Transport and Telecommunication, 2026, volume 27, no. 2, 204-213
Transport and Telecommunication Institute, Lauvas 2, Riga, LV-1019, Latvia
DOI 10.2478/ttj-2026-0015

RESEARCH OF SOME HAZARD FACTORS AND INTENSITY OF A SET SECURITY EVENTS IN THE TELECOMMUNICATION SYSTEM

Bayram Ibrahimov[1], Islam Islamov[2]

[1]Department of Radio Electronic and Aerospace Systems, Azerbaijan Technical University
Baku, Azerbaijan, H. Javid ave. 25, AZ 1073
i.bayram@mail.ru
[2]Department of Automation, Telecommunications and Energy, Baku Engineering University
Baku, Azerbaijan, Hasan Aliyev str., 120, AZ0101
isislamov@beu.edu.az

The article considers the tasks of the study and analysis some factors danger and intensity of a set of security events in multiservice local and corporate public communication networks. Based on the study, a new approach is proposed for creating a mathematical model danger and intensity of a set security events in multiservice telecommunications networks under the threat of subscriber and network unauthorized access. As a result of the study, analytical formulas were obtained for the formal dependence integrated criteria for the quality of indication as single and multiple security events and hazard factors with a parameter, components of the information security vector and the conditional probability intensity of a set of security events. For a comparative analysis, a numerical calculation was carried out and a graphical dependence of the probability of the degree resistance to security threats in a communication system on the probability danger and the intensity of a set of security events was constructed when using different feedback coefficients. The relevance of using machine learning technology in the tasks of assessing the effectiveness of management based on security events in multiservice communication networks using the *k*-nearest neighbours (KNN) method, which classifies an object as a class, is considered. Based on the modeling, the metrics for assessing the quality of classification by the KNN algorithm are presented and a graphical dependence True Positive Rate (TPR) and False Positives Rate (FPR) is constructed for comparative analysis.

Keywords: Telecommunication system, security events, quality of service, true positive rate, hazard factors, quality of protection, false positives rate

1. Introduction

Currently, the problem of information protection, the factors danger and intensity many information security events used in modern multiservice telecommunication networks is very acute (Zhou *et al*., 2015; (Erohin, 2019; Ibrahimov *et al.*, 2021). Such telecommunication networks can be connected both to multiservice local and corporate networks, and to global public communication networks, as a result of which they can be exposed to threats of subscriber and network unauthorized access, refusal nodes to service traffic packet flows, loss of messages and other threats to information security (Ibrahimov *et al*., 2021; Xiangyu *et al*., 2018).

Taking into account the above-described threats and security factors can lead to significant economic and other losses, and therefore, it is necessary to reduce the probability of their occurrence in the telecommunications system to a minimum (Chandra, 2019; Breiman, 2001). Therefore, the tasks of research and analysis of the indicators of the information security system, the factors of danger, stability and intensity of many information security events in multiservice telecommunications networks are the most relevant (Erohin, 2019; Ahmad *et al*., 2022).

Some works (Ibrahimov, 2023; Kenechi *et al*., 2025; Ibrahimov *et al.*, 2018) investigated information security systems in multi-service local and corporate networks and determined indicators of information security and reliability of hardware and software systems.

The paper examines the degree resistance to aggregate threats and threats of unauthorized access, and as a result, determines performance indicators using machine learning and artificial intelligence technologies that are well suited for studying network and useful traffic (Kenechi *et al*., 2025; Pallaprolu *et al*., 2017; Lipatnikov *et al*., 2022). The latter helps to identify normal traffic, including subscriber actions, and separate it from suspicious and potentially dangerous traffic (Ibrahimov *et al.,* 2024; Ouissale *et al*., 2024; Islamov *et al*., 2023).

This work is devoted to the problem of research and analysis of some factors of danger and intensity of many security events in communication systems using machine learning technology.

2. General statement of the problem

Considering the importance building highly efficient multiservice telecommunication networks (Ibrahimov, 2023), (Ibrahimov *et al*., 2024) based on the concept future packet-switched networks (ITU-T, Y.3000÷Y.3499) for QoP (Quality of Protection), QoS (Quality of Service) and QoE (Quality of Experience) useful and service traffic, special attention should be paid to individual and complex indicators information security of the communication network, taking into account numerous requirements (Petukhov *et al*., 2019), (Islamov, 2023).

Taking into account the constituent components of the information security vector multiservice telecommunication networks, it is functionally described by the following dependence:

$$E[I(\lambda_i)] = W[S(\lambda_i), V(w_i), P(\gamma_i), F_0(\lambda_i)],\ i = 1,2,...,S, \tag{1}$$

where $S(\lambda_i)-$ function taking into account the criteria of the degree stability multiservice telecommunication systems with a parameter λ_i in conditions information technology impacts (multiple attacks, detection threats to network security, threats to confidential data, resistance to network attacks, vulnerabilities, etc.); $V(w_i)-$ function taking into account the indicators individual and multiple safety events and hazard factors with the parameter w_i, and the tasks of the unconditional compromise are V_0^k (area of compromise) and the indication rules G_0 (Nguyen *et al*., 2008), (Islamov *et al*., 2022); $P(\gamma_i)$ is conditional probability of a hazard event and the intensity of a set of safety events with a parameter γ_i in incident cases; $F_0(\lambda_i)$ is a function that takes into account the criteria of a set of hazard factors and the intensity of a set of safety events with a parameter λ_i and is described by the following functional dependence (Islamov *et al*., 2022), (Casson Moreno *et al*., 2018; Dhanabal *et al*., 2015):

$$F_0(\lambda_i) = W[F_0^S(\lambda_i), F_u^S(\lambda_i)],\ \ i = 1,2,...,S, \tag{2}$$

Expressions (1) and (2) define the essence of the proposed new approach, which accounts for both individual and combined factors of hazardous events as well as the intensity of a set of security events. On this basis, a mathematical model of information security for multiservice telecommunication networks is developed.

3. Criteria for quality of incident indication as a network security event

To accomplish the above-described problem statements, it is necessary to study the first and second tasks, the hazard factors and the intensity of a set of security events and the degree of resistance to threats of the units (Ibrahimov *et al*., 2024; Nguyen *et al*., 2008).

It should be noted that the implementation of the conditions formulated in the last two tasks does not yet lead to obtaining an optimal solution to the incident indication rule in the traditional sense – if V_0^k it contains more than one element and does not eliminate the need to select a specific compromise scheme (Erohin, 2019; Nguyen *et al*., 2008).

1. Let us consider the first problem, where an unconditional area compromise V_0^k is defined and a general compromise w_i scheme is selected and the following condition is valid for it (Erohin, 2019):

$$V(G_0) \cap V_{opt}(w_i) = \varnothing,\ i = 1,2,...,S, \tag{3}$$

where $V_{opt.}(w_i)-$ is determined in the unconditional area of compromises (optimum).

2. The second task is an unconditional compromise V_0^k area and it is required to create an indication G_0 rule that allows optimization in this area according to any compromise scheme. In this case, the condition is equivalently fulfilled, which is described as follows (Erohin, 2019), (Islamov *et al*., 2022):

$$V_0^k \subset V(G_0),\ V_{opt}(w_i, G_i) \subset V^k(G_i), \tag{4}$$

where G_i – incident indication rule, $i = 1,2,...,S$; $V^k(G_i)$ is a conditional area of compromise.

Expression (3) and (4) are the criteria for assessing the quality of incident indication.

Based on the conditions (3) and (4) the indication V_0^k rule coincides with the conditional area of compromises $V_0^k(A_0)$ and it is necessarily a parametric safety factor.

Thus, formulas (3) and (4) are for the study of the factors danger and intensity of a set of information security events in a multiservice communication network. In addition, condition (3) and (4) guarantees only the possibility achieving optimal solutions in the sense of an arbitrary compromise scheme using the indication rule.

Nevertheless, the formulation of the last two problems is free from the limitations inherent in the problems formulated earlier, and therefore such a problem can be called a problem vector optimization of indication rules (Kenechi *et al.,* 2025; Islamov *et al.,* 2022).

4. Research and analysis some hazard factors in the telecommunication system

It should be noted that the formal dependence integrated criteria of indication quality on similar criteria of individual safety events in the system is completely determined by the specific type of response predicate (Erohin, 2019; Casson Moreno *et al*., 2018).

At the same time, abstracting from this dependence in the communication system, we formulate the properties of the transition from the quality of indication of one event to the quality of indication of several (Ibrahimov *et al*., 2024; Casson Moreno *et al*., 2018).

First of all, we note that for the disjunctive integration scheme, some danger factors increase when adding an event, especially a logical variable, to the response predicate (Erohin, 2019).

Indeed, if the set of events used for indication in the system $I-$ includes events b_i, $1 \le i \le S$, the total hazard factor will be determined by the following expression (Erohin, 2019):

$$F_0(\lambda_i, \gamma_i) = 1 - \prod_{b_i \in I} [1 - P(\gamma_i)], \; 1 \le i \le S, \tag{5}$$

where $P(\gamma_i)$ – conditional probability of an event b_i in the event of an incident, this means the danger factor of this event in the system.

Taking into account the events with factors f_{0i} in the system, expression (5) will take the following form (Erohin, 2019):

$$F_0(\lambda_i, \gamma_i) = 1 - \prod_{b_i \in I} (1 - f_{oi}), \; 1 \le i \le S, \tag{6}$$

Based on expressions (5) and (6), the same considerations can be made regarding some intensity factor for the disjunctive scheme of event integration. Since some intensity factor represents the probability of occurrence of an event independently of the incident P_{IN}, this probability for the disjunction of events is determined as follows (Erohin, 2019):

$$F_u(\lambda_i, \gamma_i) = 1 - \prod_{b_i \in I} [1 - P(\gamma_i) \cdot P_{\text{IN}} - P(\mu_i) \cdot (1 - P_{\text{IN}})], \tag{7}$$

where $P(\mu_i)$ - conditional probability of an event b_i in the absence of an incident.

Taking into account the events with factors f_{ui} in the system, expression (7) will take the following form:

$$F_u(\lambda_i, \gamma_i) = 1 - \prod_{b_i \in I} (1 - f_{ui}), \; 1 \le i \le S. \tag{8}$$

From these relationships (7) and (8) it follows that the combined factors of both danger and intensity, when increased S by one, at least do not decrease, and the larger the factor of the added event, the more noticeable the change in the overall corresponding factor.

Thus, the combined factors both the danger and the intensity of the disjunctive scheme increase with the expansion composition security events in the communication system. This increase is an asymptotically increasing function of the corresponding factors each added event with factors (Erohin, 2019; Ibrahimov, 2024).

5. Research and formation of an optimal set of security events in a telecommunication network

Now we will consider and evaluate the possibilities of forming an optimal set security event in a communication network to indicate an incident with a minimum level error. To do this, we will consider strategies that optimize the selection of events in terms of each of the criteria separately in the network (Ibrahimov *et al*., 2024; Kenechi *et al.*, 2025).

The criterion k_1 coincides with the total hazard factor $F_0(\lambda_i, \gamma_i)$ and is equal to (Erohin, 2019):

$$k_1 = F_0(\lambda_i, \gamma_i),\ k_2 = (P_{IN} \cdot k_1)/[F_u(\lambda_i, \gamma_i)], \tag{9}$$

Expressions (9) define the quality criteria of the indication for one security event associated with the indicators of the hazard factors and the intensity security of the communication network.

Based on (9), the procedures for maximizing these values are equivalent. In addition, taking into account the monotony of the increasing dependence of the total danger factor on the danger factors of the selected security events, it can be argued that in order to optimize the set I and S events according to the criterion k_1, it is sufficient to include in this set the S events with the maximum danger factors in the communication network among all possible events.

Then the indication using these events will be no worse from the point of view of the criterion k_1 than the indication using any other choice, the number of events in which does not exceed S.

6. Research into the hazard and intensity factors multiple safety events

Taking into account expression (9), it is possible to estimate the change in the indicator k_2, also with the expansion of the composition events in the communication network. Let us assume that set I and S events provides the values of the total factors of danger F_o^S and F_u^S intensity, respectively.

After adding the *i*-th event with factors f_{oi}, the values of the aggregate factors will change in the communication network, that is, they will increase (Ibrahimov *et al*., 2024):

$$F_o^{S+1}(\lambda_i, \gamma_i) = F_o^S(\lambda_i, \gamma_i) + f_{oi} - F_o^S(\lambda_i, \gamma_i) \cdot f_{oi}. \tag{10}$$

Taking into account the new addition of the *i*-th event with factors f_{ui}, the values of the total factors in formula (10) will take the following form:

$$F_u^{S+1}(\lambda_i, \gamma_i) = F_u^S(\lambda_i, \gamma_i) + f_{ui}[1 - F_u^S(\lambda_i, \gamma_i)]. \tag{11}$$

From (10) and (11) it follows that the set of factors from S events provide the values of the total factors of danger and intensity security events in the communication network.

It is worth noting that in order to ensure the growth of the indicator k_2 due to the addition of an event, the following conditions must be met (Ibrahimov *et al*., 2024):

$$k_2^{S+1} = \frac{F_o^{S+1} F_{\text{i}}^S}{F_{\text{i}}^{S+1} F_{\text{o}}^S} \cdot k_2^S > 1,\ k_2^{S+1} > k_2^S. \tag{12}$$

By putting values (10) and (11) into formula (12) for F_o^{s+1} and F_{i}^{s+1}, after some transformations, we obtain the necessary conditions (Erohin, 2019):

$$\beta_i > \frac{1 - F_{\text{i}}^S(\lambda_i, \gamma_i)}{F_{\text{i}}^S(\lambda_i, \gamma_i) \cdot [1 - F_{\text{o}}^S(\lambda_i, \gamma_i)]} \cdot F_0^S(\lambda, \gamma_i). \tag{13}$$

From conditions (12) and (13) it follows that for a stable growth of the indicator k_2 in connection with the addition of an event it is necessary that each time the ratio of the hazard factor to the safety intensity factor of the added event exceeds a certain value.

However, these assumptions characterize the already accumulated composition of events, and the greater such excess, the stronger the growth of the indicator k_2. The latter means that the ratio of the values of the indicator before and after the addition will differ more from one.

It should be noted that the obtained result does not prove the existence of events, starting from the second, the addition of which necessarily ensures the growth of the indicator k_2 it only establishes the fact that if they exist, then the sequential inclusion events with the greatest value β_i ensures the maximum k_2.

Thus, the connection between the indicators efficiency incident indication, the level indication errors with the static characteristics of the security events used is shown.

To solve the set vector optimization problem in the conditions of a specific multiservice telecommunication network, integer programming methods and applications to multicriterial optimization problems can be used (Erohin, 2019; Islamov *et al*., 2023).

7. Research quantitative assessments security taking into account the resistance to threats of the telecommunication system

Real quantitative assessments of the hazard factors and intensity for security events can be obtained in the process passive monitoring when studying the degree of resistance to threats of units and to threats to information security in the communication system.

In this subparagraph we will consider the degree of resistance to threats and it has been established (Erohin, 2019; Ouissale *et al*., 2024) that with an increase in the degree threat realization, the degree of resistance decreases according to the following exponential law (Ibrahimov *et al.,* 2024):

$$\chi_{kb}(\tau_a, t, \lambda_i) = \tau_a \cdot \Delta T_a\{1 - \exp[-(t - t_0)/\tau_a]\}, \quad (14)$$

where τ_a – relaxation time of a threat in the absence of its activity; t_0 – random time of the beginning threat implementation; ΔT_a – compensated threat activity by taking counteraction measures in communication systems, $\Delta T_a = \delta(k_f, \lambda_i)$, where k_f – feedback coefficient and $k_f \le 1$.

Expressions (14) take into account the activity of the threat - a single threat of security events of confidentiality, integrity and availability, as well as a risk measure for the asset component A_i communication systems, which significantly affect the quantitative assessment of security factors. Here, specific assets can be servers, hardware and software systems and local networks connected to multiservice telecommunication networks A_i, $i = 1,2,...,S$.

Based on (8)-(14), we will consider the probability of the degree $P[S(A_i, \lambda_i)]$ resistance to threats of each asset A_i with the parameter λ_i is as follows (Erohin, 2019):

$$P[S(A_i, \lambda_i)] = 1 - \chi_{kb}(\tau_a, t, \lambda_i),\ i = 1,2,...,S, \quad (15)$$

where $P[S(A_i, \lambda_i)]$ – probability is the degree of resistance to security threats in communication systems, taking into account the activity and security threats A_i, which characterizes the criteria confidentiality, integrity and availability of each asset.

From (15) it follows that the failure of one asset of the communication network management systems leads to a loss of resistance to threats of communication systems.

In order to assess the resistance to security threats, a communication system is considered, which has an input system λ_i and a feedback subsystem to improve their degree of resistance (Erohin, 2019):

In accordance with (14) and (15), the output of the subsystem $P[S(A_i, \lambda_i)]$ is related to its input by an $F_0^S(A_i, \lambda_i)$ equation that is expressed as follows:

$$P[S(A_i, \lambda_i)] = \frac{F_0^S(A_i, \lambda_i)}{1 - k_f[1 - F_0^S(A_i, \lambda_i)]}. \quad (16)$$

Expression (16) characterizes the probability of the degree of stability communication systems to threats of security events taking into account the feedback coefficient.

The conducted research shows that with an increase in the intensity of security events, the degree of resistance to information security threats increases. Taking into account the above, we will determine the degree of resource resistance A_i.

8. Analysis of the results mathematical modeling

For each resource A_i, the degree of its system stability $F_0^S(A_i)$ can be determined by evaluating the criteria $F_0^S(A_1)$, $F_0^S(A_2)$, $F_0^S(A_3)$ and $F_0^S(A_4)$ and can be determined as follows (Erohin, 2019; (Ibrahimov *et al*., 2018):

$$F_0^S(A_i) = [F_0^S(A_1) + F_0^S(A_2) + F_0^S(A_3) + F_0^S(A_4)] \le F_{0.all.}^S(A_i), \quad (17)$$

where $F_{0.all.}^S(A_i)$ - acceptable value degree resistance to security threats of a communication system taking into account assets or resources A_i.

Using the Communications Toolbox package (Ibrahimov *et al*., 2024; (Ouissale *et al*., 2024) on the Matlab environment, the importance of the criteria for resistance to threats communication system was $k_f \le 85$ calculated and the results are given in Table 1.

Table 1. Quantitative security assessments taking into account the resistance to communication system threats

Parameter designation	Meaning
$F_0^S(A_1)$	0,386
$F_0^S(A_2)$	0,237
$F_0^S(A_3)$	0,178
$F_0^S(A_4)$	0,121

From Table 1 it can be seen that $F_0^S(A_i) = 0{,}386 + 0{,}237 + 0{,}178 + 0{,}121 = 0{,}922 < 1$.

It is worth noting that the degree of resistance to security threats of the communication system should be no less than 0,922, that is, a deviation from the complete stability of the system is allowed of no more than 7,8% (Erohin, 2019; Lipatnikov *et al*., 2022; Islamov *et al*., 2023). This means that $F_0^S(A_i) \ge 0{,}922$, that is $0{,}922 \le F_{0.all.}^S(A_i) \le 1{,}000$.

Based on numerical calculations obtained using the Communications Toolbox package in the Matlab environment, Fig. 1 shows a family graphical dependence for a given feedback coefficient $k_f = 0{,}85$ and $k_f = 0{,}55$.

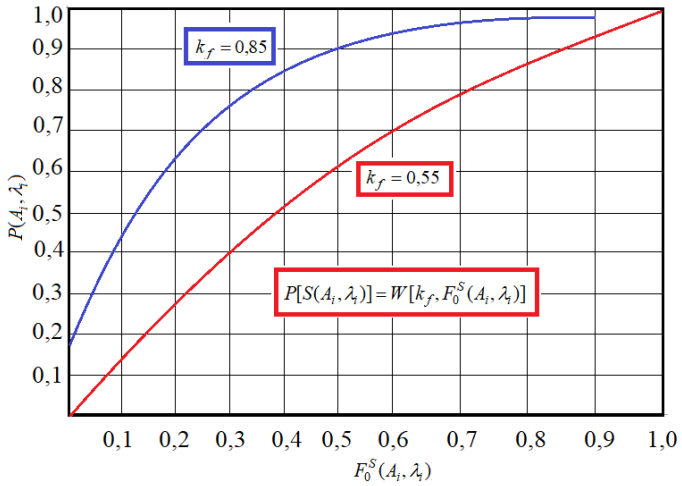


Figure 1. Graphic dependence of the probability degree of resistance to security threats in the communication system on the probability $F_0^S(A_i, \lambda_i)$ at a given coefficient $k_f = 0{,}85$ and $k_f = 0{,}55$

As can be seen from the graphical dependence $P[S(A_i, \lambda_i)] = W[k_f, F_0^S(A_i, \lambda_i)]$ with increasing probability $F_0^S(A_i, \lambda_i)$ for $k_f \le 0{,}85,...,0{,}55$ the likelihood of a degree resistance to threats in the communication system increases.

According to the graph (Figure 1), a noticeable change begins with the values $F_0^S(A_i, \lambda_i) \geq (0{,}20,...,0{,}35)$ at a given feedback coefficient $k_f = 0{,}55$ and $k_f = 0{,}85$, where they clearly demonstrate the improvement in the resilience communication systems to threats.

9. Statistical modeling and event-based management effectiveness assessment using machine learning technology

The widespread use machine learning (ML) technology for the network service of active monitoring security events in the field information security, or cybersecurity in the communication system, is in high demand among specialists (Breiman, 2001).

In particular, ML tools are used to identify threats to network security and, accordingly, threats to confidential data and hazards that are stored and transmitted through multiservice communication networks (Ibrahimov *et al.*, 2024; Ouissale *et al*., 2024).

Thus, the relevance of using machine learning technology in the tasks assessing the effectiveness of management based on security events in multiservice networks is considered.

Given the above, we will introduce some important metrics for assessing the effectiveness of security events of classification algorithms (Ahmad *et al*., 2022; Ouissale *et al*., 2024). For this, we will analyze the following indicators: reliability (Accuracy), accuracy (Precision), completeness (Recall) – also called True Positive Rate (TPR) and F-measure (F-score).

To assess the quality of trained models, various metrics are used, which are defined as follows (Ibrahimov *et al*., 2024; Ouissale *et al.*, 2024):

1. One of the important metrics is the reliability (Accuracy) of classification in the mode off-line:

$$T_{j.Acc.} = \frac{\sum_{i=1}^{n} TP_i}{\sum_{i=1}^{n} TP_i + \sum_{i=1}^{n}\sum_{j=1}^{n} F_{ij}} \leq 1,\ i, j = 1, 2,..., \text{n}, \tag{18}$$

where $TP_i -$ number correctly classified traffic packet flows; $F_{ij} -$ the number incorrectly classified traffic packet flows, and i – predicted class number; j – true class number.

2. Based on (18), the classification error can be determined as follows:

$$P_{j.error} = 1 - T_{j.Acc},\quad j = 1, 2,..., \text{n}. \tag{19}$$

3. Precision determines the proportion true positive labels among all positively labeled instances:

$$T_{i.\text{Pr}ec.} = \frac{TP_i}{TP_i + \sum_{j=1}^{n} F_{ij}} \leq 1,\quad i, j = 1, 2,..., \text{n}. \tag{20}$$

4. Recall measures the percentage correctly labeled positive instances among all instances of the positive class:

$$T_{j.\text{Re}c.} = \frac{TP_j}{TP_j + \sum_{i=1}^{n} F_{ij}} \leq 1,\quad i, j = 1, 2,..., \text{n}. \tag{21}$$

5. F-score combines the above two metrics and assigns a weighted importance to either precision or recall using a coefficient β :

$$F - score = [(1+\beta^2)\cdot(T_{j.\text{Re}c.}\cdot T_{j.\text{Pr}ec.})]/[(1+\beta^2)\cdot(\text{T}_{\text{j.Rec.}} + T_{j.\text{Pr}ec})], \tag{22}$$

where β is the significance coefficient of the influence of completeness on the *F*-score.

Since these presented metrics (18)-(22) are standard for evaluating the performance of a classifier for the metric of control effectiveness based on a set of security events.

The calculations, modeling and comparative analysis required the accuracy detection hazard factors and determination of the intensity many security events in multiservice communication networks using ML technology, which allows increasing the quality of classification in the field of information security (Lipatnikov *et al*., 2022).

In this case, machine learning technology is used to identify the hazard factors, threats to network security events and, accordingly, resistance to threats, threats to confidential data using the *k*-nearest neighbors (KNN) algorithm (Ahmad *et al*., 2022; Ouissale *et al*., 2024). Since one of the common practices is to take the parameter *k* equal to $k = N^{0,5}$, where N is the number instances in the training set (Ouissale *et al*., 2024; Nguyen *et al*., 2008). Based on the simulation, Table 2 presents the metrics for assessing the quality of classification by the KNN algorithm (Ouissale *et al*., 2024; Dhanabal *et al*., 2015).

Table 2. Metrics for assessing the quality of classification by the KNN algorithm

1	TP rate	FP rate	Precision	Recall	F-measure	Accuracy
2	0,980	0,152	0,868	0,980	0,921	0,915
3	0,848	0,020	0,977	0,848	0,908	0,915
4	0,915	0,086	0,922	0,915	0,915	0,915

In this Table 2 shown means that: 1 - Class; 2 - Normal data; 3 - Anomaly; 4 - Average value.

From Table 2 it can be seen that the highest classification accuracy of the KNN algorithm is achieved with a ratio of training and test samples 91.8%, which is a high indicator of the accuracy of detecting the hazard factors and the intensity many security events in the communication system (Lipatnikov *et al*., 2022).

Based on Table 2, the values of the relative number of correct responses (TPR) and the relative number of false positives (FPR) for different ratios training and test samples for the KNN algorithm are presented in Fig. 2.

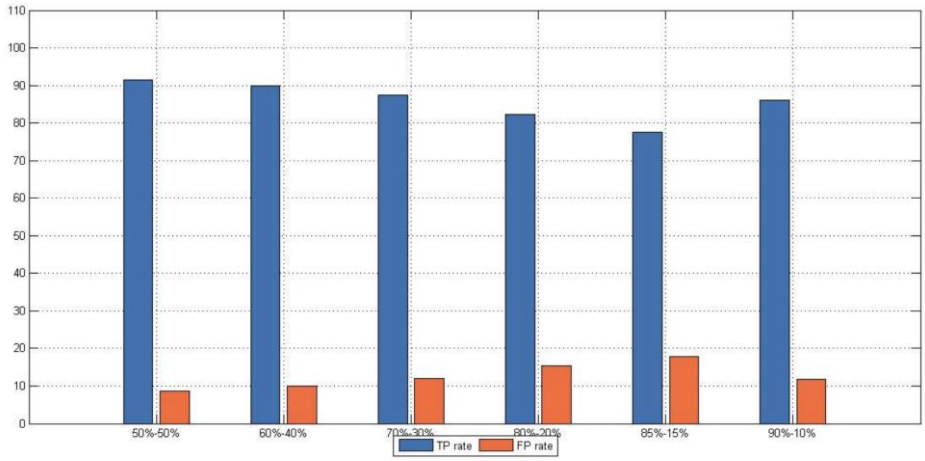


Figure 2. TPR and FPR graphs for different ratios of training and test samples for the KNN algorithm

From the graphical dependence it follows that the KNN algorithm provides the best accuracy with the ratio training and test samples 50% - 50%, which is achieved by a maximum value of 91,50.

10. Conclusions

1. As a result of the study, a mathematical model of the danger and intensity of a set of security events in a communication network under the threat of subscriber and network unauthorized access was developed based on the proposed new approach.

2. Based on the mathematical model, analytical expressions were obtained that evaluate the total danger, probability, degree of stability, and intensity of a set of security events in multiservice communication networks.

3. Numerical calculations were performed using the Communications Toolbox package on the Matlab environment and a graphical dependence of the probability of the degree of resistance to security threats in a communication system on the probability for a given feedback coefficient was constructed.

4. Based on ML technology, the best results are shown by the KNN algorithm, which has a high accuracy of 0,922.

However, due to the short training time, this algorithm can be a useful tool for non-standard analysis of the hazard factor and intensity many security events in a telecommunication system.

Declaration of Generative AI and AI-assisted technologies in the writing process:

- During the preparation of this manuscript the authors did not used Generative AI and AI-assisted technologies and take full responsibility for this declaration.

References

1. Ahmad, A., Mahmoud, K., Saed, A., Kim, K., Raymond, C., and Maysa, S. (2022) Network traffic classification: Techniques, datasets, and challenges. *Digital Communication and Network*, 10(3), 676-692. DOI: 10.1016/j.dcan.2022.09.009.
2. Breiman, L. (2001) Random forests. *Machine Learning*, 45, 5-32. DOI: 10.1023/A:1010933404324.
3. Casson Moreno, V., Reniers, G., Salzano, E., Cozzani, V. (2018) Analysis of physical and cyber security-related events in the chemical and process industry. *Process Safety and Environmental Protection*, 116, 621-631. DOI: 10.1016/j.psep.2018.03.026.
4. Chandra, K.P. (2019) *Nonlinear filtering: Methods and applications*. Springer, 197 p. DOI:10.1007/978-3-030-01797-2.
5. Dhanabal, L. and Shantharajah, S.P. (2015) A study on NSL-KDD dataset for intrusion detection system based on classification algorithms. *International Journal of Advanced Research in Computer and Communication Engineering*, 4(6), 54-64. DOI: 10.17148/IJARCCE.2015.4696.
6. Erohin, S.D. (2019) Managing security of critical information infrastructure. *Systems of Signal Synchronization, Generating and Processing in Telecommunications*, 1-14. DOI:10.1109/SYNCHROINFO.2019.8814097.
7. Ibrahimov, B. (2023) Investigation of noise immunity telecommunication systems according to the criterion energy efficiency. *Transport and Telecommunication*, 24(4), 375-384. DOI:10.2478/ttj-2023-0029.
8. Ibrahimov, B., and Valiyev, F. (2024) Research useful and service traffic based on machine learning in multiservice software defined network. *Artificial Intelligence and Digital Development*, 41-44. DOI:10.59849/aidd.2024.41.
9. Ibrahimov, B.G., Humbatov, R.T., and Ibrahimov, R.F. (2018) Cryptographic methods and means protection transmitted information in telecommunication systems. *IFAC-Papers OnLine*, 51(30), 821-824. DOI:10.1016/J.IFACOL.2018.11.187.
10. Ibrahimov, B.G., Orujov, A.O., Hasanov, A.H., and Tahirova, K.M. (2021) Research and analysis efficiency fiber optical communication lines using quantum technology. *T-Comm*, 15(10), 50-54. DOI: 10.36724/2072-8735-2021-15-10-50-54.
11. Islamov, I. (2023) Optimization of broadband microstrip antenna device for 5G wireless communication systems. *Transport and Telecommunication*, 24(4), 409-422. DOI:10.2478/ttj-2023-0032.
12. Islamov, I., and Safarli, A. (2023) Design, modelling and research of an antenna system for transmitting and receiving information in satellite systems. *Transport and Telecommunication*, 24 (3), 297-308. DOI: 10.2478/ttj-2023-0024.
13. Islamov I.J., Hunbataliyev E.Z., and Zulfugarli, A.E. (2022) Numerical simulation of characteristics of propagation of symmetric waves in microwave circular shielded waveguide with a radially inhomogeneous dielectric filling. *International Journal of Microwave and Wireless Technologies*, 9, 761-767. DOI: 10.1017/S1759078721001082.
14. Kenechi, O., and Sesan, O. (2025) Enhancing cybersecurity measures in critical infrastructure: Challenges and innovations for resilience. *Journal of Scientific Research and Reports*, 31(2), 474-484. DOI: 10.9734/jsrr/2025/v31i22868.
15. Lipatnikov, V.A., Shevchenko, A.A., Kosolapov, V.S., and Sokol, D.S. (2022) Method for ensuring information security of a VoIP telephony network with a forecast of an intruder's intrusion strategy. *Information and Control Systems*, 1, 54-67. DOI:10.31799/1684-8853-2022-1-54-67.
16. Nguyen, T.T., and Armitage, G. (2008) A survey of techniques for internet traffic classification using machine learning. *IEEE Communication Surveys & Tutorials*, 10(4), 56-76. DOI:10.1109/SURV.2008.080406.
17. Ouissale, E.G., Ikrame, K., and Hayat, E.B. (2024) Evaluating AI and ML in network security: A comprehensive literature review. *Procedia Computer Science*, 251, 727-733. DOI:10.1016/j.procs.2024.11.176.

18. Pallaprolu, S.C., Sankineni, R., Thevar, M., Karabatis, G., and Wang, J. (2017) Zero-day attack identification in streaming data using semantics and spark. In: *Proceedings of IEEE International Congress on Big Data*, Honolulu, June 2017. IEEE, 121-128. DOI:10.1109/BigDataCongress.2017.25
19. Petukhov, A.N., Erokhin, S.D., and Pilyugin, P.L. (2019) Event-oriented security policy and a formal model of the mechanism for protecting critical information infrastructures. *Proceedings of Educational Institutions of Communication*, 5(4), 99-105. DOI:10.31854/1813-324X-2019-5-4-99-105.
20. Xiangyu, X., Tong, Z., Wei, Y., Zhao, W., Shikun, Z., Dongdong, D., and Qing, G. (2018) An ensemble approach for detecting anomalous user behaviors. *International Journal of Software Engineering and Knowledge Engineering*, 28(11-12), 1637-1656. DOI: 10.1142/S0218194018400211.
21. Zhou, Y., Cheng, N., Lu, N., and Shen, X. (2015) Multi-UAV-aided networks: Aerial-ground cooperative vehicular networking architecture. *IEEE Vehicular Technology Magazine*, 10(4), 36-44. DOI:10.1109/MVT.2015.2481560.