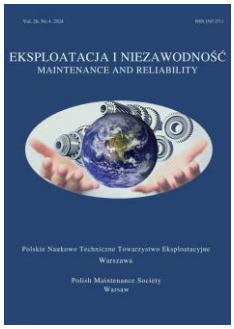


Eksploatacja i Niezawodnosc – Maintenance and Reliability

Volume 26 (2024), Issue 4

journal homepage: http://www.ein.org.pl

Article citation info:
Izdebski M, Michalska A, Jacyna-Gołda I, Gherman L, Prediction of cyber-attacks in air transport using neural networks, Eksploatacja i Niezawodnosc – Maintenance and Reliability 2024: 26(4) http://doi.org/10.17531/ein/191476

Prediction of cyber-attacks in air transport using neural networks

Indexed by:

Mariusz Izdebski[a,*], Anna Michalska[b], Ilona Jacyna-Gołda[a], Laurian Gherman[c]

[a] Warsaw University of Technology, Poland
[b] Polish Air Force University, Poland
[c] Henri Coandă Air Force Academy, Romania

Highlights

- Prediction cyber-attacks in air transport.
- Application of artificial intelligence tools in air transport.
- Determining the probability of cyber-attacks.
- Safety and reliability in air transport.

Abstract

This article addresses the topic of cyber-attacks in air transport, which is crucial for ensuring the safety and reliability of airports and air transport operations. The aim of the article was to present a new method for predicting cyber-attacks in air transport based on neural networks. The task of the neural network was to determine the multiple regression function based on which the probability of a cyberattack occurring at a specified hour and on a specific day of the week is predicted. The probability, depending on the time of the cyberattack occurrence, was determined using theoretical distributions. The method was verified with real data. Verification of the method confirmed its high effectiveness, determined at the level of 92%. The study examined the effectiveness of using the classical multiple regression method in predicting cyber-attacks in air transport. The classical multiple regression model covered only 0.14 of the input data, while the regression model generated by the neural network covered 0.99, indicating the high efficiency of the developed neural network.

Keywords
cyber-attacks, neural networks, air transport, prediction

1. Introduction

The research conducted in this article focuses on prediction cyber-attacks in air transport. This topic is crucial for ensuring the safety and reliability of airport operations and air transport [14].

In recent years, the development of information technologies and their integration into air transport systems have significantly increased the risk of cyber-attacks . Given the high criticality of aviation systems, it is necessary to develop effective methods for prediction cyber threats. One segment of the aviation industry that is frequently attacked is the information infrastructure [34], making it essential to predict such incidents and implement appropriate safeguards in IT systems.

The number of cyber-attacks is increasing worldwide, with a noticeable rise across various industries. In 2024, there was a significant increase, with some sectors experiencing a 221% growth compared to 2022 [35]. At the same time, the aviation sector is rapidly developing and will continue to do so. Recent estimates indicate that over the next 20 years, the demand for air transport will grow at an average annual rate of 4.3%.

(*) Corresponding author.
E-mail addresses: M. Izdebski (ORCID: 0000-0002-9157-7870) mariusz.izdebski@pw.edu.pl, A. Michalska (ORCID: 0000-0002-9292-589X) a.michalska@law.mil.pl, I. Jacyna-Gołda (ORCID: 0000-0001-8840-3127) ilona.golda@pw.edu.pl, L. Gherman (ORCID: 0000-0003-0315-629X) lauriang@gmail.com

According to ICAO (International Civil Aviation Organization), it is expected that by mid-2030, there will be no less than 200,000 flights taking off and landing daily worldwide [11]. Furthermore, one of the biggest trends in aviation is the digitization of all possible processes, from booking to aircraft maintenance [2], and the complete digitization of aviation ecosystems such as Airport 3.0: Smart Airports [1].

All of this makes air transport increasingly vulnerable to cyber-attacks. A review conducted in the study [34] covers 22 cyber-attacks on aviation from 2001 to 2021. Additionally, in 2023-2024, four out of six significant cyber incidents related to airports were reported [7]. The aviation industry is highly risky and becomes a target for hackers because it is perceived as an easy target [29]. Further studies show that most airports have limited resources dedicated to cyber protection and resilience [28]. This situation underscores the urgent need to enhance cyber resilience and protection measures in the aviation sector.

The trends and challenges in aviation system security mainly involve considerations of cybersecurity [36, 10]. Most research related to aviation cybersecurity focuses on specific types of threats or the cybersecurity process [21, 20]. However, there are several different approaches to the topic of cybersecurity in aviation. In the study [23], the authors focused on IoT in aviation and conducted an assessment of various security measures for smart airports, emphasizing the importance of new AI-based cyber defense techniques. Only a few studies address mathematical prediction models and primarily rely on specific prediction scenarios [22]. In the study [32], the authors used simulation models to study the behavior of air traffic networks in the face of environmental and cyber threats. Few studies focus on risk management, for example, the authors in the study [33] created a mathematical model of the cyber risk management process in an enterprise based on Fourier series. Risk management in critical infrastructure (including airports) concerning cyber threats using a game theory-based model is described in studies [6, 27, 13].

The main objective of the undertaken research was to develop a method for prediction cyber-attacks in air transport. The first stage of the method is to determine the probability of a cyberattack occurring at a specific hour of the day. In the second stage, a multiple regression function is determined, taking into account not only the hour of the attack but also the day of the week and the week of the month when the attack occurs. The value of the regression function is the probability of a cyberattack. The parameters of the regression function were determined based on a neural network. The developed method was verified with real data, confirming its effectiveness.

The work is divided into five chapters. The first chapter describes the research problem and the objective of the conducted research. The second chapter identifies the research gap and the rationale for the topic. The method for prediction cyber-attacks in air transport is presented in the third chapter. The verification of the developed method with real data is described in the fourth chapter. The summary of the research is presented in the fifth chapter.

2. Predicting Cyber-attacks in Air Transport - a literature review

In this literature review, the key achievements in the field of cyber threat prediction in air transport are presented, with an emphasis on methods for predicting these events.

The authors in work [12] presented a comprehensive analysis of cyber threats in the aviation industry. The article discusses specific threats to aviation systems and proposes methods for predicting attacks based on historical data and trends analysis. The authors in publication [18] present advanced methods for prediction cyber-attacks using machine learning techniques. The study introduces a predictive model that analyzes various patterns that may indicate future cyber-attacks . This model is highly effective in detecting potential threats. Detection of cyber threats in the airspace by the ADS-B (Automatic Dependent Surveillance-Broadcast) system is presented in work [31]. The described system enables the identification of potential security vulnerabilities and the development of strategies to address them.

Publication [38] discusses the application of machine learning algorithms to forecast cyber-attacks . The research indicates the effectiveness of methods such as decision trees and neural networks in identifying patterns related to cyber-attacks. The article emphasizes the importance of continuous monitoring and data analysis for the rapid detection and response to threats. The use of deep learning techniques for detecting cyber-attacks in aviation systems is presented in publication [3]. The authors introduced an anomaly detection

model based on neural networks, which is capable of effectively identifying unusual behaviors indicating potential cyber-attacks . This work contributes to improving the security of aviation systems through early threat detection. The application of deep machine learning for prediction cyber-attacks in the aviation sector is presented in publications [37, 5, 9]. The use of hybrid machine learning models for predicting cyber threats is discussed in publication [30]. The authors explained how combining different algorithms can increase the effectiveness of predicting cyber-attacks.

The authors in work [4] studied the application of Bayesian networks for predicting cyber-attacks. They presented a probabilistic model that assesses the risk of cyber-attacks based on various operational factors and historical threat data. The application of time series analysis for predicting cyber-attacks is presented in publication [8]. The authors proposed a multidimensional cyber-attack detection model called the Contextual Auto-Encoder (CAE). Verification confirmed the high effectiveness of the developed model. Work [24] proposed the use of data mining techniques to forecast cyber threats. It discussed how techniques such as clustering and classification can be used to analyze operational data and detect threat patterns.

The authors in work [26] present the application of genetic algorithms for predicting cyber threats. The study defined ways of mathematically modeling cybersecurity management in the aviation industry. The application of fuzzy logic for predicting cyber-attacks is presented in work [19]. The authors discussed how fuzzy models can be used to assess risk and forecast cyber threats in aviation systems.

In summary, prediction cyber-attacks in air transport is a dynamically developing field, where advanced data analysis and machine learning methods are crucial. Various types of artificial intelligence algorithms are recommended in this area. It should be noted that the authors of the study did not find research focusing on predicting the timing of potential cyber-attacks in the aviation sector. This could be crucial for decision-makers in supporting the protection system at the moment of greatest attack threat. The literature review indicated that prediction cyber threats is presented in a general way, without precisely specifying the timing of the event. The occurrence of a cyber-attack is a random event, so it is advisable to determine the probability of these events occurring, which is often overlooked in publications. This publication fills these research gaps in the field of cyberattack prediction in the aviation sector.

3. The method of forecasting cyber-attacks in air transport

The developed method for forecasting cyber-attacks in air transport determines the probability of an undesirable event occurring, such as cyber-attacks on IT systems used in air transport. The likelihood of a cyber-attack is defined for a given hour, a specific day of the week on which attacks occur, and each week of the month. The method is based on determining a multiple regression function, where the explanatory variables are the hour of the attack, the day of the week, and the week of the month. In contrast, the explained variable is the probability of the attack. The cyberattack forecasting method uses a neural network to develop a regression model determining the probability of a cyberattack occurring. The method can be presented in the following steps, Fig.1:

- Step 1. Entering input data, i.e., the moment of the cyber-attack on each day of the week and specifying the week in which the event occurred.
- Step 2. Determining the theoretical probability of a cyber-attack for individual days of the week. The random variable of the distribution is the moment of occurrence of a cyber-attack on a given day. The theoretical probabilities of the distributions will be determined by matching the theoretical distributions to emFpirical measurements [15, 16].
- Step 3. Using a neural network to determine a multiple regression model taking into account the input variables: x1 - a moment of the cyber-attack on a given day, e.g., 8:00, x2 - day of the week, e.g., Tuesday, x3 - number of the week in the month in which the attack occurred, e.g., the first week. The output variable Y is the probability of a cyber-attack.
- Step 4. Verification of the developed method. The method was verified by comparing its results with those of the classic multiple regression model.

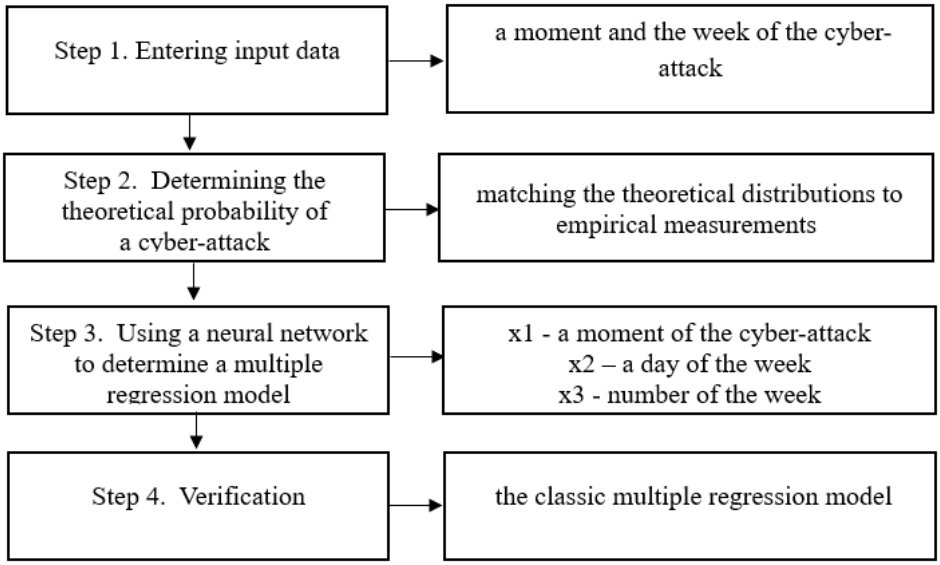


Fig. 1. The method of forecasting cyber-attacks in air transport.

The general interpretation of the neural network in the problem of forecasting cyber-attacks in rail transport, taking into account the input and output variables, is shown in Fig. 2. The detailed neural network with the type of activation function for individual neurons and the number of neurons in the hidden layer of the algorithm will be known after the network training process.

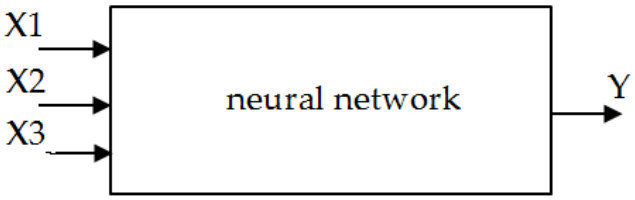


Fig. 2. Input and output variables of the neural network.

In turn, the process of matching theoretical distributions to empirical measurements is carried out based on verifying the null hypothesis regarding the adopted distribution [17, 25].

4. Verification of the method

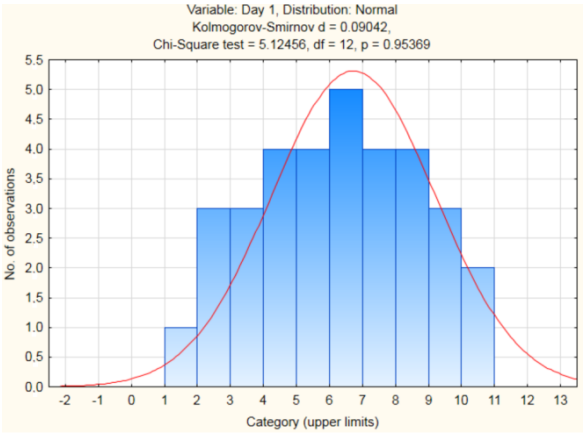
4.1. Fitting theoretical distributions to measured data

Table 1 shows the moments of cyber-attacks in air transport occurring in air traffic management IT systems at specific hours of the day for each day of the week in the first week of the selected month. Data were collected for four weeks of attack observations. The frequency and timing of attacks in the second, third, and fourth weeks were the same, so they are not presented in Table 1 [H – hour, A – attack, e.g., the record 1/0 is interpreted as no attack at 1:00 - 1:59, while the record 4/7 means seven attacks at 4:00 - 4:59].

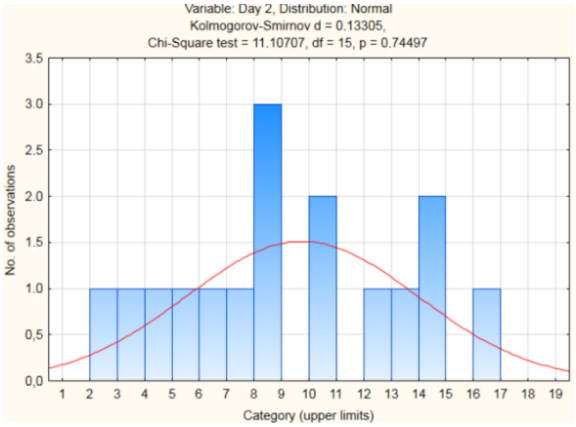
Table 1. Weekly cyber-attack moments.

Week	Day	H/A	H/A	H/A	H/A	H/A	H/A	H/A	H/A	H/A	H/A	H/A	H/A
1	1	1/0	2/1	3/3	4/3	5/4	6/4	7/5	8/4	9/4	10/3	11/2	12/0
1	1	13/0	14/0	15/0	16/0	17/0	18/0	19/0	20/0	21/0	22/0	23/0	24/0
1	2	1/0	2/0	3/1	4/1	5/1	6/1	7/1	8/1	9/3	10/0	11/2	12/1
1	2	13/1	14/2	15/0	16/1	17/0	18/0	19/0	20/0	21/0	22/0	23/0	24/0
1	3	1/0	2/0	3/0	4/0	5/0	6/0	7/0	8/0	9/0	10/0	11/1	12/1
1	3	13/1	14/2	15/2	16/3	17/3	18/2	19/2	20/1	21/1	22/0	23/0	24/0
1	4	1/1	2/1	3/1	4/1	5/2	6/4	7/4	8/2	9/2	10/1	11/1	12/1
1	4	13/1	14/1	15/2	16/3	17/3	18/2	19/2	20/1	21/1	22/0	23/0	24/0
1	5	1/0	2/0	3/0	4/0	5/0	6/0	7/0	8/1	9/1	10/1	11/1	12/2
1	5	13/2	14/2	15/3	16/3	17/2	18/2	19/1	20/1	21/1	22/1	23/0	24/0
1	6	1/0	2/0	3/0	4/0	5/0	6/0	7/0	8/0	9/0	10/0	11/1	12/2
1	6	13/1	14/1	15/2	16/3	17/3	18/2	19/1	20/1	21/1	22/1	23/0	24/0
1	7	1/0	2/0	3/0	4/1	5/1	6/1	7/1	8/1	9/1	10/2	11/3	12/2
1	7	13/2	14/1	15/1	16/1	17/1	18/1	19/0	20/0	21/0	22/0	23/0	24/0

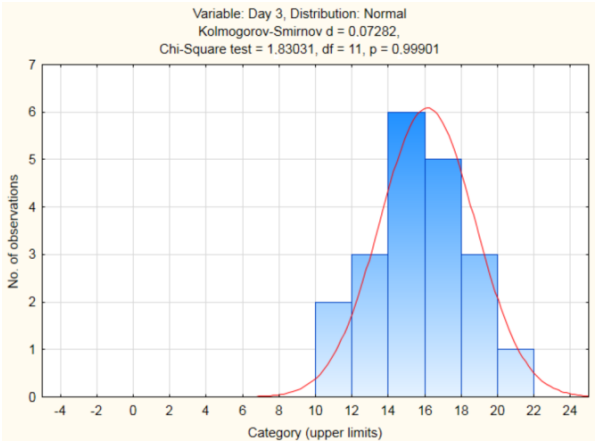
The shape of the histograms determining the frequency of cyber-attacks is similar to normal distributions, so the Ch-square and Kolmogorov-Smirnov tests were used to determine the type of distribution. The null hypothesis about the assumed type of distribution is rejected when the calculated value of the statistics belongs to the critical area specified by the adopted significance level $\alpha = 0.05$ (when $p < \alpha$, p - probability determined in the tests). The values of the Chi-square and Kolmogorov-Smirnov goodness-of-fit tests and the parameters of the tested distributions are presented in Table 2. The fits of the theoretical distributions of the random variable of cyber-attacks in the first week of the month are shown in Fig. 3. The values of the probability of a cyberattack occurring in individual hours of the day in the first week of the month are presented in Table 3 [H – hour, P – the probability].



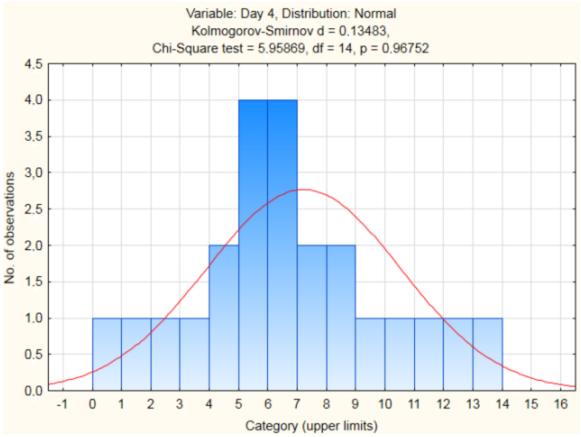
(**a**)



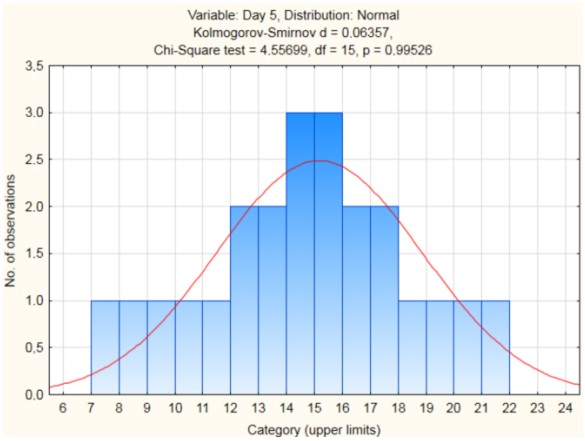
(**b**)



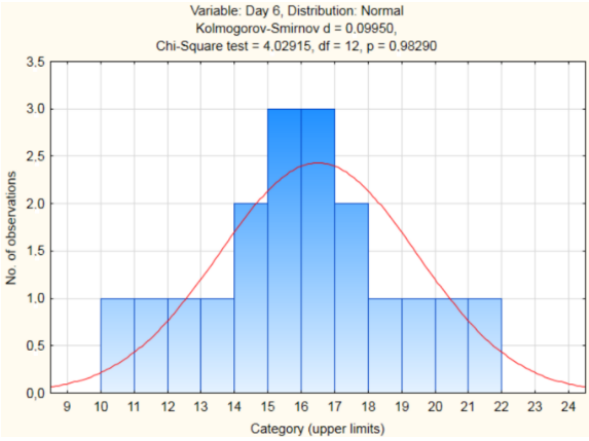
(**c**)



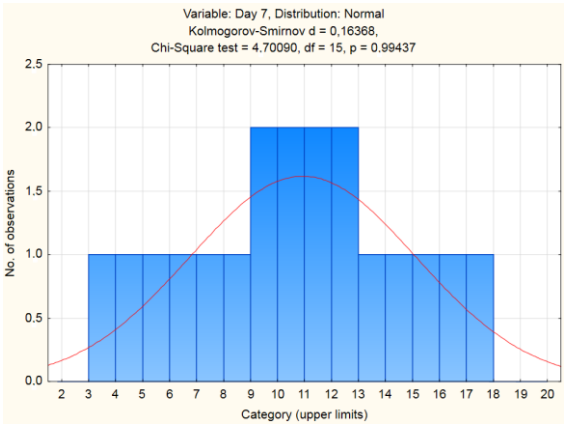
(**d**)



(**e**)



(**f**)



(g)

Fig. 3. Theoretical distributions of cyber-attacks a) day 1, b) day 2, c) day 3, d) day 4, e) day 5, f) day 6, g) day 7.

Table 2. Compliance tests and decomposition parameters.

Day	Statistics	Ch-square test	Statistics	K-S test	Distribution parameters	Distribution
1	5.124	0.9536	0.09	-	μ=6.72; s^2=6.14	normal
2	11.107	0.7449	0.13	-	μ=9.75; s^2=17.8	normal
3	1.830	0.9990	0.07	-	μ=16.15; s^2=6.87	normal
4	5.9586	0.9675	0.13	-	μ=7.21; s^2=10.99	normal
5	4.5569	0.9952	0.06	-	μ=15.17; s^2=13.60	normal
6	4.0291	0.9829	0.09	-	μ=16.5; s^2=8.73	normal
7	4.7009	0.9943	0.16	-	μ=10.94; s^2=15.55	normal

Table 3. The theoretical probability of a cyber-attack occurring at a given hour of the day [H/P].

Day 1	Day 2	Day 3	Day 4	Day 5	Day 6	Day 7
1/0.04	1/0.02	1/0.01	1/0.03	1/0.02	1/0.01	1/0.02
2/0.05	2/0.02	2/0.01	2/0.03	2/0.02	2/0.01	2/0.02
3/0.05	3/0.02	3/0.01	3/0.03	3/0.02	3/0.01	3/0.02
4/0.06	4/0.02	4/0.01	4/0.03	4/0.02	4/0.02	4/0.02
5/0.06	5/0.02	5/0.02	5/0.04	5/0.02	5/0.02	5/0.02
6/0.06	6/0.02	6/0.02	6/0.04	6/0.02	6/0.02	6/0.02
7/0.06	7/0.02	7/0.02	7/0.04	7/0.02	7/0.03	7/0.02
8/0.06	8/0.02	8/0.03	8/0.04	8/0.03	8/0.03	8/0.03
9/0.06	9/0.02	9/0.03	9/0.03	9/0.03	9/0.03	9/0.03
10/0.06	10/0.02	10/0.04	10/0.04	10/0.03	10/0.03	10/0.03
11/0.05	11/0.02	11/0.04	11/0.03	11/0.03	11/0.04	11/0.03
12/0.04	12/0.02	12/0.05	12/0.03	12/0.03	12/0.04	12/0.03
13/0.04	13/0.02	13/0.05	13/0.03	13/0.03	13/0.04	13/0.03
14/0.03	14/0.02	14/0.06	14/0.03	14/0.03	14/0.04	14/0.03
15/0.03	15/0.02	15/0.06	15/0.03	15/0.03	15/0.05	15/0.02
16/0.02	16/0.02	16/0.06	16/0.03	16/0.03	16/0.05	16/0.02
17/0.02	17/0.02	17/0.06	17/0.02	17/0.03	17/0.05	17/0.02
18/0.01	18/0.02	18/0.06	18/0.02	18/0.03	18/0.05	18/0.02
19/0.01	19/0.02	19/0.05	19/0.02	19/0.03	19/0.04	19/0.02
20/0.01	20/0.02	20/0.05	20/0.02	20/0.03	20/0.04	20/0.02
21/0.00	21/0.02	21/0.05	21/0.02	21/0.03	21/0.04	21/0.02
22/0.00	22/0.02	22/0.04	22/0.01	22/0.03	22/0.04	22/0.02
23/0.00	23/0.02	23/0.04	23/0.01	23/0.02	23/0.03	23/0.02
24/0.00	24/0.02	24/0.03	24/0.01	24/0.02	24/0.03	24/0.02

4.2. Forecasting cyber-attacks using a neural network

The process of training neural networks was carried out using Statistica 13 software. An MLP neural network with three inputs, seven hidden neurons, and one output was selected to determine the multiple regression model. The BFGS algorithm was used

in the learning process. The activation function for hidden neurons is a logistic function, while the activation function for the output neuron is exponential. The mathematical notation of the activation function for individual neurons is presented as follows:

Activation function for the first neuron:

$$N1 = \frac{1}{1-e^{0.0008 \cdot x1+1.2029 \cdot x2-1.0529 \cdot x3+0.07}} \quad (1)$$

Activation function for the second neuron:

$$N2 = \frac{1}{1-e^{0.0015 \cdot x1-14.2765 \cdot x2-2.6236 \cdot x3+5.024}} \quad (2)$$

Activation function for the third neuron:

$$N3 = \frac{1}{1-e^{-0.0030 \cdot x1-4.2487 \cdot x2-2.0854 \cdot x3+5.482}} \quad (3)$$

Activation function for the fourth neuron:

$$N4 = \frac{1}{1-e^{0.05 \cdot x1-8.2862 \cdot x2-3.1648 \cdot x3+3.1226}} \quad (4)$$

Activation function for the fifth neuron:

$$N5 = \frac{1}{1-e^{-0.0021 \cdot x1-1.1473 \cdot x2-1.1473 \cdot x3+3.2253}} \quad (5)$$

Activation function for the sixth neuron:

$$N6 = \frac{1}{1-e^{0.0330 \cdot x1-21.8348 \cdot x2-4.9094 \cdot x3+23.5154}} \quad (6)$$

Activation function for the seventh neuron:

$$N7 = \frac{1}{1-e^{0.0032 \cdot x1-37.2559 \cdot x2-0.3819 \cdot x3+11.8777}} \quad (7)$$

The output neuron function takes the form of an exponential function:

$$Y = e^{-20.1366 \cdot N1-16.8444 \cdot N2-19.8678 \cdot N3+8.9169 \cdot N4+22.7823 \cdot N5-3.0222 \cdot N6+6.2954 \cdot N7+9.0291} \quad (8)$$

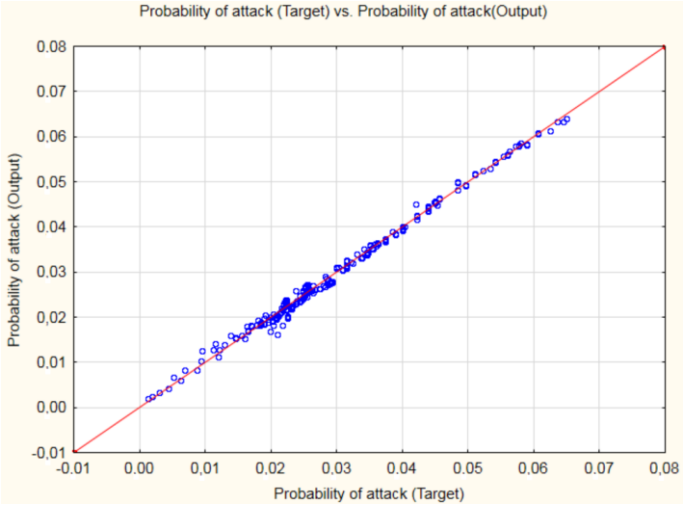


Fig. 4. Adjusting the neural network forecast to the training data

A graphical presentation of the fit of the attack probability generated by the MLP 3-7-1 networks (output) to the attack probability generated using theoretical distributions (target) is shown in Fig. 4, while sample results for one day of the week are presented in Table 4. Matching the network results to training data was set at 0.99.

Tabel 4. Operation of the neural network.

Week	Day	Hour	Target	Output
1	4	1	0.03	0.03
1	4	2	0.03	0.03
1	4	3	0.03	0.03
1	4	4	0.03	0.03
1	4	5	0.03	0.03
1	4	6	-	-
1	4	7	-	-
1	4	8	0.03	0.03
1	4	9	-	-
1	4	10	0.03	0.03
1	4	11	0.03	0.03
1	4	12	-	-
1	4	13	0.03	0.03
1	4	14	0.02	0.03
1	4	15	-	-
1	4	16	0.02	0.02
1	4	17	-	-
1	4	18	0.02	0.02
1	4	19	0.02	0.02
1	4	20	0.01	0.01
1	4	21	0.01	0.01
1	4	22	0.01	0.01
1	4	23	0.01	0.01
1	4	24	0.01	0.01

4.3. Verification of the neural network using multiple regression

To verify the prediction of cyberattack probability based on neural networks, a multiple regression function defining cyberattack determined based on the classical regression model was developed. The regression function is presented as:

$$Y = -0.038 \cdot x2 + 0.033 \quad (9)$$

Based on formula (9), it can be seen that the probability of a cyberattack depends only on the variable x2 with the interpretation of the day of the attack. The remaining variables, x1 and x3, with the interpretation of the week in which the attack occurred and the moment of the attack, are not statistically significant, so they were not included in the

regression model. The multiple regression fit was determined at a low level of 0.14, confirmed by the residual analysis presented in Fig. 5, where a large scatter of residual values from the predicted probability of a cyberattack can be seen. The comparison of the results generated by multiple regression with the neural network was not performed due to the deficient data fit coefficient achieved by the regressions.

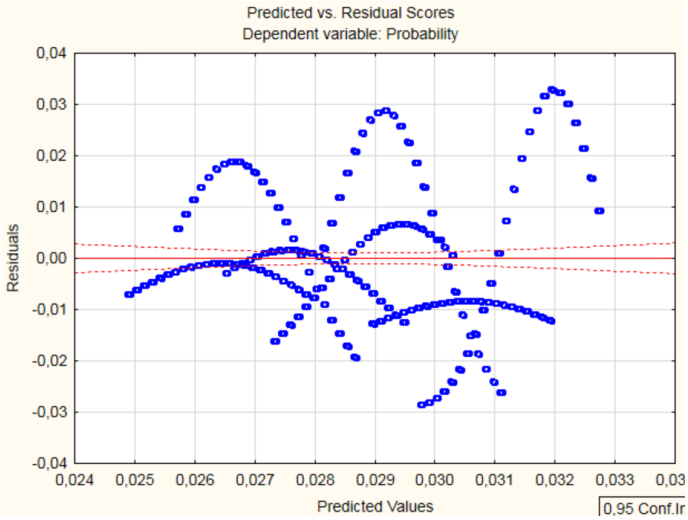


Fig 5. Fitting a multiple regression model to measured data.

The verification of the neural network is presented in Table 5. The table shows the hours of the cyberattack for the first week of the following month (other than the training sample), along with the calculated probability of the attack by the neural network. Verifying the correctness of the neural network operation consisted of comparing the likelihood of the cyberattack with the actual event (attack). Based on Table 1 and Table 3, threshold values of the probability of the cyberattack were determined, i.e., the probability on the first day of the week was set at 0.05, on the second day at 0.02, on the third day at 0.04, on the fourth day at 0.03, on the fifth day at 0.03, on the sixth day at 0.04 and the seventh day at 0.02. It is assumed that the cyberattack will occur after reaching and exceeding these probability values. The occurrence of a cyberattack, with probability values below the threshold values determined by the neural network, indicates an error in applying the method (P - probability, W - verification). In the case of correct neural network verification, the verification status "yes" is entered; in the case of incorrect verification, "no" The verification of the method confirmed its effectiveness at 92%. For example, for the record 14/1 defining the occurrence of cyber-attacks on the first day of the week at 14:00 - 14:59, the probability of a cyberattack generated by the network was 0.02, which is lower than the limit of 0.05, after which a cyberattack occurs. Theoretically, a cyberattack should not have happened at such a probability level, but it did. This indicates an error in the method.

Table 5. Neural network verification.

Hour/Day I	Hour/Day II	P I	P II	W I	W II
1/1	1/2	0.09	0.06	yes	yes
2/1	2/2	0.08	0.03	yes	yes
3/2	3/2	0.04	0.03	yes	yes
4/2	4/2	0.03	0.03	yes	yes
5/3	5/3	0.02	0.04	**no**	yes
6/3	6/3	0.04	0.04	yes	yes
7/3	7/3	0.05	0.04	yes	yes
8/3	8/3	0.04	0.07	yes	yes
9/4	9/4	0.06	0.07	yes	yes
10/1	2/4	0.06	0.08	yes	yes
11/1	3/4	0.04	0.08	**no**	yes
12/1	4/4	0.07	0.06	yes	yes
13/1	5/4	0.07	0.07	yes	yes
14/2	14/4	0.03	0.07	**no**	yes
15/1	15/4	0.08	0.08	yes	yes
16/2	16/3	0.06	0.07	yes	yes
17/2	17/3	0.06	0.06	yes	yes
18/2	18/3	0.06	0.08	yes	yes
19/2	19/3	0.05	0.08	yes	yes
20/2	20/3	0.05	0.05	yes	yes
21/2	21/3	0.05	0.03	yes	**no**
22/2	22/3	0.04	0.03	yes	**no**
23/1	23/2	0.04	0.06	yes	yes
24/1	24/2	0.03	0.06	yes	yes
14/1	15/2	0.02	0.05	**no**	yes

5. Conclusion

The conducted research aimed to develop an effective method for forecasting cyber-attacks in air transport. The process is based on a multiple regression model, where the input data of the function are the day of the attack, the hour of the attack, and a specific week of the month. The regression function determines the probability of a cyberattack occurring at a particular hour of the day and a given week of the month. A neural network determined the regression model parameters. The neural network operation was verified using the classical multiple regression method, which is widely described in statistics. The fit of the cyberattack probability generated by the neural network to the training data was 0.99, while the fit of the classical regression method was 0.14. Considering the above, in the problem of forecasting cyber-attacks, the neural network is a more effective tool than the classical regression method.

Verifying the method based on accurate data confirmed its

effectiveness at 92%. To improve the method's effectiveness, it is necessary to determine more precisely the theoretical probabilities of a cyberattack based on which the neural network performs the learning process. It should be emphasized that the normal distribution of the likelihood of a cyberattack occurring each day of the week was assumed. Verifying other types of distributions is a further direction of research to improve the method's effectiveness. Additionally, it is suggested that other artificial intelligence techniques, e.g., fuzzy sets, be checked and their efficacy in forecasting cyber-attacks in air transport.

In practice, the obtained research results can be used, for example, by air transport operators to plan aircraft flight schedules and designate flights in periods where the risk of cyberattack is minimal. Additionally, the developed method can support operators in managing safety on the airport apron by minimizing the risk of attacks on the management system of ground service vehicles or aircraft routes.

References

1. Alansari Z, Soomro S, Belgaum MR. Smart Airports: Review and Open Research Issues. In: Miraz, M., Excell, P., Ware, A., Soomro, S., Ali, M. (eds) Emerging Technologies in Computing. iCETiC 2019. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 285. Springer, Cham. https://doi.org/10.1007/978-3-030-23943-5_10.
2. Alomar I, Yatskiv I. Digitalization in aircraft maintenance processes. Aviation 2023; 27(2): 86-94, https://doi.org/10.3846/aviation.2023.18923.
3. Basora L, Olive X, Dubot T. Recent Advances in Anomaly Detection Methods Applied to Aviation. Aerospace 2019; 6(11): 117, https://doi.org/10.3390/aerospace6110117.
4. Bauranov A, Rakas J. Bayesian network model of aviation safety: Impact of new communication technologies on mid-air collisions. Reliability Engineering & System Safety 2024; 243: 109905, https://doi.org/10.1016/j.ress.2023.109905.
5. Cai K, Li Y, Fang YP, Zhu Y. A Deep Learning Approach for Flight Delay Prediction Through Time-Evolving Graphs. IEEE Transactions on Intelligent Transportation Systems 2022; 23(8): 11397-11407, https://doi.org/10.1109/TITS.2021.3103502.
6. Cano J, Pollini A, Falciani L, Turhan U. Modeling current and emerging threats in the airport domain through adversarial risk analysis. J Risk Res. 2016; 19(7): 894-912, https://doi.org/10.1080/13669877.2015.1057201.
7. Center for Strategic and International Studies (CSIS). Significant Cyber Incidents Since 2006 [Internet]. https://csis-website-prod.s3.amazonaws.com/s3fs-public/202406/240607_Significant_Cyber_Events.pdf?VersionId=E3Y46OOqM9GsO4KNWizmvg7aA2NYZ2a6.
8. Chevrot A, Vernotte A, Legeard B. CEA: Contextual auto-encoder for multivariate time-series anomaly detection in air transportation. Computers & Security 2022; 116: 102652, https://doi.org/10.1016/j.cose.2022.102652.
9. Dangut MD, Jennions IK, King S, Skaf Z. Application of deep reinforcement learning for extremely rare failure prediction in aircraft maintenance. Mechanical Systems and Signal Processing 2022; 171: 108873, https://doi.org/10.1016/j.ymssp.2022.108873.
10. Fakeeh KA. An Analysis of Airports Cyber-Security. Communications on Applied Electronics 2016; 4(7): 11-15, https://doi.org/10.5120/cae2016652129.
11. Future of Aviation. ICAO [Internet], https://www.icao.int/Meetings/FutureOfAviation/Pages/default.aspx.
12. Gaurav D, Gaurav Choudhary V, Sihag IY, Kim-Kwang RC. Cyber security challenges in aviation communication, navigation, and surveillance. Computers & Security 2022; 112: 102516, https://doi.org/10.1016/j.cose.2021.102516.
13. Gençoğlu MT. Mathematical Modeling of Cyber Attack and Defense. Bilgisayar Bilimleri ve Teknolojileri Dergisi 2022; 3(1): 10-16, https://doi.org/10.54047/bibted.997908.
14. Gołda P, Zawisza T, Izdebski M. Evaluation of efficiency and reliability of airport processes using simulation tools. Eksploatacja i Niezawodnosc – Maintenance and Reliability 2021; 23 (4): 659–669, http://doi.org/10.17531/ein.2021.4.8.
15. Izdebski M, Jacyna M, Bogdański J. Minimisation of the Energy Expenditure of Electric Vehicles in Municipal Service Companies, Taking into Account the Uncertainty of Charging Point Operation. Energies 2024; 17(9): 2179, https://doi.org/10.3390/en17092179.
16. Izdebski M, Jacyna-Gołda I, Gołda P. Minimisation of the probability of serious road accidents in the transport of dangerous goods. Reliability Engineering & System Safety 2022; 217: 108093, https://doi.org/10.1016/j.ress.2021.108093.
17. Izdebski, M. Risk management in the allocation of vehicles to tasks in transport companies using a heuristic algorithm. Archives of

Transport 2023; 67(3): 139-153. https://doi.org/10.5604/01.3001.0053.7463.

18. Jamal M, Ashraf H, Jhanjhi N. Machine Learning-based Aircraft Conflict Prediction: A Systematic Literature Review. Preprints 2023; 2023121600, https://doi.org/10.20944/preprints202312.1600.v1.
19. Jana DK, Ghosh R. Novel interval type-2 fuzzy logic controller for improving risk assessment model of cyber security, Journal of Information Security and Applications 2018; 40: 173-182, https://doi.org/10.1016/j.jisa.2018.04.002.
20. Jang-Jaccard J, Nepal S. A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences 2014; 80(5): 973-993, https://doi.org/10.1016/j.jcss.2014.02.005.
21. Karpiuk M, Kelemen M. Cybersecurity in civil aviation in Poland and Slovakia. Cybersecurity Law. 2022; 8(2): 70-83, https://doi.org/10.35467/cal/157125.
22. Koch T, Moller DPF, Deutschmann A, Milbredt O. Model-based airport security analysis in case of blackouts or cyber-attacks. IEEE International Conference on Electro Information Technology (EIT) 2017; Lincoln, NE, USA 14-17 May 2017, 2154-0373, https://doi.org/10.1109/EIT.2017.8053346.
23. Koroniotis N, Moustafa N, Schiliro F, Gauravaram P, Janicke H. A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports. IEEE Access. 2020; 8:209802-209834, https://doi.org/10.1109/ACCESS.2020.3036728.
24. Koroniotis N, Moustafa N, Schiliro F, Gauravaram P, Janicke H. A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports. IEEE Access 2020; 8: 209802-209834, https://doi.org/10.1109/ACCESS.2020.3036728.
25. Kozłowski E, Borucka A, Oleszczuk P, Jałowiec T, Evaluation of the maintenance system readiness using the semi-Markov model taking into account hidden factors, Eksploatacja i Niezawodnosc – Maintenance and Reliability 2023: 25(4), http://doi.org/10.17531/ein/172857
26. Kuznietsova T, Chyrkov A. Angstromtechnology of aviation cybersecurity. Ukrainian Scientific Journal of Information Security 2020; 26(1): 28-34. https://doi.org/10.18372/2225-5036.26.14667.
27. Majeed K, Masood Z, Ghori MR, Raja MAZ. Design and analysis of cyber warfare model with intelligent predictive stochastic networks for attack–defend strategies on critical infrastructures. Appl Soft Comput. 2023; 148: 110847, https://doi.org/10.1016/j.asoc.2023.110847.
28. Malhotra O, Dey S, Foo E, Helbig M. Cyber Security Maturity Model Capability at The Airports. ACIS 2021; 55.
29. Meyer S. Airline Data Breaches Worrying - CPO Magazine 2018, https://www.cpomagazine.com/cyber-security/airline-data-breaches-worrying/.
30. Nassar A, Kamal M. Machine Learning and Big Data Analytics for Cybersecurity Threat Detection: A Holistic Review of Techniques and Case Studies. Journal of Artificial Intelligence and Machine Learning in Management 2021; 5(1): 51-63. https://doi.org/10.1007/978-3-030-57024-8.
31. Ray G, Ray J. Detecting ADS-B replay cyber-attacks in the national airspace system. Issues in Information Systems 2023; 24(1): 170-185, https://doi.org/10.48009/1_iis_2023_115.
32. Roy S, Tamimi A, Hahn A, Xue M, Das S, Vosughi A, Varnick S. A Modeling Framework for Assessing Cyber Disruptions and Attacks to the National Airspace System. AIAA Modeling and Simulation Technologies Conference. Kissimmee, Florida: American Institute of Aeronautics and Astronautics 2018, https://doi.org/10.2514/6.2018-0109.
33. Sobchuk V, Barabash O, Musienko A, Tsyganivska I, Kurylko O. Mathematical Model of Cyber Risks Management Based on the Expansion of Piecewise Continuous Analytical Approximation Functions of Cyber-attacks in the Fourier Series. Axioms 2023; 12(10): 924, https://doi.org/10.3390/axioms12100924.
34. Ukwandu E, Ben-Farah MA, Hindy H, Bures M, Atkinson R, Tachtatzis C, Andonovic I, Bellekens X. Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. Information 2022; 13(3): 146, https://doi.org/10.3390/info13030146.
35. Wåhlén M, Fahlström P, Näslund A. Threat Intelligence Report 2024 [Internet]. Truesec; Report No.: 1, https://insights.truesec.com/hub/report/truesec-threat-intelligence-report-2024.
36. Zalewski J, Kornecki A. Trends and challenges in the aviation systems safety and cybersecurity. TASK Q. 2019; 23(2):159-175, https://doi.org/10.17466/tq2019/23.2/a
37. Zhang J, Pan L, Han QL, Chen C, Wen S, and Y. Xiang Y. Deep Learning Based Attack Detection for Cyber-Physical System Cybersecurity: A Survey. IEEE/CAA Journal of Automatica Sinica 2022; 9(3): 377-391, https://doi.org/10.1109/JAS.2021.1004261.
38. Zhang X, Mahadevan S. Ensemble machine learning models for aviation incident risk prediction. Decision Support Systems 2019; 116:

48-63, https://doi.org/10.1016/j.dss.2018.10.009.