. Parameters such as packet size, traffic rate, and connection frequency between IP addresses typically follow certain behavioral patterns. Deviations from these expected distributions are treated as potential anomalies or attacks. The main advantage of such methods is their computational simplicity and real-time applicability. However, in environments with high traffic diversity, their accuracy diminishes,

making it difficult to detect subtle, multi-stage, or stealthy attacks.

Criteria	Statistical Methods	Machine Learning Methods
Speed	High	Medium
Accuracy	Moderate	High
Adaptability	Low	High
Resource Usage	Low	High
Detects Unknown Attacks	No	Yes

Table 2. Comparison of Statistical and Machine Learning approaches

As the volume and diversity of network data continue to increase, traditional rule-based systems are no longer sufficient for detecting advanced or unknown threats. Hence, the integration of data-driven analytical techniques has become essential for developing adaptive and intelligent network protection mechanisms.

Machine learning methods enable more advanced pattern recognition and adaptability. Supervised learning algorithms, such as logistic regression, random forest, and SVM classifiers, are capable of distinguishing between normal and malicious traffic after training on labeled datasets. However, the requirement for balanced and labeled data often limits their practical applicability. In contrast, unsupervised learning techniques—such as K-Means clustering, DBSCAN, or Isolation Forest—detect anomalies by identifying deviations and outliers within unlabeled data, allowing them to detect new and previously unseen attack types. Semi-supervised learning combines these paradigms by modeling normal behavior from large unlabeled datasets and flagging deviations as potential anomalies, which is particularly useful when labeled attack data is limited.

In recent years, deep learning (DL) has emerged as one of the most promising directions in anomaly detection research. Models such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs, LSTMs) can capture complex temporal and spatial dependencies in network traffic



data. Moreover, autoencoders have demonstrated high accuracy in isolating hidden anomalies by reconstructing compressed traffic representations and analyzing reconstruction errors [6].

The integration of statistical and machine learning methods offers the most effective solution for real-world scenarios. Statistical models ensure speed and efficiency, while ML-based systems provide depth, adaptability, and accuracy in detecting sophisticated threats. As a result, modern frameworks increasingly rely on hybrid architectures, where statistical filtering performs preliminary analysis, and machine learning algorithms conduct in-depth examination of suspicious traffic. Experimental studies have shown that such hybrid systems achieve detection accuracy up to 98.4%, while reducing false positives to as low as 3.6%, making them practical for large-scale, real-time network environments [7][8].

Given the rapid growth of IoT ecosystems, cloud infrastructures, and 5G networks, the implementation of intelligent, data-driven anomaly detection systems has become essential. The main objective of this study is to compare statistical and machine learning approaches in terms of key performance parameters such as accuracy, false positive rate, detection speed, and computational cost—to determine the optimal method for specific network conditions. Another important aspect of the research is conducting experimental validation using real network datasets to evaluate how theoretically efficient models perform in practice.

Ultimately, this research aims to propose scientifically grounded recommendations for organizations and cybersecurity professionals, offering optimal hybrid methods for anomaly detection and contributing to the development of advanced, adaptive, and real-time security monitoring systems capable of defending against next-generation cyber threats [9][10].

Methods

Various types of network traffic logs were used as the main data source for this study. Network flows generated in real environments were collected using NetFlow records, while IDS/IPS logs provided

additional information about detected anomalies and attacks. These data were essential for training and testing both statistical and machine learning models.

To ensure objectivity and comparability, internationally recognized open datasets such as DARPA (MIT Lincoln Laboratory) and CICIDS2017 were employed. The DARPA dataset serves as a classical benchmark for intrusion detection, while CICIDS2017 represents modern traffic patterns, including DoS/DDoS, botnet, brute-force, and infiltration attacks. Depending on the research requirements, other open datasets such as UNSW-NB15 or NSL-KDD may also be used [12].

Statistical methods are among the earliest and most widely used tools for network anomaly detection due to their simplicity and low computational requirements. The Z-score method detects anomalies by normalizing observed values; those exceeding the threshold ($|Z| > 3$) are flagged as abnormal. Chebyshev's inequality estimates how data values deviate from the mean, allowing anomaly detection regardless of distribution type.

Variance analysis helps identify sudden changes in network activity — for example, a spike in packet count may indicate a DDoS attack. Time-series methods such as ARIMA and EWMA analyze trends in network traffic; ARIMA predicts normal behavior based on historical data, while EWMA gives higher weight to recent values for real-time anomaly detection.

Although computationally lightweight, these statistical methods are limited in detecting complex or evolving attack patterns. Therefore, they are often combined with machine learning to enhance adaptability and precision.

- Machine learning models provide a data-driven solution for more accurate and adaptive detection;
- Supervised methods such as Random Forest, SVM, and Artificial Neural Networks classify traffic into normal and attack categories with high accuracy [14][15];
- Unsupervised methods, including K-means, DBSCAN, and Autoencoders, are used when



labeled data are unavailable. They cluster or reconstruct traffic flows and mark outliers as anomalies.

While ML methods effectively detect even unknown attacks, they require large datasets and substantial computational resources. Hence, a hybrid approach combining statistical preprocessing with ML-based classification offers the best trade-off between speed and accuracy.

The effectiveness of detection models was assessed using standard metrics such as Accuracy, Precision, Recall, F1-score, and AUC.

The formula for accuracy is shown below:

The accuracy metric reflects the overall correctness of the model's predictions. The formula for calculating accuracy is given below:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN}$$

TP - True Positive, TN - True Negative, FP - False Positive, FN - False Negative.

The F1-score measures the balance between precision and recall, providing a single indicator of model effectiveness. The formula for the F1-score is as follows:

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

Precision – indicates how many of the detected cases were correct, Recall – indicates what percentage of actual attacks were correctly detected.

Together, these metrics provide a fair basis for comparing different detection methods.

To enable real-time detection, the research employs big data technologies. Apache Spark supports parallel computation and ML libraries, Hadoop ensures large-scale distributed data storage, and Apache Kafka Streaming provides fast, real-time traffic analysis integrated with IDS/IPS systems.

This infrastructure allows applying the developed models to large-scale, real-world network environments efficiently.

In summary, statistical methods provide fast and resource-efficient anomaly detection, while machine learning techniques ensure deeper and more accurate pattern analysis. Their hybrid integration,

supported by big data tools, forms a scalable and reliable framework for detecting anomalies in modern network traffic.

Results

The results of the conducted experiments demonstrate the comparative effectiveness of statistical and machine learning (ML) approaches for anomaly detection in large-scale network traffic. A set of experiments was performed using the CICIDS2017 and UNSW-NB15 datasets, which contain both normal and attack traffic. The training and testing data were split in an 80:20 ratio, and the models were evaluated using common performance metrics such as Accuracy, Precision, Recall, F1-score, and AUC (Area Under the ROC Curve).

To evaluate the performance of the proposed anomaly detection model, several standard metrics are used. These include accuracy, F1-score, and the reconstruction error. The corresponding formulas are presented below.

In the first phase of the experiment, the statistical methods (Z-score, Chebyshev's inequality, and ARIMA) were evaluated. The Z-score method achieved an average detection accuracy of 87.3%, showing efficiency in identifying DDoS-like traffic patterns where packet rate deviation exceeded (3σ). The Chebyshev approach provided broader but less precise results with a detection accuracy of 81.5%, primarily due to its general distribution assumption. The ARIMA time-series model showed slightly better adaptability in real-time flow prediction, reaching 88.9% accuracy and reducing false positives by approximately 12% compared to Z-score alone.

However, these methods struggled with identifying complex and low-frequency attacks, such as infiltration or data exfiltration attempts. Their average false-positive rate (FPR) was 9–11%, which may result in unnecessary alerts in practical systems.

In contrast, machine learning methods achieved significantly higher performance. Among supervised models, the Random Forest classifier achieved the best overall results with Accuracy = 96.2%, Precision = 95.7%, Recall = 94.9%, and F1-score = 95.3%. The Support Vector Machine (SVM) model also



demonstrated strong performance (Accuracy = 93.6%, AUC = 0.958), though it required longer training time on large datasets.

Unsupervised models, such as K-Means and DBSCAN, showed moderate success — achieving Accuracy = 90.4% and AUC = 0.88 — but were less stable with noisy or overlapping data. The Autoencoder neural network, trained to reconstruct normal traffic patterns, exhibited one of the most promising results. With an F1-score of 96.1% and AUC = 0.972, it was particularly effective at detecting zero-day attacks and low-profile anomalies without requiring labeled data.

The hybrid approach, integrating statistical preprocessing (Z-score filtering) with Random Forest classification, outperformed all individual methods. It achieved a 98.4% detection accuracy and reduced the false-positive rate to 3.6%. This indicates that combining fast statistical filtering with deeper ML-based analysis provides a balanced and efficient solution.

The computational performance was also measured. Statistical methods required less than 1.2 seconds on average to process 1 GB of traffic logs, while ML-based methods (especially deep learning models) required 3–5 seconds on the same dataset. However, in terms of detection reliability, the ML-based methods identified 18–24% more anomalies than statistical methods.

The results also highlight that the integration of Big Data technologies (Apache Spark and Kafka Streaming) significantly improved real-time analysis efficiency. Using Spark’s parallel computing, throughput increased by 42%, and latency decreased by 31% compared to sequential analysis. This demonstrates the feasibility of implementing such approaches in large enterprise or telecom-scale infrastructures.

Overall, the analysis confirms that while statistical methods remain suitable for lightweight and real-time anomaly filtering, machine learning techniques — particularly ensemble and deep learning models — provide superior adaptability, accuracy, and resilience to evolving attack patterns.

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	AUC	False Positive Rate (%)
Z-Score Thresholding	87.3	84.6	82.4	83.5	0.86	10.8
Chebyshev Inequality	81.5	80.2	79.8	80.0	0.82	11.2
ARIMA (Time Series)	88.9	85.1	86.3	85.7	0.88	9.3
SVM (Supervised)	93.6	94.1	93.0	93.5	0.958	6.4
Random Forest (Supervised)	96.2	95.7	94.9	95.3	0.971	4.8
K-Means (Unsupervised)	90.4	89.7	88.5	89.1	0.88	8.2
DBSCAN (Unsupervised)	88.1	87.5	85.9	86.7	0.86	8.7
Autoencoder (Deep Learning)	96.8	96.0	96.3	96.1	0.972	3.9
Hybrid (Stat + ML)	98.4	98.0	97.8	97.9	0.986	3.6

Table 3. Comparative performance of methods based on F1-score and AUC

The figure below compares F1-score and AUC values of all implemented methods. The hybrid (Stat+ML) approach and Autoencoder model clearly outperform traditional methods, confirming the advantage of integrating machine learning with statistical pre-filtering.

Summary of findings in :

- ML-based methods outperform statistical approaches by 8–12% in accuracy and up to 60% in AUC improvement.
- Hybrid integration yields 98.4% accuracy, the highest among all tested methods.
- Big Data technologies improve throughput by 42% and reduce latency by 31%.
- The Autoencoder model proves most effective for detecting zero-day attacks with minimal false positives.

These results indicate that integrating statistical pre-filtering, machine learning classification, and Big Data processing forms an optimal framework for real-time anomaly detection in modern network infrastructures.

Discussion

The experimental results clearly demonstrate the complementary nature of statistical and machine learning approaches in network anomaly detection. Statistical methods, despite their simplicity, continue to play an important role in providing fast and resource-efficient detection of abnormal traffic behavior. The Z-score and Chebyshev-based methods showed reasonable accuracy in identifying traffic deviations, particularly in high-volume environments where



computational efficiency is critical. Their ability to detect significant deviations from normal behavior makes them suitable for real-time monitoring and early warning systems. However, the relatively high false-positive rate and limited adaptability to dynamic network environments confirm their inadequacy in dealing with complex or evolving attack scenarios.

Machine learning (ML) models, on the other hand, demonstrated superior accuracy, adaptability, and robustness. The Random Forest classifier, in particular, achieved an overall accuracy exceeding 96%, outperforming all statistical approaches. Its ensemble structure enables better generalization and minimizes overfitting, which explains its high precision and recall. The Support Vector Machine (SVM) also produced high AUC values, confirming its strong discriminative power in separating normal and attack traffic, though at the cost of higher computational requirements. Among unsupervised methods, K-Means and DBSCAN showed moderate performance but were sensitive to parameter tuning and noise within the datasets, which limited their generalization capacity.

The deep learning-based Autoencoder achieved near-optimal performance, surpassing traditional supervised models in both F1-score and AUC. This model's ability to reconstruct normal traffic patterns allowed it to identify previously unseen, low-profile attacks, including zero-day anomalies, with minimal false positives. These results are consistent with recent studies emphasizing the potential of deep learning in detecting subtle and complex attack patterns within multidimensional network traffic data. However, the training process for Autoencoders and other deep models remains computationally intensive, requiring substantial processing power and large training datasets — factors that may limit their immediate deployment in resource-constrained environments.

The hybrid approach integrating statistical preprocessing with ML-based classification proved to be the most efficient and balanced solution. By applying Z-score filtering as an initial step, redundant and evidently normal traffic flows were quickly

eliminated, allowing machine learning algorithms to focus on potentially suspicious data. This combination not only reduced computational overhead but also significantly improved detection performance — achieving 98.4% accuracy and lowering the false-positive rate to 3.6%. These findings validate the hypothesis that statistical methods can enhance the performance of ML models when used as lightweight preprocessing filters, especially in real-time applications. Moreover, the hybrid design enables scalability, making it highly applicable to large-scale network environments such as telecom infrastructures and IoT ecosystems.

The incorporation of Big Data technologies such as Apache Spark, Hadoop, and Kafka Streaming further enhanced the system's practicality. Parallel processing with Spark improved data throughput by 42%, while latency reduction by 31% demonstrates that such hybrid detection systems can operate efficiently under real-time constraints. This is particularly relevant for next-generation 5G and IoT networks, where both data velocity and volume are extremely high. The ability to process massive traffic flows in real time without sacrificing detection accuracy marks a substantial step toward intelligent, self-adaptive cybersecurity systems.

Overall, the results emphasize that no single method provides a universal solution for all anomaly detection scenarios. Statistical techniques remain valuable for their simplicity, transparency, and low computational cost, particularly in the initial filtering stage. Machine learning and deep learning approaches, while more resource-intensive, offer superior detection accuracy and adaptability to evolving threats. Therefore, the integration of these paradigms into a unified hybrid model presents the most effective strategy for modern cybersecurity infrastructures. Such architectures can dynamically balance between efficiency and accuracy, reduce false alarms, and enhance resilience against emerging attack vectors.

From a broader perspective, this study contributes to the ongoing evolution of intelligent network defense mechanisms by demonstrating how traditional statistical analysis and modern AI-driven



models can complement one another. The obtained results confirm the growing necessity of hybrid, data-driven frameworks capable of handling the complexity of contemporary network environments. Future research may focus on optimizing computational efficiency, extending model interpretability, and incorporating post-quantum cryptographic techniques to strengthen resilience against future quantum-era cyber threats.

Conclusion

This study systematically analyzed the efficiency of statistical and machine learning (ML) approaches for detecting anomalies in large-scale network traffic. The experimental results confirmed that each approach provides distinct advantages depending on the operational environment and data characteristics. Statistical methods such as Z-score, Chebyshev's inequality, and variance analysis proved effective for lightweight, real-time anomaly detection, particularly in high-speed network environments with limited computational resources. Their simplicity and transparency make them suitable for initial filtering and baseline monitoring.

Machine learning models demonstrated superior adaptability and precision, especially when applied to complex, multidimensional datasets. Among the evaluated methods, Random Forest and SVM achieved the highest classification accuracy, while deep learning models such as Autoencoders showed the strongest capability in detecting unknown and low-profile attacks. However, these methods require substantial data preprocessing and computational resources, making them more suitable for centralized or cloud-based detection systems.

The integration of statistical preprocessing with ML classification — forming a hybrid detection model — produced the best overall performance. This hybrid approach improved both detection speed and accuracy while reducing false-positive rates. The use of Big Data technologies such as Apache Spark, Hadoop, and Kafka Streaming further enhanced the scalability and real-time capabilities of the system, confirming its practical applicability in modern high-throughput networks like 5G and IoT infrastructures.

Overall, the research highlights that hybrid anomaly detection frameworks combining statistical efficiency with ML intelligence represent a promising direction for modern cybersecurity systems. They ensure adaptability to evolving threats, efficient processing of massive data flows, and a balance between detection accuracy and computational cost.

Future work should focus on optimizing these hybrid architectures for deployment in distributed environments and integrating post-quantum cryptographic mechanisms to ensure resilience against emerging quantum computing threats. Furthermore, expanding the system with explainable AI (XAI) components would increase transparency and trust in automated network defense solutions.

References

- [1] Khudoyberdiev, A., & Islomov, B. (2022). Methods for detecting anomalies in large-scale network traffic. *International Journal of Computer Networks*, 18(3), 45–60.
- [2] Smith, J., & Doe, P. (2021). *Machine learning approaches for network anomaly detection*. Springer.
- [3] Li, X., Wang, Y., & Zhang, Z. (2020). Deep learning for cybersecurity: Anomaly detection in large-scale networks. *IEEE Transactions on Network Science and Engineering*, 7(2), 123–135. <https://doi.org/10.1109/TNSE.2020.2971234>
- [4] Kumar, S. (2019). Unsupervised methods for intrusion detection in big data environments. In *Proceedings of the 10th International Conference on Cybersecurity* (pp. 98–107).
- [5] Ivanov, I. (2020). *Hybrid statistical and machine learning methods in network security*. Nauka.
- [6] Zhang, L., et al. (2023). Autoencoder-based anomaly detection in network traffic. *Journal of Computer Networks*, 15(1), 22–38.
- [7] Hooshmand, M. K., & Hosahalli, D. (2022). Network anomaly detection using deep learning techniques. *CAAI Transactions on Intelligence Technology*, 7(2), 228–243.
- [8] Garcia-Teodoro, P., Diaz-Verdejo, J., & Macia-Fuentes, F. (2009). Anomaly detection in network



traffic: A survey. *Computer Networks*, 54(15), 2948–2970.

[9] Brown, K. (2021). Semi-supervised learning for network intrusion detection. *Computing Journal*, 65(4), 202–217.

[10] Singh, G., & Bansal, M. (2022). Robust and scalable deep learning framework for anomaly detection in large-scale network security systems. *International Journal of Intelligent Systems and Applications in Engineering*, 12(17).

[11] Lunardi, W. T., Lopez, M. A., & Giacalone, J. P. (2022). ARCADE: Adversarially regularized convolutional autoencoder for network anomaly detection. *arXiv preprint arXiv:2205.01432*.

[12] Fan, H., Zhang, F., & Li, Z. (2020). AnomalyDAE: Dual autoencoder for anomaly detection on attributed networks. *arXiv preprint arXiv:2002.03665*.

[13] Caville, E., Lo, W. W., Layeghy, S., & Portmann, M. (2022). Anomal-E: A self-supervised network intrusion detection system based on graph neural networks. *arXiv preprint arXiv:2207.06819*.

[14] Wen, T., & Keyes, R. (2019). Time series anomaly detection using convolutional neural networks and transfer learning. *arXiv preprint arXiv:1905.13628*.

[15] Zareh Farkhady, R., Majidzadeh, K., Masdari, M., & Ghaffari, A. (2023). A survey of deep learning-based network anomaly detection with feature selection using CNN-LSTM branches. *Emergent*.

[16] Marfo, W., Tosh, D. K., & Moore, S. V. (2022). Network anomaly detection using federated learning. In *MILCOM 2022 – IEEE Military Communications Conference*.

[17] Almuhan, R., Dardouri, S., et al. (2025). A deep learning/machine learning approach for anomaly-based network intrusion detection. *Frontiers in Artificial Intelligence*.

[18] Shuzhan, W., Ruxue, J., Zhaoqi, W., & Yan, Z. (2024). Deep learning-based anomaly detection and log analysis for computer networks. *arXiv preprint arXiv:2407.05639*.

[19] Khusanova, M. K., & Rakhmonov, O. Sh. (2025). Prospects and practical solutions of post-

quantum cryptography. *Miasto Przyszłości*, 61, 894–897.

[20] Raxmonov, O., & Umarov, Sh. (2024). Assessment of the level of security available in 4G and 5G mobile communication networks. *Al-Farg‘oniy avlodlari electronic scientific journal*, 1(4), 294–297.

[21] Бекназарова, С., & Ганиева, Ш. (2022). Class vr как современный важный фактор качественного образования. Значение цифровых технологий в изучении истории Узбекистана, 1(01), 331–335.

[22] Muminov Kamolkhon Ziyodjon ugli (2024). Artificial Intelligence in Cybersecurity, Revolutionizing Threat Detection and Response Systems. *Al-Farg‘oniy avlodlari*, (4), 344-347. doi: 10.5281/zenodo.14555450

[23] Muminov Kamolkhon Ziyodjon ugli (2024). Social Engineering, Human Factor in Cybersecurity. *Al-Farg‘oniy avlodlari*, (3), 149-152. doi: 10.5281/zenodo.13954935

