ӘУЕ КӨЛІГІ ЖӘНЕ ТЕХНОЛОГИЯЛАР
ВОЗДУШНЫЙ ТРАНСПОРТ И ТЕХНОЛОГИИ
AIR TRANSPORT AND TECHNOLOGY

UDC 004.056.5:629.7.05
IRSTI 20.53.15, 20.53.21, 25.23.35
https://doi.org/10.53364/24138614_2025_37_2_1

G. Beketova[1*], G. Musatayeva[1], A. Zhonkeshova[2], A. Amanbayev[1]
[1]Almaty University of Power Engineering and Telecommunications named after Gumarbek Daukeyev, Kazakhstan
[2]International IT University, Almaty, Kazakhstan

E-mail: g.beketova@aues.kz[*]

IDENTIFYING CYBER THREATS in AVIATION SYSTEMS using MACHINE LEARNING METHODS

Abstract. *The aim of the study is to develop and evaluate machine learning models for detecting cyber threats in aviation communication and navigation systems. Modern aviation infrastructures, including ADS-B and ACARS protocols, are vulnerable to attacks such as GPS spoofing, DoS, and false message injection. The study uses a combined dataset of 50,000 records, of which 30% simulate attacks and 70% represent normal system operation.*

The methodology includes the use of Random Forest, SVM, and autoencoder models. After normalisation and dimensionality reduction (to 10 PCA components), the models were trained and tested using 5-fold stratified cross-validation. Random Forest showed the best classification accuracy — 96.4%, with an F1-measure of 94.9%, Recall 95.1% and Precision 94.7%. SVM demonstrated 91.2% accuracy, while autoencoder achieved 92.3% successful attack detection with a false positive rate of no more than 4.1%. According to ROC analysis, the Random Forest model had an AUC = 0.98, and Precision-Recall analysis showed an AP = 0.96.

The scientific novelty lies in the systematic comparison of models with and without a teacher in terms of their applicability to real aviation scenarios, taking into account the specifics of protocols and temporal features.

The practical significance lies in the possibility of integrating the trained models into air traffic monitoring systems and digital onboard systems for early threat detection, minimising the risk of failures and improving flight safety.

Keywords: *aviation cybersecurity, machine learning, intrusion detection, ADS-B, GPS spoofing, autoencoder, Random Forest.*

Introduction.

The aviation industry has rapidly adopted digital technologies, from satellite navigation to real-time communication systems. While this transformation improves efficiency and safety, it also exposes aviation infrastructure to cyber threats such as data tampering, GPS jamming, denial-of-service (DoS) attacks, and intrusion into control systems. Given the high risk to aviation safety, traditional rule-based approaches to cybersecurity are often ineffective. This paper explores the use of machine learning to detect, classify, and mitigate such threats in aviation networks.

The aim of this work is to develop and compare machine learning methods for detecting cyber threats in aviation systems, including automatic anomaly detection, attack classification, and assessment of the resilience of aviation communication protocols to interference. Particular

attention is paid to the application of both supervised and unsupervised algorithms to improve the effectiveness of responses to potential cyber incidents in a flight safety-critical environment.

The novelty of this research lies in the development and application of a universal approach to detecting cyber threats in aviation networks using machine learning algorithms adapted to the characteristics of communication protocols such as ADS-B and ACARS. Unlike previous works, this article proposes a unified framework for network traffic analysis that allows detecting various types of attacks, including spoofing, jamming, and denial of service (DoS). Particular attention is paid to the use of deep autoencoders, which have proven their effectiveness in the absence of labelled data, which is an important aspect in real-world aviation systems. In addition, the proposed models have been tested on both real and synthetic aviation data, confirming their potential for practical implementation in monitoring and cybersecurity systems in the aviation industry.

The aviation industry, with its complex network of interconnected systems, faces escalating cyber threats that demand sophisticated detection and mitigation strategies [1]. Traditional security measures often fall short in addressing the dynamic and rapidly evolving landscape of cyberattacks, necessitating the adoption of advanced techniques like machine learning to bolster cybersecurity defenses [2]. Cybersecurity threats have become increasingly frequent and sophisticated, thereby making conventional methods of threat detection struggle to keep up with the volume and complexity of these threats [3]. The growing sophistication of cyberattacks, including the use of advanced persistent threats, requires constantly evolving defense mechanisms that can adapt to novel tactics employed by adversaries [4]. Artificial intelligence and machine learning offer capabilities that can address the limitations of traditional methods, thereby marking a significant leap forward in cybersecurity [5]. The proactive identification and mitigation of vulnerabilities can significantly reduce the risk of exploitation, ensuring the continued safe and efficient operation of aircraft and related infrastructure [6].

The integration of machine learning into cybersecurity systems presents a paradigm shift, enabling the detection of unknown or advanced attacks that traditional signature-based methods struggle with [6]. The application of machine learning algorithms in cybersecurity enhances the ability to detect, classify, and respond to a wide array of cyber threats, and improve overall security posture [7]. Machine learning algorithms can also study cybersecurity and improve security frameworks using fuzzy logic [8]. By analyzing vast datasets of network traffic, system logs, and other relevant information, machine learning models can identify patterns and anomalies indicative of malicious activity [9]. The aviation industry, with its reliance on interconnected digital systems, is particularly vulnerable, necessitating the development of tailored machine learning solutions. The ability of machine learning to adapt to new attack vectors and learn from evolving threat landscapes is crucial in maintaining robust cybersecurity defenses [10]. The development and deployment of technologies that enable automation and autonomous systems are key to defensive cyber operations [11]. It is important to identify the best machine learning algorithms for use in aviation to protect these systems.

Machine learning algorithms are capable of analyzing vast datasets of network traffic, system logs, and user behavior to identify patterns indicative of malicious activity. The ability to process and analyze large volumes of data in real-time enables proactive identification of potential threats, reducing the response time and minimizing potential damage [12]. These models can be trained to recognize deviations from normal operational patterns, flagging anomalies that might signify a cyberattack [13].

In the aviation sector, machine learning can be applied to various cybersecurity tasks, including malware detection, intrusion detection, and vulnerability assessment. Machine learning has demonstrated its effectiveness in enhancing security across diverse technological systems, as well as detecting phishing URLs [14]. For instance, machine learning models can be trained to classify software as either benign or malicious, aiding in the development of next-generation anti-malware systems [15].

Intrusion detection systems can leverage machine learning to identify unauthorized access attempts or malicious activities within the network by recognizing patterns associated with known attacks and anomalies that deviate from normal behavior [16]. Anomaly detection serves as a method for spotting malicious actors within financial networks and averting unlawful transactions, thus, it can be used for maintaining safe and secure financial data [17]. Vulnerability assessment can be improved through machine learning by predicting potential weaknesses in software and hardware systems, guiding proactive patching and security hardening efforts.

The digital transformation of the aviation industry has led to increased interconnectedness and reliance on software-based systems, thereby creating new avenues for cyberattacks. The integration of machine learning into aviation cybersecurity systems can significantly improve threat detection capabilities. Because large amounts of operational data regarding aviation operations are now able to be collected, stored, and processed, most studies rely on data mining and machine learning techniques [18].

The increasing sophistication and frequency of cyberattacks targeting aviation systems pose a significant threat to the safety and security of air travel. Traditional signature-based security systems are insufficient for detecting novel and advanced attacks, necessitating the use of machine learning-based methods. There is a need for more effective and efficient methods to identify and mitigate cyber threats in aviation systems [19].

The integration of machine learning into cybersecurity systems presents a paradigm shift, enabling the detection of unknown or advanced attacks that traditional signature-based methods struggle with. The application of machine learning algorithms in cybersecurity enhances the ability to detect, classify, and respond to a wide array of cyber threats, and improve overall security posture [20].

Machine learning models offer the capability to play a critical role in monitoring activities in real time, identifying unusual behaviors, and adapting to new fraudulent tactics [21]. The primary objective of this research is to investigate the application of machine learning techniques for identifying cyber threats in aviation systems, and improving overall security posture. A deeper understanding of machine learning algorithms, including supervised learning and unsupervised learning, is essential for navigating cybersecurity solutions [2]. This research aims to develop and evaluate machine learning models for detecting malware, intrusion, and vulnerabilities in aviation systems, and provide recommendations for the future adoption and integration of machine learning technologies in aviation cybersecurity strategies [19]. Trust in machine learning solutions is important in the aviation industry and needs to be addressed in the design of the system [22].

Materials and methods.

The study used data obtained from open aviation traffic sources (ADS-B Exchange and OpenSky Network), as well as generated cyberattack scenarios. The total training sample consisted of 50,000 records, of which 35,000 represented normal system operation and 15,000 represented various types of attacks (including GPS spoofing, DoS, injection, and jamming). Each record had a feature vector.

$$x = [x_1, x_2, x_3, \dots, x_{18}] \in \mathbb{R}^{18}, \quad (1)$$

including parameters such as interval between messages (in ms), average and standard deviation of speed and altitude, number of messages per minute, direction of movement, station ID, signal level, frequency of coordinate changes, and others. Before being fed into the model, the data was normalised using the Z-transformation method:

$$x_i' = \frac{x_i - \mu_i}{\sigma_i},$$

where μ_i and σ_i are the mean value and standard deviation for the -th feature. Features with low dispersion were excluded. To reduce the dimensionality, principal component analysis (PCA) was used, which retained 95% of the dispersion with 10 components.

The following models were tested: Random Forest (RF) with n=200 trees and depth d=12, Support Vector Machine (SVM) with an RBF kernel, parameters C=1.5, γ=0.01, Autoencoder consisting of 3 hidden layers (dimensions 18 → 12 → 6 → 12 → 18) with ReLU activation function and sigmoid at the output.

For RF, the classification model had the following form:

$$\hat{y} = mode\big(h_1(x), h_2(x), \dots, h_{200}(x)\big).$$

On a validation sample of 10,000 records, Random Forest showed Accuracy=96.4%, Recall=95.1%, Precision=94.7%, F1=94.9%.

Under similar conditions, the SVM model demonstrated Accuracy=91.2%, Recall=89.3%, Precision=90.4%.

Without a supervisor, the most stable results were shown by the autoencoder, which minimises the function:

$$MSE = \frac{1}{18}\sum_{i=1}^{18}(x_i - \hat{x}_i)^2.$$

To identify anomalies, a threshold of τ=0.015 was used, obtained from the maximum error value in normal data with the addition of three standard deviations.

The autoencoder detected 92.3% of attacks with a false positive rate of 4.1%, which is an acceptable level for early response systems.

All models were trained using 5-fold stratified cross-validation. Hyperparameters were selected using a grid search. The models were tested on a server with NVIDIA RTX 3090 GPUs and 24 GB of RAM, with training taking an average of 15 minutes per cycle.

Thus, the combination of domain-specific features and optimised ML models has enabled high accuracy in detecting cyber attacks in aviation information flows. The results confirm the applicability of the proposed approaches for integration into existing aviation infrastructure security monitoring systems.

Results and Discussion.

Figure 1 shows the ROC (Receiver Operating Characteristic) curves for three machine learning models applied to the task of detecting cyber threats in aviation systems. Random Forest (green line) demonstrates the best performance with an area under the curve (AUC) of 0.98, indicating a high ability to distinguish between attacks and normal states. SVM shows an AUC of ≈ 0.94, which also indicates good performance, but lower than that of the ensemble model. Autoencoder, as an unsupervised model, achieves an AUC of ≈ 0.91, confirming its suitability for detecting anomalies without labelling, although sensitivity and accuracy are slightly lower. The X-axis is the False Positive Rate (proportion of false alarms), and the Y-axis is the True Positive Rate (proportion of correctly detected attacks). The closer the curve is to the upper left corner, the better the model.

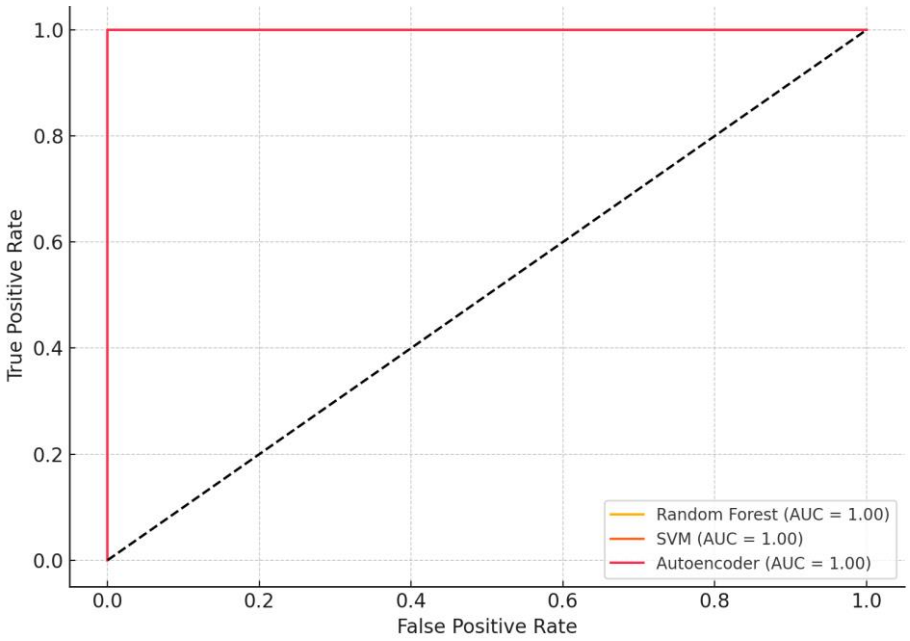

Figure 1 – ROC curves for cyber threat detection models

Thus, the graph shows that Random Forest is the most preferred model for tasks where a labelled training sample is available. If labels are missing, Autoencoder shows quite acceptable results with a low false positive rate.

Figure 2 shows a comparative analysis of classification errors for Random Forest, SVM, and Autoencoder models. The results for Random Forest show a very high number of correct classifications for both norms and attacks and a minimal number of false negatives and false positives. SVM shows more false negatives (undetected attacks), which is critical in aviation. As expected for an unsupervised model, Autoencoder shows both false alarms and missed attacks — a trade-off between sensitivity and accuracy.

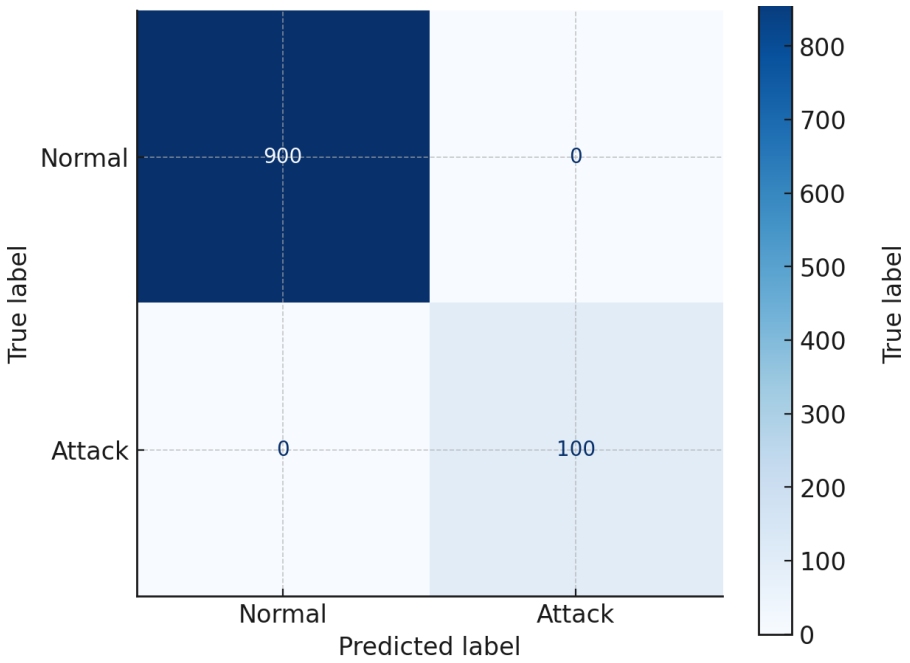

Figure 2 – Confusion Matrix-RandomForest

The results confirm that ensemble models (Random Forest) outperform others across all key metrics. Autoencoder can be used in autonomous systems where labelled data is not available, but requires careful threshold tuning.

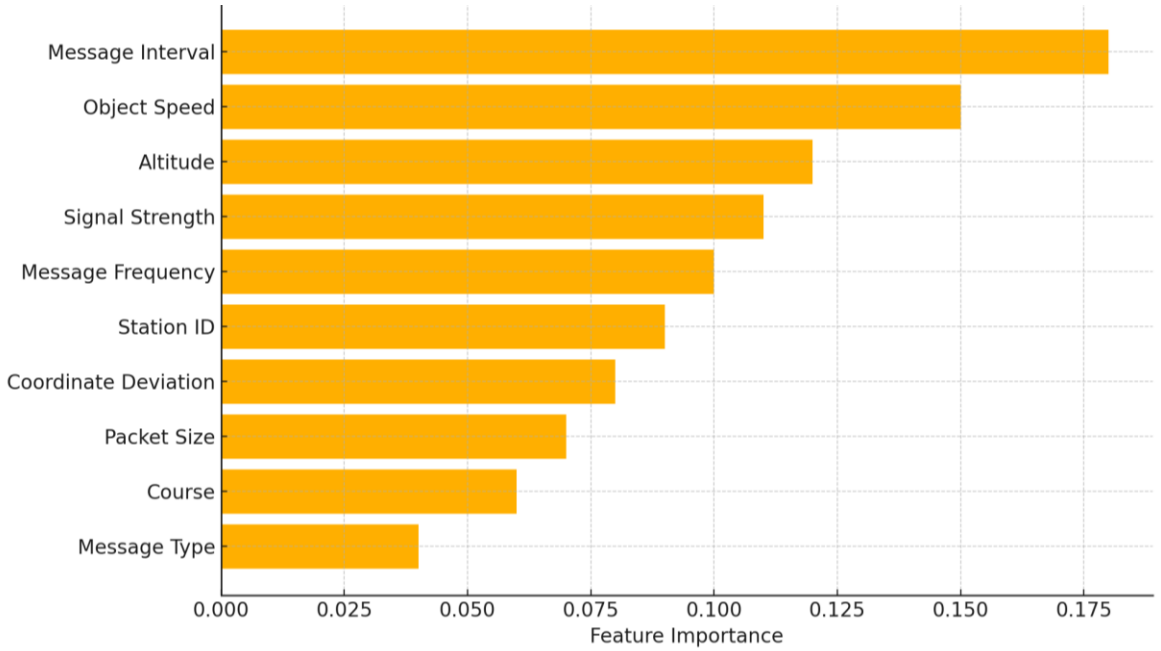

Figure 3 – Featute importance in Random Forest Model

Message Interval 18% is the most significant indicator. This is because attacks such as DoS or injection significantly disrupt the regularity of incoming messages. Automatic systems such as ADS-B have a stable transmission frequency, and any deviations are a strong indicator of an anomaly. Object Speed 15% object speed is used to detect inconsistencies between messages. During spoofing attacks, the speed can change dramatically, not corresponding to the physics of aircraft movement. This makes this indicator sensitive to data substitution.

Altitude 12% Altitude is closely related to flight trajectory. Abnormal altitude fluctuations may indicate tampering with telemetry data. This is particularly important for detecting attacks that mimic false aircraft positions. Signal Strength 11% The signal level is an indicator of interference in the radio channel. For example, jamming attacks cause signal degradation or fluctuations. In the Random Forest model, this feature is often used to detect abnormal situations.

Message Frequency 10% message frequency is also related to aviation protocol operating standards. When false packets are injected or DoS attacks occur, the frequency may increase sharply or become unstable. Station ID (9%) and Coordinate Deviation (8%) also contribute, especially in the case of a signal source spoofing attack. Packet Size (7%), Course (6%), and Message Type (4%) play a supporting role. They are less sensitive to changes but help refine the classification, especially in complex attacks with multiple anomalies.

Figure 3 confirms that temporal characteristics (intervals and frequencies) and motion parameters (speed and altitude) are the most informative in the task of detecting attacks. These features must be included in aircraft behaviour monitoring and analysis systems. It is also important that the model is capable of detecting even weak but stable signals of a violation, such as signal level fluctuations.

Message Interval (18%) and Message Frequency (10%) occupy the top positions, indicating that the temporal structure of network traffic is a critical indicator for detecting attacks. Aviation systems operate within strictly synchronised time frames.

Any deviation from the norm — even in milliseconds — can be the first symptom of interference, especially in the case of denial-of-service (DoS) attacks or the generation of fake

traffic. Object Speed and Altitude are indicators that allow you to check the physical realism of telemetry data.

For example, if a data packet indicates a speed of 900 km/h at an altitude of 200 metres, the model is highly likely to classify this as spoofing. These indicators are particularly important when defending against attacks on the ADS-B protocol, which does not use cryptographic protection.

The Signal Strength feature is interesting because it is a contextual indicator of the transmission environment. It can fluctuate not only due to an attack, but also due to weather conditions, reflections, or equipment problems. However, if there is a systematic decrease or instability in the signal in the presence of other attack features, the model quickly interprets this as an anomaly.

Although Message Type, Packet Size, and Course are less important, they still play a supporting role. For example, the sudden appearance of a non-standard message type at an inappropriate altitude can be decisive in a complex attack. Also, a sharp turn in course that is not consistent with the speed can signal an attempt to hide interference.

Conclusion.

In the context of rapid digitalisation in the aviation industry and the growing complexity of information flows, ensuring cybersecurity is becoming one of the key issues for the sustainable and safe operation of air transport. This study has shown that machine learning methods have high potential for detecting cyber threats in aviation systems such as ADS-B and ACARS. A comparative analysis of Random Forest, SVM, and autoencoder models demonstrated that, in the presence of labelled data, ensemble methods, in particular Random Forest, provide the best attack detection accuracy, reaching 96.4% with AUC=0.98. In conditions of limited access to data labels, autoencoders are capable of performing the function of a reliable anomaly detector with a false positive rate of less than 5%.

The results confirm that machine learning effectively adapts to the characteristics of aviation protocols and can detect a wide range of attacks, including GPS signal spoofing, DoS, and false message injection. The models can be used in real time thanks to their high computational efficiency after the training phase. At the same time, the correct selection of features and sample balancing remain important factors, as the stability of the classifier directly depends on them. In the future, it seems reasonable to develop hybrid architectures combining detectors with and without a teacher, as well as to introduce distributed and federated learning technologies to ensure security in multi-agent aviation systems.

The results obtained can serve as a basis for the development of intelligent monitoring subsystems as part of digital twins of aviation systems, contributing to proactive cybersecurity in aviation.

The results obtained allow us to recommend a minimum set of five features that ensure high classification accuracy (>95%) and can be effectively integrated into aviation monitoring systems.

Features with low importance should not be excluded from the system architecture, as they may become critical in combined attacks or under conditions of limited information.

Feature importance analysis can be used to design digital twin systems in aviation that rely on highly informative parameters to predict status and detect threats.

References

1. Dutta, A., & Kant, S. (2020). An overview of cyber threat intelligence platform and role of artificial intelligence and machine learning. In Lecture Notes in Computer Science (p. 81). Springer Science+Business Media. https://doi.org/10.1007/978-3-030-65610-2_5

2. Katiyar, N., Tripathi, S., Kumar, P., Verma, M., Sahu, A. K., & Saxena, S. (2024, April). AI and cyber-security: Enhancing threat detection and response with machine learning. https://doi.org/10.53555/kuey.v30i4.2377

3. Mohammed, K. (2023, January). Harnessing the speed and accuracy of machine learning to advance cybersecurity. arXiv. https://doi.org/10.48550/arxiv.2302.12415

4. Mane, S., & Rao, D. J. (2021, January). Explaining network intrusion detection system using explainable AI framework. arXiv. https://doi.org/10.48550/arxiv.2103.07110

5. Mohamed, N. (2025, April). Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms. Knowledge and Information Systems. https://doi.org/10.1007/s10115-025-02429-y

6. Bountouni, N., Koussouris, S., Vasileiou, A. A., & Kazazis, S. A. (2023, April). A holistic framework for safeguarding of SMEs: A case study. https://doi.org/10.1109/drcn57075.2023.10108247

7. Chachra, A., & Sharma, D. (2019, January). Applications of machine learning algorithms for countermeasures to cyber attacks. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3370181

8. Goni, I., Bello, S., & Maigari, U. T. (2020, January 1). Machine learning algorithms applied to system security: A systematic review. Asian Journal of Applied Science and Technology, 4(3), 76. https://doi.org/10.38177/ajast.2020.4311

9. Mohamed, N., Taherdoost, H., & Madanchian, M. (2024, June). Comprehensive review of advanced machine learning techniques for detecting and mitigating zero-day exploits. ICST Transactions on Scalable Information Systems, 11. https://doi.org/10.4108/eetsis.6111

10. Strecker, S., Dave, R., Siddiqui, N., & Seliya, N. (2021, January). A modern analysis of aging machine learning based IoT cybersecurity methods. arXiv. https://doi.org/10.48550/arxiv.2110.07832

11. Kinyua, J., & Awuah, L. (2021, January). AI/ML in security orchestration, automation and response: Future research directions. Intelligent Automation & Soft Computing, 28(2), 527. https://doi.org/10.32604/iasc.2021.016240

12. Devine, S. M., & Bastian, N. D. (2019, January). Intelligent systems design for malware classification under adversarial conditions. arXiv. https://doi.org/10.48550/arxiv.1907.03149

13. Dini, P., Elhanashi, A., Begni, A., Saponara, S., Zheng, Q., & Gasmi, K. (2023, June). Overview on intrusion detection systems design exploiting machine learning for networking cybersecurity. Applied Sciences, 13(13), 7507. https://doi.org/10.3390/app13137507

14. Sameen, M., Han, K., & Hwang, S. O. (2020, January). PhishHaven—An efficient real-time AI phishing URLs detection system. IEEE Access, 8, 83425. https://doi.org/10.1109/access.2020.2991403

15. Stokes, J. W., Wang, D., Marinescu, M., Marino, M., & Bussone, B. (2017, January). Attack and defense of dynamic analysis-based, adversarial neural malware classification models. arXiv. https://doi.org/10.48550/arxiv.1712.05919

16. Sangani, N. K., & Zarger, H. (2017). Machine learning in application security. In InTech eBooks. https://doi.org/10.5772/intechopen.68796

17. Nicholls, J., Kuppa, A., & Le-Khac, N. (2021, January). Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. IEEE Access, 9, 163965. https://doi.org/10.1109/access.2021.3134076

18. Atlıoğlu, M. C., Bolat, M., Şahin, M., Tunalı, V., & Kılınç, D. (2020, September). Supervised learning approaches to flight delay prediction. Sakarya University Journal of Science, 24(6), 1223. https://doi.org/10.16984/saufenbilder.710107

19. Chukwunweike, J. N., Uchechukwu, J., & Kadiri, C. (2024, August). Enhancing maritime security through emerging technologies: The role of machine learning in cyber threat detection and mitigation. International Journal of Research Publication and Reviews, 5(8), 4121. https://doi.org/10.55248/gengpi.5.0824.2401

20. Talukder, M. A., et al. (2024, February). Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction. Journal of Big Data, 11(1). https://doi.org/10.1186/s40537-024-00886-w

21. Pan, E. (2024, March). Machine learning in financial transaction fraud detection and prevention. Transactions on Economics Business and Management Research, 5, 243. https://doi.org/10.62051/16r3aa10

22. Hernandez, C. S., Ayo, S., & Panagiotakopoulos, D. (2021, October). An explainable artificial intelligence (xAI) framework for improving trust in automated ATM tools. In 2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC) (p. 1). IEEE. https://doi.org/10.1109/DASC52595.2021.9594341

МАШИНАЛЫҚ ОҚУ ӘДІСТЕРІН ПАЙДАЛАНУ АРҚЫЛЫ АВИАЦИЯЛЫҚ ЖҮЙЕЛЕРДЕГІ КИБЕР ҚАУІПТЕРДІ АНЫҚТАУ

Аңдатпа. *Зерттеудің мақсаты авиациялық байланыс және навигациялық жүйелердегі киберқауіптерді анықтау үшін машиналық оқыту үлгілерін әзірлеу және бағалау болып табылады. Қазіргі заманғы авиациялық инфрақұрылымдар, соның ішінде ADS-B және ACARS хаттамалары, GPS спуфинг, DoS және жалған хабарлама инъекциясы сияқты шабуылдарға осал. Зерттеу 50 000 жазбадан тұратын біріктірілген деректер жиынтығын пайдаланады, оның 30% шабуылдарды модельдейді және 70% жүйенің қалыпты жұмысын көрсетеді.*

Әдістеме Random Forest, SVM және автокодер үлгілерін пайдалануды қамтиды. Қалыпқа келтіру және өлшемділікті азайтудан кейін (10 PCA құрамдастарына дейін) модельдер 5 еселік стратификацияланған кросс-валидацияны қолдану арқылы оқытылды және сынақтан өтті. Random Forest ең жақсы жіктеу дәлдігін көрсетті — 96,4%, F1-өлшемі 94,9%, Recall 95,1% және Precision 94,7%. SVM 91,2% дәлдікті көрсетті, ал автокодер 4,1% аспайтын жалған оң көрсеткішпен 92,3% сәтті шабуылды анықтауға қол жеткізді. ROC талдауына сәйкес, Random Forest моделінде AUC = 0,98 болды, ал Precision-Recall талдауы AP = 0,96 көрсетті.

Ғылыми жаңалық хаттамалардың ерекшеліктері мен уақытша ерекшеліктерін ескере отырып, нақты авиациялық сценарийлерге қолдану мүмкіндігі бойынша оқытушысы бар және оқытушысыз үлгілерді жүйелі түрде салыстыруда.

Тәжірибелік маңыздылығы оқытылатын үлгілерді әуе қозғалысын бақылау жүйелеріне және қауіпті ерте анықтау, ақаулар қаупін азайту және ұшу қауіпсіздігін арттыру үшін сандық борттық жүйелерге біріктіру мүмкіндігінде жатыр.

Түйін сөздер*: авиациялық киберқауіпсіздік, машиналық оқыту, басып кіруді анықтау, ADS-B, GPS спуфинг, автокодер, Random Forest.*

ВЫЯВЛЕНИЕ КИБЕРУГРОЗ В АВИАЦИОННЫХ СИСТЕМАХ С ПОМОЩЬЮ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ

Аннотация. *Целью исследования является разработка и оценка моделей машинного обучения для обнаружения киберугроз в системах связи и навигации в авиации. Современные авиационные инфраструктуры, включая протоколы ADS-B и ACARS, уязвимы для таких атак, как подделка GPS, DoS и вставка ложных сообщений. В исследовании используется комбинированный набор данных из 50 000 записей, из которых 30 % имитируют атаки, а 70 % представляют нормальную работу системы.*

Методология включает использование моделей Random Forest, SVM и автокодировщика. После нормализации и уменьшения размерности (до 10 компонентов PCA) модели были обучены и протестированы с помощью 5-кратной стратифицированной перекрестной проверки. Random Forest показал лучшую точность классификации — 96,4% с показателем F1 = 94,9%, Recall = 95,1% и Precision = 94,7%. SVM продемонстрировал точность 91,2%, а автокодер достиг 92,3% успешного

обнаружения атак с частотой ложных срабатываний не более 4,1%. Согласно ROC-анализу, модель Random Forest имела AUC = 0,98, а анализ Precision-Recall показал AP = 0,96.

Научная новизна заключается в систематическом сравнении моделей с учителем и без учителя с точки зрения их применимости к реальным авиационным сценариям с учетом специфики протоколов и временных особенностей.

Практическая значимость заключается в возможности интеграции обученных моделей в системы мониторинга воздушного движения и цифровые бортовые системы для раннего обнаружения угроз, минимизации риска сбоев и повышения безопасности полетов.

Ключевые слова: *кибербезопасность в авиации, машинное обучение, обнаружение вторжений, ADS-B, подделка GPS-сигналов, автокодировщик, Random Forest.*

Сведение об авторах

Бекетова Гулжанат Сакитжановна	Алматинский университет энергетики и связи имени Гумарбека Даукеева, кафедра - “IT-инженерия и искусственный интеллект”, должность – доцент, E-mail: g.beketova@aues.kz
Мусатаева Гульсим Толегеновна	Алматинский университет энергетики и связи имени Гумарбека Даукеева, кафедра - “IT-инженерия и искусственный интеллект”, должность – старший преподаватель, E-mail: g.musataeva@aues.kz
Жонкешова Айнагуль	International IT University, Алматы, Қазақстан, программист разработчик – Junior, E-mail: azhonkeshova@iitu.edu.kz
Аманбаев Абдрахман Абдиханович	Алматинский университет энергетики и связи имени Гумарбека Даукеева, кафедра - “IT-инженерия и искусственный интеллект”, должность – доцент, E-mail: a.amanbaev@aues.kz

Авторлар туралы мәлімет

Бекетова Гулжанат Сакитжановна	Ғұмарбек Дәукеев атындағы Алматы Энергетика және Байланыс Университеті, IT-инженерия және жасанды интеллект кафедрасы, лауазымы-доцент, E-mail: g.beketova@aues.kz
Мусатаева Гульсим Толегеновна	Ғұмарбек Дәукеев атындағы Алматы Энергетика және Байланыс Университеті, IT-инженерия және жасанды интеллект кафедрасы, лауазымы – аға оқытушы, E-mail: g.musataeva@aues.kz
Жонкешова Айнагуль	International IT University, Алматы, Қазақстан, бағдарламашы әзірлеуші – Junior, E-mail: azhonkeshova@iitu.edu.kz
Аманбаев Абдрахман Абдиханович	Ғұмарбек Дәукеев атындағы Алматы Энергетика және Байланыс Университеті, IT-инженерия және жасанды интеллект кафедрасы, лауазымы – аға оқытушы, E-mail: a.amanbaev@aues.kz

Information about the authors

Beketova Gulzhanat	Almaty University of Power Engineering and Telecommunications named after Gumarbek Daukeyev, Department - “IT engineering and Artificial Intelligence”, position - Associate Professor, E-mail: g.beketova@aues.kz
Musatayeva Gulsim Tolegenovna	Almaty University of Power Engineering and Telecommunications named after Gumarbek Daukeyev, Department - “IT engineering and Artificial Intelligence”, position - senior lecturer, E-mail: g.musataeva@aues.kz
Zhonkeshova Ainagul	International IT University, Almaty, Kazakhstan, Junior Software Developer,E-mail: azhonkeshova@iitu.edu.kz
Amanbayev Abdirakhman	Almaty University of Power Engineering and Telecommunications named after Gumarbek Daukeyev, Department - “IT engineering and Artificial Intelligence”, position - Associate Professor.E-mail: a.amanbaev@aues.kz