КОМПЬЮТЕРНЫЕ НАУКИ, ПРИБОСТРОЕНИЕ И АВТОМАТИЗАЦИЯ
КОМПЬЮТЕРЛІК ҒЫЛЫМДАР, АСПАП ЖАСАУ ЖӘНЕ АВТОМАТТАНДЫРУ
COMPUTER SCIENCE, INSTRUMENTATION AND AUTOMATION

UDC 004.855
IRSTI 28.23.01
https://doi.org/10.53364/24138614_2025_38_3_9

G. Dzhsupbekova[1], G. Ordabayeva[2*], A. Beketova[2], G. Baispay[2]

[1]M. Auezov South Kazakhstan State University, Shymkent,160019, Kazakhstan
[2]Kazakh National University named after Al-Farabi, Almaty; 050038; Kazakhstan

[*]*E-mail: ordabayeva.gulzinat@kaznu.kz*

APPLYING ARTIFICIAL INTELLIGENCE METHODS TO DETECT NETWORK TRAFFIC ANOMALIES

Abstract. *The development of information technology continues to highlight the importance of ensuring the security of information resources. The increasing number of various types of information threats complicates the detection of attacks. The objective of the study is to apply artificial intelligence methods for attack detection while minimizing the number of traffic features to achieve the required detection quality. To train AI, it is necessary to create a high-quality dataset that allows for the accurate identification of attack features in network traffic. The proposed approach uses AI trained on the UNSW-NB 15 dataset, which includes nine types of network attacks: Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms. For implementation, Python is used with the Pytorch and Pandas libraries for data processing. An analysis of the software module's performance was conducted, along with the application of binary evaluation methods such as the Kappa Coefficient and the Jaccard Index. The effectiveness of the proposed AI model is evaluated using classification metrics: Accuracy, Precision, Recall, and F1 Score. Testing of the developed model with different sets of features revealed that the model achieves high-quality prediction of anomalous traffic when using five selected features. The performance of the AI model was assessed using the Kappa Coefficient and the Jaccard Index. Effective classification thresholds were calculated based on the results, improving the quality of anomalous traffic prediction. The evaluation results show that the developed model, trained on the UNSW-NB 15 dataset, can accurately detect traffic anomalies, thereby contributing to the information security of information resources.*

Keywords: *network traffic, artificial intelligence, neural networks, attack detection, dataset, UNSW-NB, Kappa Coefficient, Jaccard Index.*

Introduction

The application of information technologies is growing at a rapid pace today. This digital transformation has led to a range of security issues. According to data from the State Technical Service for the first quarter of the current year, over 16 million cyberattacks were blocked using the Unified Internet Access Gateway (UIAG). Among the identified cases of malware distribution, a total of 9,586 instances were registered and processed, with 2,795 in January, 1,317 in February, and 5,474 in March [1].

Gartner has released a new report on technologies used in everyday information security practices, showing that ITDR (Identity Threat Detection and Response) has reached the peak of inflated expectations in the Hype Cycle for Security Operations, 2024 [2].

According to data from Positive Technologies, the number of incidents increased by 7% in the first quarter of 2024 compared to the previous quarter. One of the most common outcomes of successful cyberattacks was the leakage of confidential information, which accounted for 72% of incidents involving individuals and 54% involving organizations. Additionally, cybersecurity researchers from Secure Works observed a rise in domains registered with keywords related to obituaries. Cybercriminals used artificially generated obituaries to attract potential victims. Their targets included compromising the personal data of website visitors, stealing money under the guise of donations for fictitious causes, and infecting devices with malware [3].

All these incidents are linked to the fact that modern attack scenarios are characterized by high complexity, multi-stage processes, and automation. Attackers possess advanced technical skills and actively employ artificial intelligence methods. The increasing frequency of attacks necessitates a reassessment of protection strategies and the adoption of cutting-edge technologies for network traffic analysis during the early stages of developing security solutions.

Materials and Methods.

Analyze the dataset

Analyzing network traffic for threat and anomaly detection requires processing large volumes of data in real-time. One approach to addressing this challenge is the use of Artificial Intelligence (AI). The network should incorporate various types of AI and be pre-trained for the system's operation. These conditions will help mitigate the complexities associated with applying AI for attack recognition in network traffic [4].

The paper aims to apply artificial intelligence methods for detecting attacks while minimizing the number of traffic features to achieve the desired detection quality. To achieve this goal, the following tasks need to be addressed: 1. Analyze the UNSW-NB 15 dataset [5] to identify the most significant features that will aid in detecting anomalous traffic associated with various attacks; 2. Determine the model parameters for constructing a neural network in accordance with the selected training methodology and prepare the necessary software; 3. Test the developed anomaly detection module for different sets of input features; 4. Evaluate the performance of the software module, considering effective threshold selection and applying binary evaluation methods such as the Kappa coefficient and the Jaccard index.

For training and testing the developed neural network model, the UNSW-NB 15 dataset was used, which is freely accessible [5]. UNSW-NB 15 is a dataset of network traffic created using the IXIA PerfectStorm tool in the Cyber Range laboratory of the Australian Centre for Cyber Security (ACCS). This dataset includes both normal traffic and traffic associated with one of nine types of network attacks: Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms. The dataset contains separate training and testing sets in *.csv format, with 171,716 and 82,331 records, respectively. For the classification task, a combined dataset was created from the original training and testing sets, containing a total of 254,047 records. A snippet of the UNSW-NB 15 dataset is shown in Figure 1.

	id	dur	proto	service	state	spkts	dpkts	sbytes	dbytes	rate	sttl	dttl	sload	dload	sloss	dloss	sinpkt	dinpkt	sjit	djit	swin	stcpb	dtcpb	dwin	tcprtt	synack	ack
0	1	0.000011	udp	-	INT	2	0	496	0	90909.09020	254	0	1.803636e+08	0.0	0	0	0.011	0.0	0.0	0.0	0	0	0	0	0.0	0.0	
1	2	0.000008	udp	-	INT	2	0	1762	0	125000.00030	254	0	8.810000e+08	0.0	0	0	0.008	0.0	0.0	0.0	0	0	0	0	0.0	0.0	
2	3	0.000005	udp	-	INT	2	0	1068	0	200000.00510	254	0	8.544000e+08	0.0	0	0	0.005	0.0	0.0	0.0	0	0	0	0	0.0	0.0	
3	4	0.000006	udp	-	INT	2	0	900	0	166666.66080	254	0	6.000000e+08	0.0	0	0	0.006	0.0	0.0	0.0	0	0	0	0	0.0	0.0	
4	5	0.000010	udp	-	INT	2	0	2126	0	100000.00250	254	0	8.504000e+08	0.0	0	0	0.010	0.0	0.0	0.0	0	0	0	0	0.0	0.0	
5	6	0.000003	udp	-	INT	2	0	784	0	333333.32150	254	0	1.045333e+09	0.0	0	0	0.003	0.0	0.0	0.0	0	0	0	0	0.0	0.0	
6	7	0.000006	udp	-	INT	2	0	1960	0	166666.66080	254	0	1.306667e+09	0.0	0	0	0.006	0.0	0.0	0.0	0	0	0	0	0.0	0.0	
7	8	0.000028	udp	-	INT	2	0	1384	0	35714.28522	254	0	1.977143e+08	0.0	0	0	0.028	0.0	0.0	0.0	0	0	0	0	0.0	0.0	
8	9	0.000000	arp	-	INT	1	0	46	0	0.00000	0	0	0.000000e+00	0.0	0	0	60000.688	0.0	0.0	0.0	0	0	0	0	0.0	0.0	
9	10	0.000000	arp	-	INT	1	0	46	0	0.00000	0	0	0.000000e+00	0.0	0	0	60000.712	0.0	0.0	0.0	0	0	0	0	0.0	0.0	

Figure 1 – The source dataset UNSW-NB 15

The UNSW-NB 15 dataset includes both numerical and categorical values. For the neural network to function properly, all features must be represented in numerical format. Feature selection, which is crucial for the binary classification task, plays a key role in ensuring the performance and accuracy of the traffic anomaly detection model [6]. The UNSW-NB 15 dataset contains 40 features, some of which are irrelevant, weakly correlated, or partially redundant, potentially impacting the quality of the traffic anomaly detection model. To identify the most informative features, a correlation matrix (Figure 2) was constructed based on Pearson correlation coefficients [7], using the training dataset. The Pearson correlation coefficient is calculated as the ratio of the covariance of two variables to the product of their standard deviations, where covariance is defined as the expected value of the product of deviations of the variables from their mean values (1).

$$r_{xy} = \frac{cov(x,y)}{\sqrt{s_x^2 s_y^2}} = \frac{\sum_{i=1}^{m}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum_{i=1}^{m}(x_i-\bar{x})^2 \sum_{i=1}^{m}(y_i-\bar{y})^2}}, \quad (1)$$

where $\bar{x}, \bar{y}$ - are the mean values of the vectors x and y; s_x^2, s_y^2 - are the variances of the vectors x and y.

The correlation coefficient can range from -1 to 1. The greater the absolute value of the coefficient, the stronger the correlation between the variables. A value close to 0 indicates a weak correlation. If the correlation coefficient is between 0 and 1, it signifies a positive correlation, whereas a value between -1 and 0 indicates a negative correlation. A value of 1 means a perfect positive correlation between two variables, -1 indicates a perfect negative correlation, and 0 denotes no correlation.

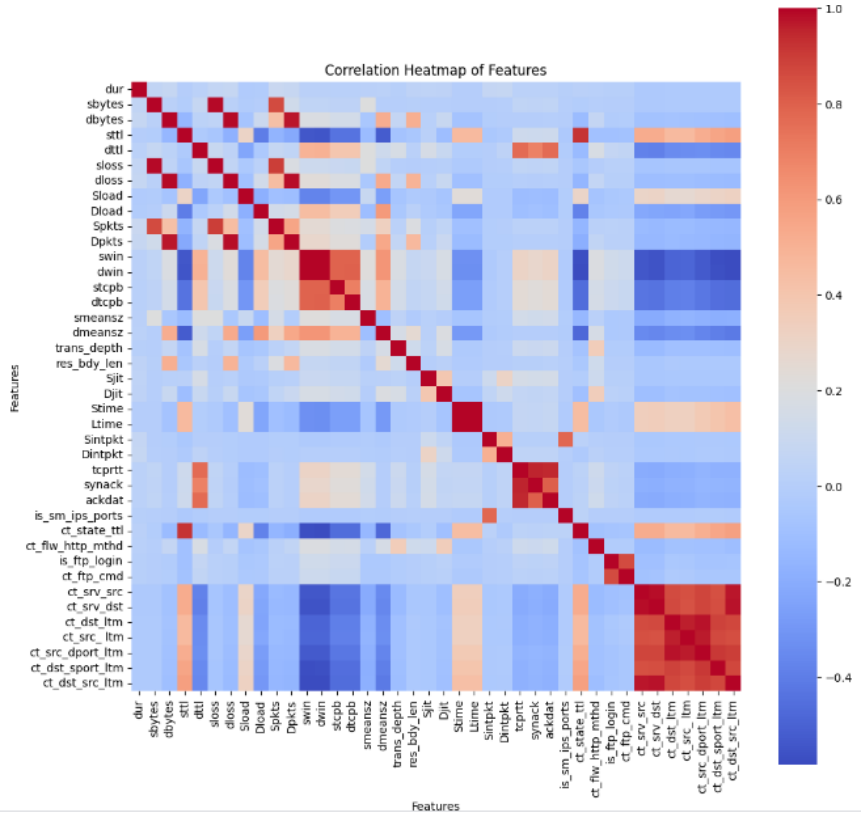

Figure 2 – The correlation matrix based on Pearson correlation coefficients for 40 features

As a result of using the correlation matrix, the 40 features were sorted in descending order of their correlation coefficients and summarized in Table 1.

Table 1 – Results of Traffic Feature Ranking

№	feature	№	feature	№	feature	№	feature
1	dur	11	Dpkts	21	Djit	31	ct_flw_http_mthd
2	sbytes	12	swin	22	Stime	32	is_ftp_login
3	dbytes	13	dwin	23	Ltime	33	ct_ftp_cmd
4	sttl	14	stcpb	24	Sintpkt	34	ct_srv_src
5	dttl	15	dtcpb	25	Dintpkt	35	ct_srv_dst
6	sloss	16	smeansz	26	tcprtt	36	ct_dst_ltm
7	dloss	17	dmeansz	27	synack	37	ct_src_ ltm
8	Sload	18	trans_depth	28	ackdat	38	ct_src_dport_ltm
9	Dload	19	res_bdy_len	29	is_sm_ips_ports	39	ct_dst_sport_ltm
10	Spkts	20	Sjit	30	ct_state_ttl	40	ct_dst_src_ltm

Neural Network Model

The architecture of the created neural network is shown in Fig. 3. The neural network model is implemented in Python using the PyTorch machine learning framework [9]. Data preprocessing and metric calculations for classification quality evaluation were performed using the Scikit-learn [10] and Pandas [11] libraries.

The development was carried out in the specialized online environment Kaggle [12].

The input layer consists of 3 neurons. Each neuron receives binary data (0 or 1) representing various features of the input message, such as the presence of certain words or other characteristics of the text. The hidden layer contains 3 neurons. Each neuron receives a linear combination of input signals, which is weighted. After summing the signals, a sigmoid activation function is applied, which limits the output value to a range from 0 to 1. The weights are changed during the training process to improve the accuracy of predictions. The output layer consists of a single neuron. This neuron takes values from the hidden layer and also uses the sigmoid activation function. The implementation of the neural network model is calculated in the MS Excel program (Figure 3).

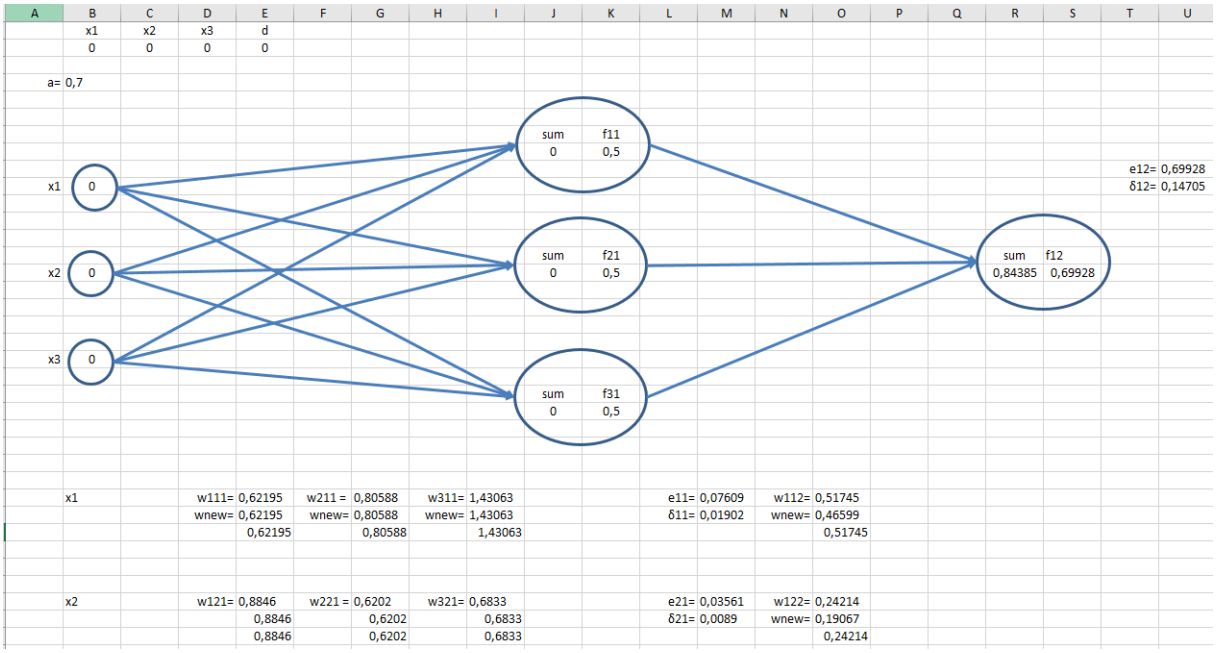

Figure 3 – Proposed neural network architecture

The neural network is trained using the backpropagation method. The purpose of training is to minimize the error between the predicted result and the actual label. During training, the weights of the neurons are adjusted to improve predictions. The main parameters of the model:

- The number of input neurons is 3;
- The number of neurons in the hidden layer is 3;
- Number of output neurons – 1;
- Activation function - sigmoid function;
- Learning algorithm - error propagation back;
- Learning rate (α): 0.7.

After completing the training, the neural network is able to accept new input data and make predictions based on the trained weights.

Neural Network Models in Literature

The 1950s marked the beginning of artificial intelligence, and recent advancements in this field have significantly driven manufacturing innovations. Despite the clear benefits of AI technologies, their use has sparked debates over potential misuse [13]. AI is a branch of computer science focused on developing theories, methods, technologies, and systems to model human intelligence and integrate it into machines [14]. The primary goal of AI is to endow machines with capabilities similar to human intelligence. Machine learning is a method of implementing AI through algorithms that analyze data and learn from it. Deep learning, in turn, is a technology within machine learning that enhances the scope of AI applications [15]. The essence of AI lies in the idea that human intelligence can be precisely described, allowing its reproduction by machines and software [16].

Bindra and Sood investigated six machine learning (ML) methods — LR, KNN, RF, NB, linear SVM, and linear discriminant analysis (LDA) — to determine the most effective method for detecting DDoS attacks [17]. Testing on the CIC IDS dataset revealed that the RF technique achieved the best results with an accuracy of 96.5%, outperforming all other methods. Similarly, Chavan et al. assessed the effectiveness of four ML methods — KNN, SVM, DT, and LR — for detecting DDoS attacks [18]. Among these methods, LR achieved the highest accuracy of 90.4%, surpassing the other techniques. Ensemble methods generally provide higher accuracy compared to base classifiers. Consequently, Das, Saikat, et al. [19] proposed an ensemble model that combines four base ML methods — Multilayer Perceptron (MLP), SVM, KNN, and DT. Experiments conducted on the NSL-KDD dataset showed that the ensemble classifier outperformed the individual classifiers used in the same study.

In [20] and [21], machine learning has been applied for classifying network traffic to detect anomalies. The issue of non-binary network traffic classification during attack detection has also been addressed. Authors [22] conducted a comprehensive evaluation of datasets using the CSE-CIC-IDS2018 dataset and developed a generation model to create a reliable benchmark dataset for IDS and IPS. Data corresponding to normal traffic as well as two types of attacks—DDOS and Infiltration—were selected from this dataset. In the DDOS attack scenario, an attempt is made to cause a denial of service by overwhelming the server with excessive load. In the Infiltration attack scenario, the objective is to gain remote access to a workstation within the targeted network.

In the study [23], an AI algorithm for developing cyberattack detection systems in a Wireless Sensor Network (WSN) is examined (Figure 4).

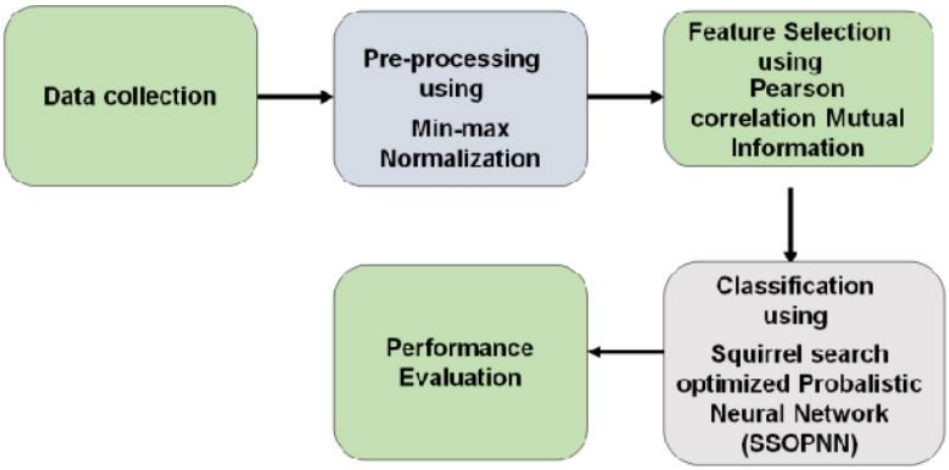

Figure 4 – Data description [23]

The study also proposes several classification methods for detecting cyberattacks in WSN, including Squirrel Search Optimized Probabilistic Neural Network (SSOPNN), Gaussian Naïve Bayes (Gaussian NB), K-Nearest Neighbors (KNN), and Random Forest (RF). A comparative analysis of these methods is presented in the study, using metrics such as detection rate, false positive rate, false negative rate, and average prediction time per sample.

Aslam, N. et al. [24] propose using machine learning (ML) and deep learning (DL) for detecting DDoS attacks in Software-Defined Networking (SDN) in their research. The study develops a taxonomy of solutions for protecting against DDoS attacks. Based on an analysis of 260 scientific articles, 132 papers were selected based on ML and DL solutions for detecting DDoS attacks in SDN. The study suggests security challenges and the development of new protection methods for SDN.

Bolshakov, A.S. et al. [8], an analysis of the dataset was conducted using Pearson correlation coefficients, which allowed for the ranking of these coefficients. A neural network architecture with a sigmoid activation function was developed, effectively addressing the binary classification problem, and the choice of model parameters was justified. The performance of the neural network model was evaluated using ROC and PR curves. Based on the area under the ROC curve (AUC-ROC), optimal classification thresholds were determined, leading to an improvement in the quality of traffic anomaly prediction.

Research Gap and Contribution

Existing studies predominantly rely on classical ML algorithms or isolated deep learning models without systematically evaluating the impact of feature selection on performance. Furthermore, comprehensive comparisons of state-of-the-art DL architectures on recent, high-quality datasets such as UNSW-NB15 remain limited.

The present study addresses these limitations by implementing a hybrid approach that combines correlation matrix-based feature selection with multiple deep learning models, including CNN, LSTM, GRU, MLP, and RNN. The experimental results demonstrate that the CNN model achieved the highest accuracy (99.21%), significantly surpassing the performance metrics reported in prior studies. The use of UNSW-NB15, a dataset with more diverse and realistic traffic scenarios, enhances the generalizability of the findings. Additionally, the study introduces evaluation metrics such as the Kappa Coefficient and Jaccard Index, offering a more nuanced assessment of model reliability. The highest F1-scores achieved were 0.97 (Kappa) and 0.95 (Jaccard), reinforcing the robustness of the proposed method in distinguishing normal and anomalous traffic patterns.

Results.

The developed neural network model was tested with varying numbers of features as shown in Table 1, using a learning rate of 0.001.

The model was trained for 30 epochs. After training, the effectiveness of the neural network was evaluated on a test dataset. The obtained confusion matrix results and their values - TP, TN, FP, FN - formed the basis for calculating classification quality metrics [25].

True Positive (TP): The number of samples correctly predicted as anomalous.

True Negative (TN): The number of samples correctly predicted as normal.

False Positive (FP): The number of samples incorrectly predicted as anomalous.

False Negative (FN): The number of samples incorrectly predicted as normal.

Accuracy $\left(\frac{TP+TN}{TP+TN+FP+FN}\right)$ - this metric represents the proportion of predictions that the model made correctly relative to the total number of samples. This metric performs well only if there is an equal number of samples belonging to each class.

Precision $\left(\frac{TP}{TP+FP}\right)$ - this metric represents the proportion of predicted anomalous samples that are indeed anomalous.

Recall $\left(\frac{TP}{TP+FN}\right)$ - this metric represents the proportion of anomalous samples detected by the model.

F1 $\left(2 * \frac{\text{precision} * \text{recall}}{\text{precision} + \text{recall}}\right)$ – this is a weighted average of accuracy and memorability. This metric can tell you how accurate and reliable the model in question is [26, 27].

Using the given formulas, the metrics Accuracy, Precision, Recall, and F1 were calculated, and the results are presented in the form of a histogram in Figure 5.

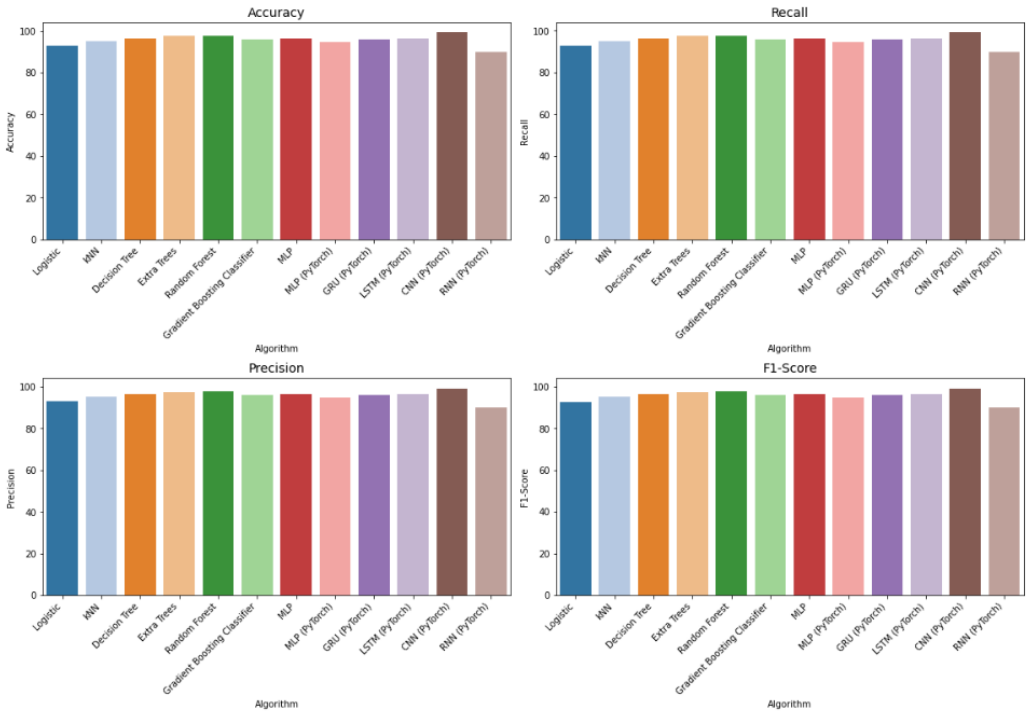

Figure 5 – Performance Metrics Comparison

To enhance the model's performance, it was decided to compute the values of the Kappa Coefficient and the Jaccard Index (table 2) [28].

The Kappa Coefficient provides valuable insight into the agreement between the model's predictions and the true labels, accounting for random chance. This makes it useful for assessing classification quality, comparing models, and evaluating clustering quality. The Kappa Coefficient is a powerful tool for a more precise evaluation of model performance in AI tasks.

The Jaccard Index is a metric that measures the degree of similarity between two sets. In AI, it is often used to assess the quality of binary classification, clustering, and anomaly detection. The

Jaccard Index helps evaluate the accuracy of classifiers, especially when interested in positive results, such as in rare events or anomaly detection tasks.

Table 2 - Results of the Metrics for Kappa Coefficient and Jaccard Index

Traffic	Accuracy	Precision	Recall	F1	Kappa Coefficient	Jaccard Index
Normal	0,9925	0,9925	0,9925	0,992503	0,984479	0,9843
Anomalous	0,9925	0,9925	0,9960	0,9912	0,9633	0,9223

Thus, using the classification threshold determined by the Kappa Coefficient and Jaccard Index metrics, the F1 scores achieved are 0.97 and 0.95, respectively, which represent the best-obtained evaluation of the classification quality of the developed neural network model.

Discussion.

The study presents the results of testing five types of AI (MLP, GRU, LSTM, CNN, and RNN) for binary classification tasks aimed at detecting attacks (Table 3).

Table 3 – Performance evaluation of AI

	Accuracy	Recall	Precision	F1-Score	time to train	time to predict	total time
MLP (PyTorch)	94.98%	94.98%	94.98%	94.98%	43.7	0.2	43.9
GRU (PyTorch)	96.34%	96.34%	96.34%	96.34%	203.0	0.2	203.1
LSTM (PyTorch)	96.32%	96.32%	96.32%	96.32%	207.0	0.3	207.3
CNN (Pytorch)	99.26%	99.20%	99.20%	99.18%	830.0	0.2	830.2
RNN (Pytorch)	90.00%	90.20%	90.20%	90.20%	1150.0	0.2	1150.2

Table 3 presents a comparison of the effectiveness of four AI methods using four different performance metrics.

The study employed supervised learning. After tuning the model parameters, an AI architecture with a minimal number of layers was used. The configurable parameters were set to a learning rate of 0.001 and a batch size of 2000 (Figure 6).

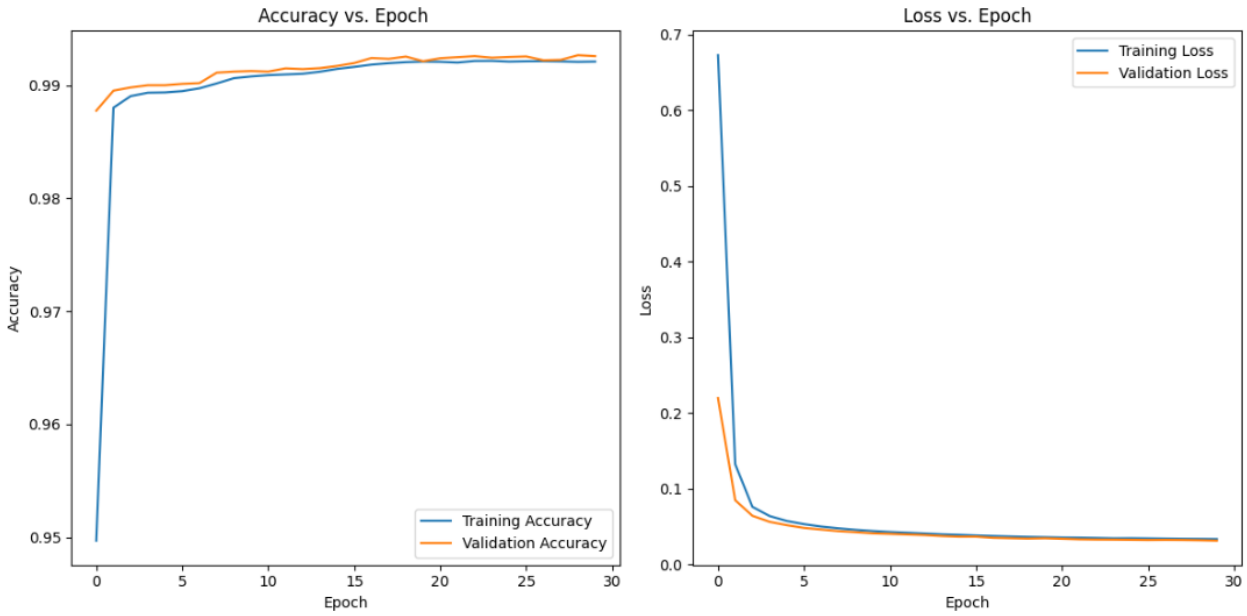

Figure 6 – Training schedule for CNN (PyTorch)

According to the results shown in Figure 6, the training process was stable and no overfitting was observed. The model's accuracy was 0.9924, and the error loss was 0.0334.

Figure 7 displays the confusion matrix for the four AI models.

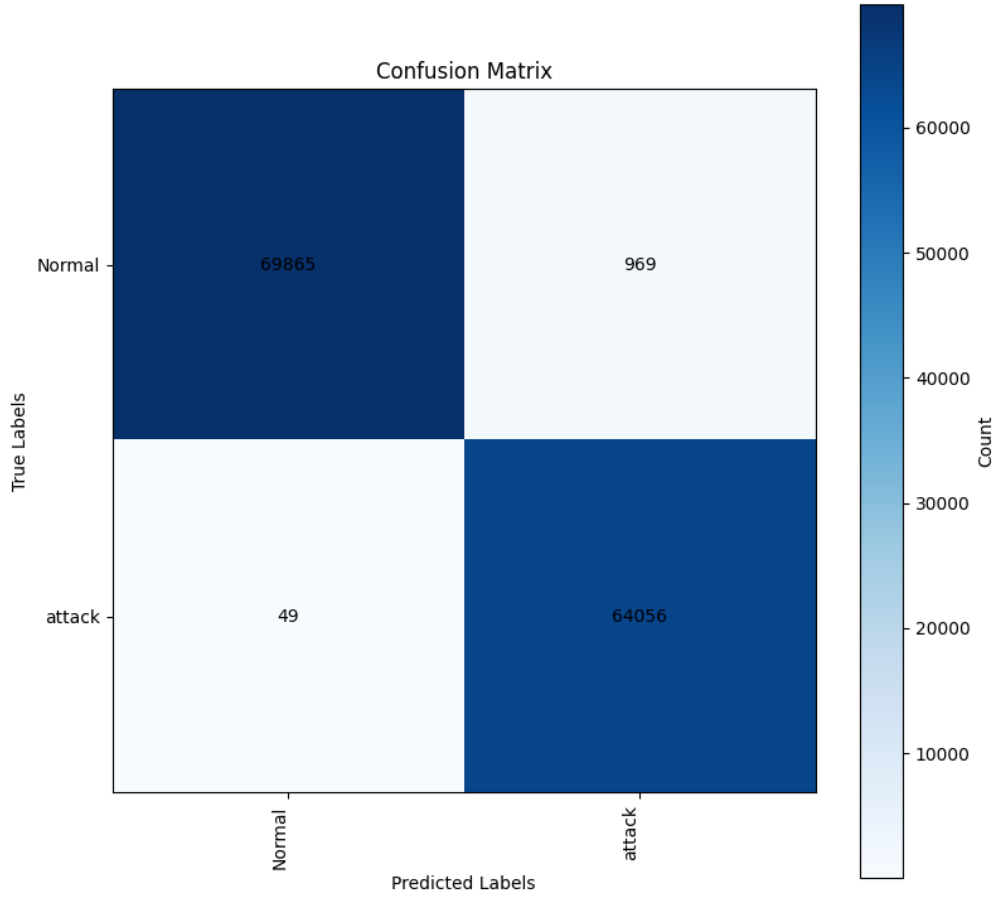

Figure 7 – Confusion Matrix

Based on the data from Figure 6, the total number of correctly predicted instances for the Normal class is 69,865, while the number of incorrect predictions is 969. The overall total number of correctly predicted instances is 133,921, with incorrect predictions totaling 1,010, which represents less than 1%.

Preprocessing and feature selection are crucial steps before implementing AI methods. The preliminary implementation of data preprocessing and testing critical functions could improve accuracy by approximately 47%. Thus, in this study, the proposed model demonstrated promising results after selecting important and influential features and applying the appropriate AI model.

Conclusions.

The conducted research demonstrated that using a correlation matrix for feature selection and applying a neural network enables the development of an effective system for attack detection. With the selected number of features, the classification scores achieved, according to the Kappa Coefficient and Jaccard Index metrics, were F1=0.97 and F1=0.95, respectively, marking the highest classification quality for the developed neural network model.

The UNSW-NB 15 dataset used in this study was divided into 80% for training the models and 20% for testing. The effectiveness of the four methods was compared on only 31 instances from the selected dataset using a sample selection method. Among the models tested, CNN achieved the highest accuracy at 99.21%, surpassing all other models. The LSTM model ranked second with an accuracy of 96.33%, followed by the GRU model with an accuracy of 95.90%. The MLP model was in fourth place with an accuracy of 94.76%, while the RNN method achieved the lowest accuracy at 90.15%.

Exploring various types of AI, and analyzing and comparing them, will further aid in optimizing neural network parameters, thereby reducing computational resource costs for the system. The evaluation of the AI model's performance using the Kappa Coefficient and Jaccard Index demonstrated effective classification threshold results, which enhanced the accuracy of anomaly detection in network traffic.

Having an intelligent system capable of detecting intrusions significantly contributes to ensuring user privacy and security. Future work could focus on classifying different types of attacks on cybersecurity systems. Additionally, classification accuracy could be improved by employing integrated methods that combine multiple individual classifiers.

Acknowledgement

This research has been funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP26102055).

References

1. Incident Review for Q1 2024. (2024). http://cert.gov.kz/news/11/2641 (accessed: 26.01.2025)

2. Gartner Research. Hype Cycle for Security Operations. (2024). Published: July 29, 2024 http://www.gartner.com/en/documents/5622491 (Accessed: 26.01.2025)

3.Current Cyber Threats: Q1 2024. (2024) http://ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2024-q1/ (accessed: 26.01.2025)

4.Glushanskij S.M., Buglov V.E. Inzhenernyj vestnik Dona. (2023). http://ivdon.ru/ru/magazine/archive/n1y2023/8150 (accessed: 08.01.2025).

5.The UNSW-NB15 Dataset. (2024). // UNSW Research URL: https://research.unsw.edu.au/projects/unsw-nb15-dataset (accessed: 10.01.2025).

6. Sheluhin O.I., Erohin S.D., Vanyushina A.V. (2018). Classification of IP traffic using machine learning methods. Edited by prof.Sheluhin O.I.: Goryachaya liniya – Telekom. 282 p. DOI: 10.21681/2311-3456-2018-4-21-28

7. Chen P., Li F., Wu C. (2021). Research on Intrusion Detection Method Based on Pearson Correlation Coefficient Feature Selection Algorithm. Journal of Physics: Conference Series. Vol. 1757. No. 1. P. 012054. DOI: 10.1088/1742-6596/1757/1/012054

8. Bolshakov, A.S., Khusainov, R.V., Osin, A.V. (2021). "Traffic Anomaly Detection Using Neural Networks for Information Security Protection" // Journal of the Institute "INTECH": I-methods. Vol. 13, No. 4. URL: http://intech-spb.com/wp-content/uploads/archive/2021/4/6-bolshakov.pdf (Accessed: 16.01.2025).

9. Electronic resource. URL: https://pytorch.org (Accessed: 26.01.2025).

10. Electronic resource. URL: https://scikit-learn.org/stable/ (Accessed: 26.01.2025).

11. Electronic resource. URL: https://pandas.pydata.org (Accessed: 26.01.2025).

12. Electronic resource. URL: https://www.kaggle.com (Accessed: 26.01.2025).

13. Angelopoulos, A.; Michailidis, E.T.; Nomikos, N.; Trakadas, P.; Hatziefremidis, A.; Voliotis, S.; Zahariadis, T. (2020). Tackling Faults in the Industry 4.0 Era-A Survey of Machine-Learning Solutions and Key Aspects. Sensors 2020, 20, 109. DOI: 10.3390/s20010109

14. Li, J. (2018). Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering, 19(12), 1462–1474. DOI: 10.1631/FITEE.1800573

15. H. Ji, O. Alfarraj and A. Tolba. (2020). "Artificial Intelligence-Empowered Edge of Vehicles: Architecture, Enabling Technologies, and Applications," in *IEEE Access*, vol. 8, pp. 61020-61034, 2020, DOI: 10.1109/ACCESS.2020.2983609

16. R. Trifonov, O.Nakov and V. Mladenov. (2018). "Artificial Intelligence in Cyber Threats Intelligence,"2018 International Conference on Intelligent and Innovative Computing

Applications (ICONIC), Mon Tresor, Mauritius, 2018, pp. 1-4, DOI**:** 10.1109/ICONIC.2018.8601235

17. Bindra, Naveen & Sood, Manu. (2019). Detecting DDoS Attacks Using Machine Learning Techniques and Contemporary Intrusion Detection Dataset. Automatic Control and Computer Sciences. 53. 419-428. DOI: 10.3103/S0146411619050043

18. N. Chavan, M. Kukreja, G. Jagwani, N. Nishad and N. Deb. (2022). "DDoS Attack Detection and Botnet Prevention using Machine Learning," 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2022, pp. 1159-1163, DOI: 10.1109/ICACCS54159.2022.9785247

19. Das, S., Mahfouz, A. M., Venugopal, D., & Shiva, S. (2019). DDoS Intrusion Detection Through Machine Learning Ensemble. 2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C). DOI: 10.1109/qrs-c.2019.00090

20. Babicheva M.V., Tret'yakov I.A. (2023). Application of machine learning methods for automated detection of network intrusions. Herald of Dagestan State Technical University. Technical Sciences. Vol. 50. no.1. Pp. 53–61. DOI: 10.21822/2073-6185-2023-50-1-53-66 (In Russian)

21. Chastikova, V.A., Zherlitsyn, S.A., Volya, Y.I., & Sotnikov, V. (2020). Neural network technology for detecting anomalous network traffic. CASPIAN JOURNAL: Control and High Technologies, 49(1), 20-32. DOI: 10.21672/2074-1707.2020.49.4.020-032

22. Sharafaldin, I., Gharib, A., Lashkari, A. H., … Ghorbani, A. A. (2017). Towards a Reliable Intrusion Detection Benchmark Dataset. Software Networking, 2017(1), 177–200. DOI: 10.13052/jsn2445-9739.2017.009

23. Aneja, A. (2023). Attack Detection in Wireless Sensor Networks using Novel Artificial Intelligence Algorithm. 2023 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 295-300. DOI: 10.1109/I-SMAC58438.2023.10290399

24. Aslam, N., Srivastava, S. & Gore, M.M. A. (2024). Comprehensive Analysis of Machine Learning- and Deep Learning-Based Solutions for DDoS Attack Detection in SDN. Arab J Sci Eng 49, 3533–3573 DOI: 10.1007/s13369-023-08075-2

25. Powers, David & Ailab. (2011). Evaluation: From precision, recall and F-measure to ROC, informedness, markedness & correlation. J. Mach. Learn. Technol. 2. 2229-3981. 10.9735/2229-3981. http://www.bioinfo.in/contents.php?id=51

26. Soleymani, Roghayeh & Granger, Eric & Fumera, Giorgio. (2019). F-Measure Curves: A Tool to Visualize Classifier Performance Under Imbalance. Pattern Recognition. 100. 107146. DOI: 10.1016/j.patcog.2019.107146

27. Hand, D.J., Christen, P. & Kirielle, N. (2021). F*: an interpretable transformation of the F-measure. Mach Learn 110, 451–456 (2021). DOI: 10.1007/s10994-021-05964-1

28. Pravin, S. C., & Palanivelan, M. (2022). WDSAE-DNDT BASED SPEECH FLUENCY DISORDER CLASSIFICATION. Malaysian Journal of Computer Science, 35(3), 222–242. DOI: 10.22452/mjcs.vol35no3.3

ЖЕЛІЛІК ТРАФИК АНОМАЛИЯЛАРЫН АНЫҚТАУ ҮШІН ЖАСАНДЫ ИНТЕЛЛЕКТ ӘДІСТЕРІН ҚОЛДАНУ

Аңдатпа. *Ақпараттық технологиялардың дамуы ақпараттық ресурстардың қауіпсіздігін қамтамасыз етудің маңыздылығын көрсетуді жалғастыруда. Ақпараттық қауіптердің әртүрлі түрлерінің көбеюі шабуылдарды анықтауды қиындатады. Зерттеудің мақсаты талап етілетін анықтау сапасына қол жеткізу үшін трафик элементтерінің санын азайту кезінде шабуылдарды анықтау үшін жасанды интеллект әдістерін қолдану болып табылады. AI үйрету үшін желілік трафиктегі шабуыл мүмкіндіктерін дәл анықтай алатын жоғары сапалы деректер жиынтығын жасау қажет. UNSW-NB 15 деректер жинағында оқытылған жасанды интеллектті қолдана*

отырып ұсынылған тәсіл желілік шабуылдардың тоғыз түрін қамтитын: Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode және Worms. Деректерді өңдеу үшін Pytorch және Pandas кітапханалары бар Python тілі пайдаланылды. Бағдарламалық модульдің өнімділігіне талдау жасалды, Kappa коэффициенті және Жаккар индексі сияқты екілік бағалау әдістері қолданылды. Ұсынылған AI моделінің тиімділігі жіктеу көрсеткіштері арқылы бағаланады: Accuracy, Precision, Recall және F1 Score. Әртүрлі мүмкіндіктер жиынтығымен әзірленген модельді тестілеу бес таңдалған мүмкіндікті пайдалану кезінде модельдің қалыптан тыс трафикті жоғары сапалы болжауға қол жеткізуге мүмкіндік беретінін көрсетті. AI моделінің өнімділігі Kappa коэффициенті мен Жаккар индексі арқылы бағаланды. Алынған нәтижелер бойынша классификацияның тиімді шектері есептелді, бұл қалыптан тыс трафикті болжау сапасын жақсартты. Бағалау нәтижелері көрсеткендей, UNSW-NB 15 деректер жинағында әзірленген модель трафик ауытқуларын дәл анықтай алады, осылайша ақпараттық ресурстардың ақпараттық қауіпсіздігіне ықпал етеді.

***Түйін сөздер**: желілік трафик, жасанды интеллект, нейрондық желілер, шабуылдарды анықтау, деректер жинағы, UNSW-NB, Kappa коэффициенті, Жаккард индексі.*

ПРИМЕНЕНИЕ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛИЙ СЕТЕВОГО ТРАФИКА

***Аннотация.** Развитие информационных технологий продолжает выдвигать на первый план важность обеспечения безопасности информационных ресурсов. Растущее количество различных видов информационных угроз усложняет обнаружение атак. Цель исследования — применение методов искусственного интеллекта для обнаружения атак при минимизации количества элементов трафика для достижения требуемого качества обнаружения. Для обучения ИИ необходимо создать высококачественный набор данных, позволяющий точно выявлять особенности атаки в сетевом трафике. В предлагаемом подходе используется искусственный интеллект, обученный на датасете UNSW-NB 15, который включает в себя девять типов сетевых атак: Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode и Worms. Для реализации используется Python с библиотеками Pytorch и Pandas для обработки данных. Был проведен анализ производительности программного модуля, а также применены методы двоичной оценки, такие как коэффициент Каппа и индекс Жаккара. Эффективность предложенной модели ИИ оценивается с помощью метрик классификации: Accuracy, Precision, Recall, F1 Score. Тестирование разработанной модели с различными наборами признаков показало, что модель позволяет достичь высокого качества прогнозирования аномального трафика при использовании пяти выбранных признаков. Производительность модели ИИ оценивалась с помощью коэффициента Каппа и индекса Жаккара. На основе полученных результатов были рассчитаны эффективные пороги классификации, что повысило качество прогнозирования аномального трафика. Результаты оценки показывают, что разработанная модель, обученная на наборе данных UNSW-NB 15, может точно выявлять аномалии трафика, тем самым способствуя безопасности информационных ресурсов.*

***Ключевые слова**: сетевой трафик, искусственный интеллект, нейронные сети, обнаружение атак, набор данных, UNSW-NB, коэффициент Каппа, индекс Жаккарда.*

Information about the authors

Ordabayeva Gulzinat	Senior lecturer at the Department of Cybersecurity and Cryptology, Kazakh National University named after Al-Farabi, Almaty; 050038; Kazakhstan; e-mail: ordabayeva.gulzinat@kaznu.kz
Beketova Aiman	Senior lecturer at the Department of Cybersecurity and Cryptology, Kazakh National University named after Al-Farabi, Almaty; 050038; Kazakhstan; e-mail: aiman.beketova@gmail.com
Dzhsupbekova Gulzat	Candidate of Pedagogical Sciences, Head of the Department of Information Technology, M. Auezov South Kazakhstan State University, Shymkent, Kazakhstan; E-mail: gulzat20.10@mail.ru
Baispay Gulshat	Senior lecturer at the Department of Cybersecurity and Cryptology, Kazakh National University named after Al-Farabi, Almaty; 050038; Kazakhstan; e-mail: gulshat.bgb2@gmail.com

Сведения об авторах

Ордабаева Гулзинат	ст.преп. кафедры «Кибербезопасность и криптология», Казахский национальный университет имени аль-Фараби, г.Алматы, E-mail: ordabayeva.gulzinat@kaznu.kz
Бекетова Айман	ст.преп. кафедры «Кибербезопасность и криптология», Казахский национальный университет имени аль-Фараби, г.Алматы, E-mail: aiman.beketova@gmail.com
Джусупбекова Гулзат	кандидат педагогических наук, зав. кафедрой «Информационно-коммуникационные технологии», Южно-Казахстанский университет имени М.Ауэзова, г.Шымкент;E-mail: gulzat20.10@mail.ru
Байспай Гүлшат	ст.преп. кафедры «Кибербезопасность и криптология», Казахский национальный университет имени аль-Фараби, г.Алматы, E-mail: gulshat.bgb2@gmail.com

Авторлар туралы мәлімет

Ордабаева Гулзинат	«Киберқауіпсіздік және криптология» кафедрасының аға оқытушысы, әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қаласы; E-mail: ordabayeva.gulzinat@kaznu.kz
Бекетова Айман	«Киберқауіпсіздік және криптология» кафедрасының аға оқытушысы, әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қаласы; E-mail: aiman.beketova@gmail.com
Джусупбекова Гулзат	педагогика ғылымдарының кандидаты, «Ақпараттық-коммуникациялық технологиялар» кафедрасының меңгерушісі, М.Ауэзов атындағы Оңтүстік Қазақстан университеті, Шымкент қаласы; E-mail: gulzat20.10@mail.ru
Байспай Гүлшат	«Киберқауіпсіздік және криптология» кафедрасының аға оқытушысы, әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қаласы; E-mail: gulshat.bgb2@gmail.com