DOI 10.20535/2411-1031.2025.13.1.328754
UDC 621.396.6:004.89

VIACHESLAV RIABTSEV,
PAVLO PAVLENKO

MACHINE LEARNING METHODS FOR ANOMALY DETECTION IN THE RADIO FREQUENCY SPECTRUM: RESEARCH METHODOLOGY

The experience of the past three years of full-scale warfare testifies to the dynamic transformation of the conceptual foundations of combat operations and the shifting prioritization of the means employed to conduct them. The emergence and increasingly active use of various unmanned systems, the widespread deployment of precision-guided munitions, and the development of advanced electronic warfare capabilities have collectively underscored the strategic significance of the radio frequency spectrum. The provision of continuous spectral monitoring and the detection of anomalous activity in the electromagnetic environment have become critically important components of electronic warfare systems, signals intelligence, and secure communications networks. Traditional approaches to signal analysis – based on fixed thresholds, heuristic rules, or a priori statistical assumptions – are proving insufficiently effective in the highly dynamic and noise-intensive environment of the modern electromagnetic battlespace.

In this context, there arises a need to investigate innovative approaches, particularly machine learning methods, for their ability to enable the automatic detection of anomalous signals without reliance on labeled data. Such solutions are expected to enhance the accuracy, adaptability, and response speed of spectral monitoring systems.

A research methodology is proposed to assess the feasibility of applying machine learning methods to the task of anomaly detection in the radio frequency spectrum, taking into account the complexity of the data structure, its high dimensionality, and the limited availability of a priori information regarding anomalous samples. This research methodology encompasses the following stages:

- formulation of the experimental task;
- selection of anomaly detection methods for experimental evaluation;
- determination of evaluation metrics;
- selection and/or generation of test datasets;
- direct execution of the experimental study;
- analysis and assessment of the results;
- visualization and interpretation of the obtained findings;
- formulation of conclusions based on the experimental outcomes.

This article focuses on the theoretical framework of the experimental study. Practical results will be published separately.

Keywords: artificial intelligence, anomaly detection, machine learning, radio frequency spectrum, classification, Analytic Hierarchy Process (AHP), Isolation Forest, Autoencoder, Local Outlier Factor (LOF), One-Class SVM, Generative Adversarial Networks (GAN).

Problem statement. Classical approaches to anomalous signal detection are based on statistical criteria and hypotheses regarding data distributions. They are based on the assumption that “normal” data belong to high-probability regions of the statistical model, while anomalies occur in low-probability regions [1].

A common approach is the **three-sigma rule** (3σ), which assumes that the measurements follow a normal distribution. According to the 3σ, approximately 99.7% of the values of a random variable fall within the interval:

$$m - 3\sigma, \quad m + 3\sigma ,$$

where m is the mean value and σ is the standard deviation [1]. Any measurement falling outside this interval is considered a potential anomaly – an outlier.

The advantage of the 3σ lies in its simplicity of implementation and interpretation: the threshold value is easy to compute and explain. This method has been widely used in quality control and technical diagnostics, where deviations that are highly unlikely under normal operating conditions are considered anomalous.

The primary drawback of this approach is the assumption of a normal distribution. In real-world radio signals, the noise distribution may deviate significantly from Gaussian behavior (e.g., due to the presence of impulsive interference), meaning that a fixed threshold based on the 3σ may result in excessive false positives or missed anomalies, particularly when the baseline noise level exhibits heavy “tails”. Moreover, the 3σ is insensitive to small deviations and may fail to detect anomalies whose amplitude is less than three standard deviations. In cases where the distribution is unknown or non-normal, more robust criteria are often employed.

Similarly, the ***“box plot rule”*** (***interquartile range method***, IQR) defines normal values as those falling within the range of [1]:

$$Q_1 - 1,5IQR, Q_3 + 1,5IQR$$

where Q_1 and Q_3 are the lower and upper quartiles, respectively;

$IQR = Q_3 - Q_1$.

Points lying outside this range are considered statistical outliers (anomalies). For a normal distribution, the *IQR*-based boundaries approximately correspond to the interval $\mu \pm 2,7\sigma$ (which covers about $\sim 99,3\%$ of the data) [1].

Thus, the *IQR* method is somewhat more sensitive to outliers (and may detect more anomalies) compared to the 3σ. In particular, experimental results have shown that the *IQR* method can produce a higher number of false alarms, whereas the 3σ yields more stable results under the assumption of normality [1].

The null hypothesis of the Grubbs' test states that there are no outliers, while the alternative hypothesis asserts the presence of at least one anomalous value [2]. The test statistic is calculated as:

$$C = \frac{\max_t |x_t - \bar{x}|}{s},$$

where $\bar{x}$ is the mean value of the time series X;

s is the standard deviation of the time series X.

For a two-sided test, the null hypothesis of no outliers is rejected at the significance level α if:

$$C > \frac{N-1}{\sqrt{N}} \cdot \sqrt{\frac{t_{\alpha/(2N),\,N-2}^{\quad 2}}{N - 2 + t_{\alpha/(2N),\,N-2}^{\quad 2}}},$$

where $t_{\alpha/(2N),\,N-2}$ denotes the upper critical value of the *t*-distribution withз $N-2$ degrees of freedom at the significance level $\alpha/(2N)$.

For a one-sided test $\alpha/(2N)$ is transformed into α/N. The largest point in the time series that exceeds the test statistic is classified as an anomaly [2]. In other words, the observation with the largest absolute value is considered an anomaly if it is statistically inconsistent with the rest of the sample. The Grubbs' test is effective for detecting a single outlier; however, it must be applied iteratively to detect multiple anomalies, which may reduce its accuracy (generalizations for multiple outliers exist, such as the Tietjen–Moore test or the generalized extreme Studentized deviate (*ESD*-test) [2].

In addition to the Grubbs' test, the statistical toolkit includes other methods, such as Dixon’s Q test for small samples, Mahalanobis distance for multivariate data, and the chi-squared χ^2 goodness-of-fit test, among others [3].

These methods offer a simple and interpretable means of anomaly detection but critically depend on assumptions regarding the data distribution (e.g., normality) [4]. When the actual signal distribution significantly deviates from these assumptions, the accuracy of such methods deteriorates sharply.

Thus, classical methods for radio signal analysis do not provide sufficient real-time operational responsiveness under conditions of high spectral density, active jamming countermeasures, and rapidly changing signal parameters. This necessitates the adoption of innovative approaches, particularly machine learning methods capable of autonomously detecting anomalous signals in high-dimensional data without the need for a priori labeled samples.

Analysis of recent research and publications. A comparison between traditional methods of anomaly detection in the radio frequency spectrum and *machine learning* (ML) approaches demonstrates that the latter enable the identification of anomalies within high-dimensional data and complex radio signal patterns, outperforming simple statistical criteria in terms of flexibility [4]. Most of these approaches operate in an *unsupervised* or *semi-supervised learning* mode, where the model is trained solely on normal data and attempts to detect deviations from it. In other words, the algorithm learns to recognize the "normal" behavior without access to anomalous samples and subsequently flags observations that significantly deviate from this learned norm as potential anomalies.

In [5], the authors investigate various ML algorithms. The approach, based on the ***One-Class Support Vector Machine*** (One-Class SVM), is an unsupervised learning algorithm that seeks to delineate the boundary of the region containing normal data, thereby identifying new points outside this region as anomalies. In this setting, the algorithm attempts to find a boundary that encloses the majority of the data (normal points) while separating them from the origin in the feature space. The One-Class SVM is trained exclusively on normal data and distinguishes between normal and anomalous examples by predicting whether a new instance falls within the learned region (norm) or is considered an “outlier”. Geometrically, this can be interpreted as constructing a hypersurface (or a sphere) around the normal data; new points located significantly outside this region are classified as anomalies. Formally, the following problem is solved:

$$\min_{w,\xi_i,\rho} \frac{1}{2} \left|w\right|^2 + \frac{1}{vn}\sum_{i=1}^{n}\xi_i ,$$

subject to the conditions: $\left[\ w\cdot x_i \ \geq \rho - \xi_i, \xi_i \geq 0, i = \overline{1,n}\right]$,

where v is the parameter that determines the proportion of anomalies.

Advantages of One-Class SVM: it can model fairly complex boundaries (not only spherical ones) and takes into account multidimensional dependencies. When applied to radio signals, the One-Class SVM is capable of simultaneously considering multiple signal features (e.g., energy at different frequencies) and detecting complex anomalous patterns.

Disadvantages: high computational complexity (training an SVM typically scales as $O(n^2)$ with respect to the number of samples, which does not scale well to large datasets), the need for careful tuning of the kernel and parameters (which significantly affect the results), and a lack of transparency – making it difficult to interpret why a particular point is classified as anomalous beyond the fact that it lies outside the learned boundary.

Autoencoders are neural networks capable of learning to compress and reconstruct data. They have found widespread application in anomaly detection tasks for radio signals [5]. The architecture of an autoencoder consists of two main parts: an *encoder*, which compresses the input data (e.g., a digitized radio signal or its spectrum) into a low-dimensional latent representation (*bottleneck*), and a *decoder*, which reconstructs the output from this compressed code.

The network is trained on normal data in such a way as to minimize the reconstruction error (the difference between the input and the reconstructed signal):

$$L = |x - \hat{x}|^2,$$

where x is the input signal;

$\hat{x}$ is its reconstruction by the network.

If the L exceeds a predefined threshold, the signal is classified as anomalous.

Advantages of autoencoders:

– flexibility – they do not require an explicit model of the data distribution and can capture nonlinear dependencies;

– context-awareness – for example, a recurrent autoencoder can take into account the temporal structure of the signal;

– no need for labeled data – like other models discussed, the autoencoder is trained solely on unlabeled (normal) data.

Disadvantages:

– require a significant amount of data and computational resources for training (especially deep networks);

– risk of overfitting – if the network is too powerful, it may begin to accurately reconstruct even anomalous data encountered during training, thereby reducing sensitivity;

– difficulty in architecture and hyperparameter selection (e.g., bottleneck size, number of layers, etc.).

The interpretability of autoencoders is limited – at best, one can analyze which features contribute most significantly to the reconstruction error, but the neural weights themselves are difficult to interpret physically. For normal signals, the autoencoder accurately reconstructs the structure, whereas for anomalous signals, the reconstruction error is significantly larger [5].

The application of autoencoders to radio engineering data has been successfully demonstrated in the literature. In particular, a deep autoencoder and its variant, the LSTM-autoencoder, have been employed to detect unauthorized transmissions in shared spectrum environments by analyzing the *IQ* data of Wi-Fi/LTE signals [4].

Another approach is based on the use of ***convolutional autoencoders*** (CAE) to analyze spectrograms as images, which enables achieving high accuracy in anomaly detection within wireless networks [6].

Isolation Forest (IF) is an ensemble algorithm based on decision trees, specifically designed for anomaly detection. Its key idea is the random isolation of observations: the algorithm constructs numerous random trees, each time randomly selecting a feature and a threshold to split the data [7]. Unlike density-based or distance-based methods, IF directly isolates anomalous points without modeling the normal data distribution. The core concept is that anomalies are objects that are “easy to separate” from others, as they are rare and have feature values that differ significantly. Intuitively, anomalous points (which are located far from the main cluster of normal data) are isolated after fewer splits, meaning that the path from the root to the leaf node is shorter for anomalies [8].

In contrast, for normal points that are grouped together, more random splits are required to completely isolate them. Thus, the average path length to isolation (averaged over the ensemble of trees) serves as a measure of anomaly: shorter average paths correspond to more “isolated”, and therefore more anomalous, points [8]:

$$s(x,n)=2^{-\frac{E\ h(x)}{c(n)}},$$

where $E\ h(x)$ is the average path length for point x;

$c(n)$ is the normalization constant.

The IF algorithm offers several significant *advantages*. First, it exhibits high computational efficiency: it scales linearly with respect to the number of data points and features. Second, Isolation Forest performs well in high-dimensional spaces and does not require explicit calculation of distances or densities, which is particularly useful when features are heterogeneous or difficult to normalize. As noted in research studies, the algorithm is effective for high-dimensional data and has become a popular choice for anomaly detection [8]. Third, IF does not require labeled data and is minimally dependent on hyperparameters. Fourth, IF is fairly robust to noise in the data: if a few anomalous points are present in the training set, they are likely to be isolated at shallow depths in most trees and assigned high anomaly scores, but they do not significantly affect the isolation of normal points (unlike, for instance, the mean and standard deviation estimates, which can be heavily distorted by strong outliers).

In radio engineering applications, IF has been employed, for example, for detecting radio frequency interference and anomalous spectral patterns. However, the effectiveness of IF may degrade if the proportion of anomalies in the training data is substantial or if the anomalies are not well-separated in the feature space.

The Local Outlier Factor (LOF) is another popular unsupervised machine learning method. It estimates the data density within the local neighborhood of each point and compares it to the density of its neighboring points [9]. The underlying idea is that normal objects have a density similar to that of their nearest neighbors, whereas anomalous points (outliers) exhibit significantly lower local density.

The algorithm computes an LOF score for each point, which represents the ratio of the average local reachability of its neighbors to the local reachability of the point itself.

$$LOF(x)=\frac{\sum_{i=1}^{k}\frac{lr\,d_k(x_i)}{lr\,d_k(x)}}{k},$$

where $lr\,d_k(x)$ is the local density of points within a neighborhood of radius k.

If this factor significantly exceeds 1, the point is considered to be sparsely populated relative to its neighbors and thus potentially anomalous.

Advantages of LOF: the ability to detect local anomalies – a point may be an outlier relative to its immediate neighborhood even if its global value is not extreme. This is particularly important for non-uniform data. For example, in the radio spectrum, certain frequency bands may be densely populated while others have sparse signals – LOF can detect an anomalously strong signal in a quiet band, even if a similar signal strength would be considered normal in a noisy band.

Disadvantages: calculating k-nearest neighbors for each point can be computationally expensive (a naive realization is – $O(n^2)$), although acceleration techniques such as k-d trees exist. LOF is harder to scale to very large datasets compared to tree-based algorithms. Moreover, the result of LOF depends heavily on the parameter k (the size of the local neighborhood), and improper selection of k can lead either to missed anomalies (if k is too small and noise is mistaken for anomalies) or to blurring of the local structure (if k is too large and the algorithm becomes effectively global). From an interpretability perspective, LOF provides a numerical score for each point, but explaining the anomaly still requires analyzing its neighbors – specifically, how the point differs from them (e.g., significantly lower density indicates a gap in the local distribution).

In addition to the methods mentioned above, generative models are also being explored in the context of radio spectrum monitoring tasks**. *Generative Adversarial Networks*** (GAN) represent an approach where two neural networks – a *generator* and a *discriminator* – are trained in a competitive manner: the generator attempts to produce fake data resembling real data, while the discriminator strives to distinguish between real and fake samples. For anomaly detection, a GAN is typically trained on normal data, and subsequently, either the discriminator (or, in some cases, the generator) is used to evaluate new samples [4].

When applied to radio signals, a GAN can generate spectra of normal signals; if a real signal cannot be well distinguished by the discriminator from generated ones (or if the generator fails to accurately reproduce it), this serves as an indication of anomaly.

GANs are capable of modeling highly complex data distributions and, in theory, can capture even the most subtle anomalies. However, training GANs is an unstable process that requires careful balancing between the generator and the discriminator. The absence of a clear loss function further complicates convergence. Moreover, like other deep models, GANs involve millions of parameters and thus represent a “black box” from an interpretability perspective.

The application of GANs for streaming anomaly detection in radio data is currently an active area of research, although notable progress has already been made. For example, in [4] the authors combined an autoencoder and a GAN for radio spectrum analysis: first, the autoencoder was used to obtain a compressed representation, and then a sigma-criterion was applied to the generator/discriminator error.

Contemporary approaches often advocate for combining multiple machine learning methods or employing ensemble techniques to enhance reliability.

The aim of this article is to develop a research methodology for assessing the feasibility of applying machine learning methods to the task of anomaly detection in the radio frequency spectrum. The characteristic features of this task include the complex structure of high-dimensional data and the limited availability of a priori information regarding anomalous samples. To achieve this aim, the following objectives are addressed:

1. Analysis of current approaches to anomaly detection based on machine learning algorithms.
2. Development of a methodology for the experimental evaluation of selected algorithms on synthetic radio signal data.
3. Identification of methods for analyzing and visualizing the results of the experimental study.

The exposition of the main research material. The objective of the experimental study is to conduct a comprehensive comparative analysis of the effectiveness of modern machine learning methods in anomaly detection tasks within the radio frequency spectrum. The sequence of stages of the experimental study is presented in Fig. 1.

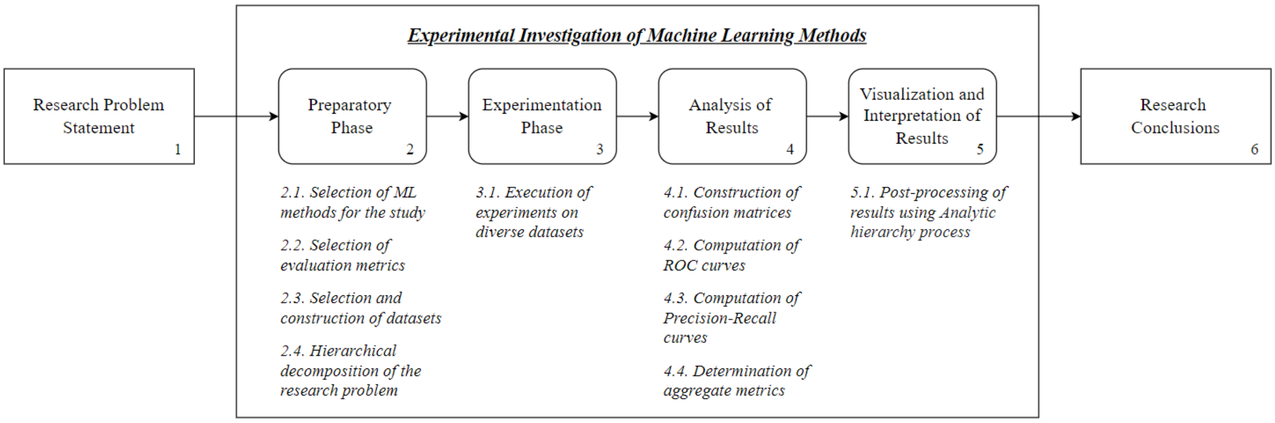
Experimental Investigation of Machine Learning Methods
Research Problem Statement 1
Preparatory Phase 2
Experimentation Phase 3
Analysis of Results 4
Visualization and Interpretation of Results 5
Research Conclusions 6
2.1. Selection of ML methods for the study
2.2. Selection of evaluation metrics
2.3. Selection and construction of datasets
2.4. Hierarchical decomposition of the research problem
3.1. Execution of experiments on diverse datasets
4.1. Construction of confusion matrices
4.2. Computation of ROC curves
4.3. Computation of Precision-Recall curves
4.4. Determination of aggregate metrics
5.1. Post-processing of results using Analytic hierarchy process

Figure 1 – Research Stages

During the preparatory phase of the study, the ML methods whose effectiveness will be evaluated are selected. In addition, evaluation metrics are chosen. Ready-made datasets are selected or synthetic datasets are generated. Furthermore, hierarchical decomposition of the task of selecting the optimal ML method is performed during this phase. The content of each task within the preparatory phase of the experimental study is detailed below.

Selection of ML methods for evaluating their effectiveness in anomaly detection tasks within the radio frequency spectrum. A review of the literature enabled the selection of five methods [4]–[9]. These methods are:

– Isolation Forest;
– Local Outlier Factor;
– One-Class SVM;
– Autoencoder;
– Generative Adversarial Networks.

Selection of evaluation metrics for anomaly detection methods. *Anomaly detection* is the task of identifying rare, atypical instances within a dataset. A key feature of this task is class imbalance: anomalies occur very infrequently, which means that a simple accuracy measure can be misleading. For example, a model that always classifies every instance as “normal” would achieve very high classification accuracy if anomalies constitute only a small fraction of the data [10]. Therefore, specialized metrics are used to evaluate anomaly detection models, focusing specifically on the quality of detecting the rare class (anomalies).

For the formal definition of evaluation metrics, the *Confusion Matrix* is used, which includes four indicators:

– *TP* (*True Positives*) is the number of anomalies correctly identified as anomalies;
– *TN* (*True Negatives*) is the number of normal samples correctly identified as normal;
– *FP* (*False Positives*) is the number of normal samples incorrectly classified as anomalies;
– *FN* (*False Negatives*) is the number of anomalies that the model failed to detect, i.e., incorrectly classified as normal.

На основі значень цих показників розраховують таки метрики.

1) *Accuracy* reflects the overall proportion of correct decisions among all examples [11]:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}. \quad (1)$$

Despite its widespread use, *Accuracy* can be misleadingly high in the presence of significant class imbalance (when anomalies are extremely rare).

2) To avoid bias in situations with a strong predominance of one class, *Balanced Accuracy* is used – the arithmetic mean between the *Recall* for anomalies and the *Specificity* for normal samples:

$$Balanced\ Accuracy = \frac{1}{2}\left(\frac{TP}{TP+FN} + \frac{TN}{TN+FP}\right). \tag{2}$$

This metric treats the detection of both classes as equally important, which is particularly relevant when the cost of a false positive (FP) is comparable to the damage caused by missing an anomaly (FN).

In anomaly detection evaluation, the primary focus is placed on how well the algorithm identifies all deviations (*Recall*) and how often it incorrectly labels normal points as anomalies (*Precision*).

3) *Precision* [11]:

$$Precision = \frac{TP}{TP+FP} \tag{3}$$

reflects the proportion of detected anomalies that are truly anomalous, thereby reducing the risk of an excessive number of false alarms.

4) *Recall*:

$$Recall = \frac{TP}{TP+FN} \tag{4}$$

indicates the proportion of true anomalies that have been correctly identified, thereby reducing the likelihood of missing an anomaly. Instead of the term *Recall*, the designation TPR (*True Positive Rate*) is often used.

In the context of *anomaly detection*, *Recall* is considered a critical metric when missed anomalies could lead to severe consequences (e.g., fraud) [10]. High *Precision* , on the other hand, is essential when minimizing the number of false alarms is a priority (e.g., in medical or industrial systems).

5) To balance *Precision* and *Recall* within a single metric, the $F1$ - score is used – the harmonic mean of these two measures [11]:

$$F1 = 2 \cdot \frac{Recall \cdot Precision}{Recall + Precision}. \tag{5}$$

A low value of either component significantly reduces the $F1$, making it a generalized metric for evaluating anomaly detection performance at a specific threshold.

6) *Specificity* (or *True Negative Rate*) is the probability of correctly classifying a normal sample:

$$Specificity = \frac{TN}{TN+FP}. \tag{6}$$

In anomaly detection, it measures how rarely the method incorrectly labels normal instances as anomalies (i.e., it corresponds to a low FP). With high specificity, there are virtually no unnecessary alarms [13].

7) FPR (*False Positive Rate*) – the percentage of normal samples incorrectly labeled as anomalies:

$$FPR = \frac{FP}{TN+FP}. \tag{7}$$

8) The *ROC-curve* (*Receiver Operating Characteristic*) is constructed by varying the decision threshold and depicts the relationship between TPR (*Recall*) та FPR. The quantitative interpretation

of the ROC curve is provided by the $AUC = 0,1$ (*Area Under the ROC Curve*) – the area bounded by the ROC curve and the axis of the false positive rate (FPR). Values of $AUC\text{-}ROC$, close to 1 indicate a strong ability of the algorithm to distinguish between anomalous and normal samples across different thresholds [12].

The advantagec of the $AUC\text{-}ROC$ is its relative independence from overall class imbalance [12]. It reflects the ranking power of the classifier – how well it ranks anomalies higher than normal instances.

The drawback is that, under extreme imbalance between positive and negative examples, even models that perform poorly in practical applications can sometimes achieve high $AUC\text{-}ROC$ values [12].

9) FNR (*False Negative Rate*) – the percentage of anomalies that were missed:

$$FNR = \frac{FN}{FN + TP}. \tag{8}$$

In *anomaly detection* tasks, a high FNR indicates that the model has "missed" a portion of the anomalies and may be unacceptable in critical applications.

10) The *Matthews Correlation Coefficient* (MCC) takes into account all elements of the confusion matrix and can evaluate the balance of classification even in the presence of significant class imbalance [11]. Formally:

$$MCC = \frac{TP \cdot TN - FP \cdot FN}{\sqrt{TP + FP \quad TP + FN \quad TN + FP \quad TN + FN}}. \tag{9}$$

A value of 1 corresponds to perfect classification, 0 indicates random guessing, and -1 signifies complete disagreement between predictions and actual outcomes.

11) *Cohen's Kappa Coefficient* reflects the agreement between the obtained classification and the true labels, adjusted for "random agreement":

$$\kappa = \frac{\rho_0 - \rho_e}{1 - \rho_e}, \tag{10}$$

where $\rho_0 = \dfrac{TP + TN}{TP + TN + FP + FN}$ is the empirical probability of agreement;

$\rho_e = \dfrac{TP + FP \quad TP + FN \quad TN + FP \quad TN + FN}{TP + TN + FP + FN \ ^{2}}$ is the expected probability of agreement.

A value of 1 indicates perfect agreement, while 0 corresponds to the level of agreement expected by random chance.

12) $G\text{-}mean$ is considered as the geometric mean between TRP and TNR:

$$G\text{-}mean = \sqrt{\frac{TP}{TP + FN} \cdot \frac{TN}{TN + FP}}. \tag{11}$$

This metric "encourages" the algorithm to simultaneously maintain a high ability to detect anomalies (*Recall*) and avoid incorrectly labeling normal instances as anomalies (*Specificity*).

According to studies [10]–[13], the use of a combined set of metrics provides the most comprehensive evaluation of the effectiveness of machine learning methods in anomaly detection tasks.

The developed methodology for assessing the effectiveness of machine learning methods in anomaly detection within the radio frequency spectrum involves the integrated use of the 12 metrics described above.

Selection/Formation of Datasets. The experimental evaluation of machine learning methods for anomaly detection in the radio frequency spectrum is conducted using two datasets. *The generation of synthetic data* is performed during the preparatory phase.

Due to the need for an initial evaluation of the methods on relatively simple material, a synthetic two-dimensional dataset was created with clearly separated normal and anomalous samples (Fig. 2). Specifically, the normal data were generated according to a $N(0,1)$ distribution, while the anomalous data were generated according to a $N(5,1)$ distribution. This choice of parameters ensures a noticeable shift between the centers of the two groups, simplifying the problem setup.

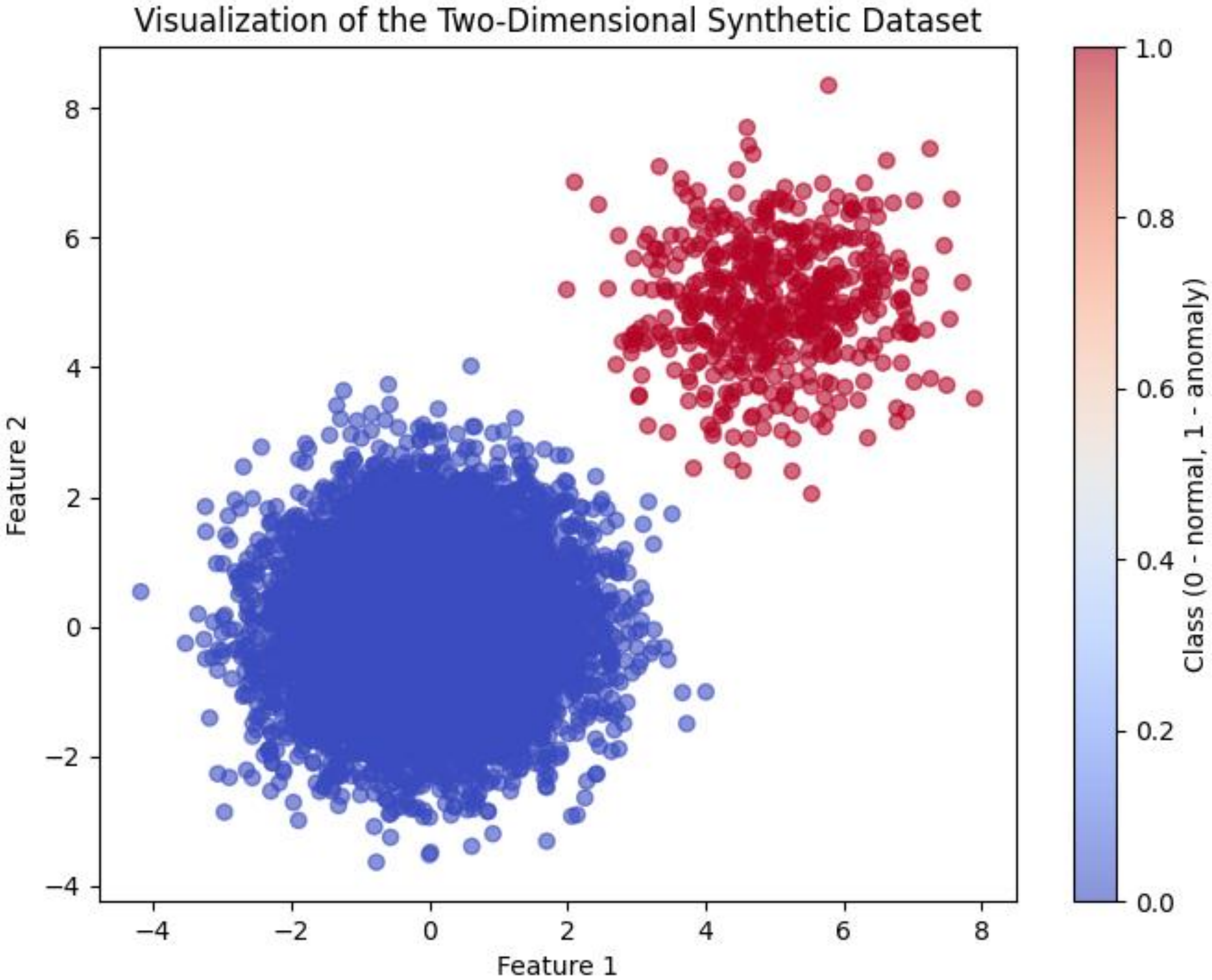

Figure 2 – Visualization of the Two-Dimensional Synthetic Dataset

In addition to the dimensionality of the space, which in this case is $d = 2$, the sample size also significantly affects robustness. To achieve sufficient statistical coverage, 10,000 normal examples and 500 anomalous examples were generated, clearly demonstrating the algorithms' ability to handle both the dominant class and the relatively rare cases.

To evaluate the performance of the algorithms under conditions closer to real-world applications, a complex dataset was generated consisting of 10 radio signal parameters: frequency, amplitude, phase, modulation index, signal-to-noise ratio (SNR), bandwidth, symbol rate, power, noise variance, and carrier frequency offset (Fig. 3).

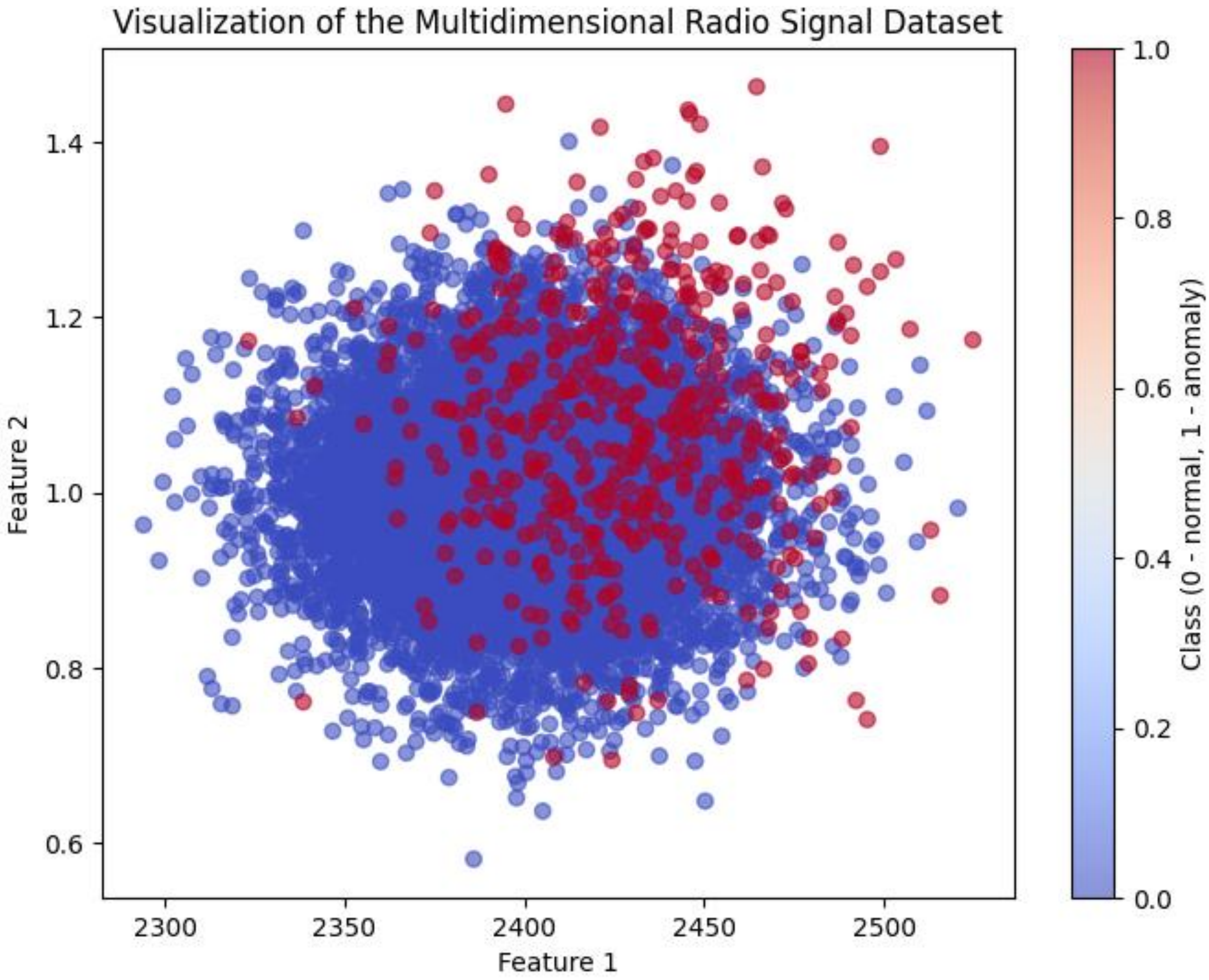

Figure 3 – Visualization of the Multidimensional Radio Signal Dataset

Normal signals were created based on distributions centered around “typical” values (e.g., ~ 2400 MHz for frequency, ~ 25 dB for SNR), whereas anomalous signals exhibited shifts in these characteristics (e.g., increased frequency and amplitude, decreased SNR, etc.).

Hierarchical decomposition of the task of selecting the optimal ML method. From the problem statement above regarding the evaluation of the effectiveness of machine learning methods in anomaly detection within the radio frequency spectrum, it is evident that this is a multi-criteria selection task over a space of alternatives. One of the well-known methods for solving such tasks is the *Analytic Hierarchy Process* (AHP) [14]. We construct a hierarchical model. At the first level is the goal of the study (evaluation of the effectiveness of ML methods). The second level of the hierarchy consists of the evaluation metrics. The third level comprises the ML methods (Fig. 4).

Next, it is necessary to assign weights to the selection criteria (in this case, the metrics) and to form the vector Ω [14].

$$\begin{gathered} \Omega = \quad \omega_i \quad , \\ \sum_i \omega_i = 1, \end{gathered} \tag{12}$$

where ω_i is the relative weight of the i-th metric.

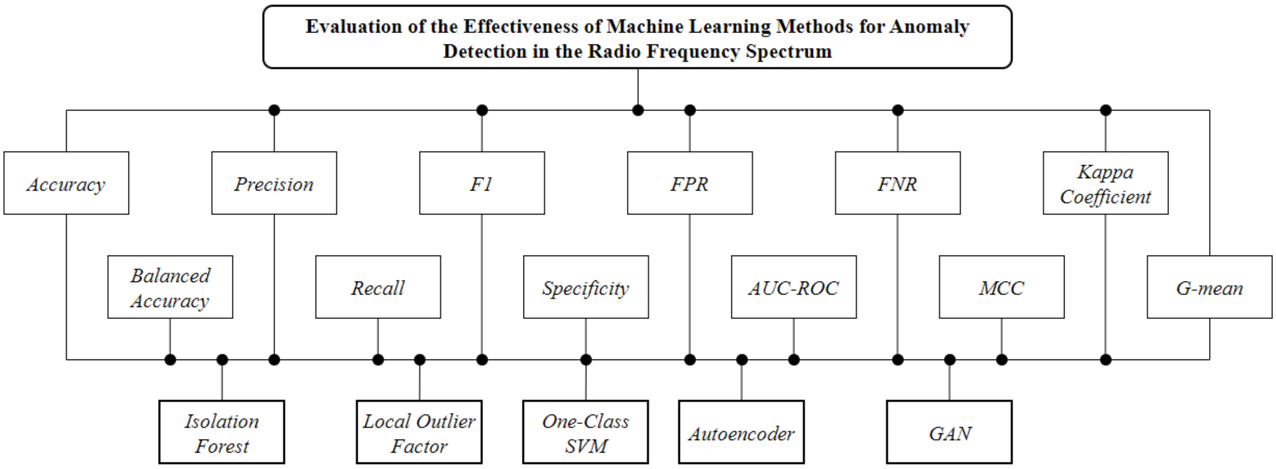

Figure 4 – Hierarchical Decomposition of the ML Methods Selection Task

The vector Ω (12) is determined by experts who are involved in the interpretation of the experimental study results.

Conclusions and prospects for further research. A methodology has been developed for investigating the feasibility of applying machine learning methods to the task of anomaly detection in the radio frequency spectrum. The preparatory phase of the methodology includes:

– the selection of five machine learning methods based on a review of the literature;

– the selection of evaluation metrics for assessing the effectiveness of ML methods (12 metrics);

– the hierarchical decomposition of the ML method selection task, based on the AHP, into a three-level model.

Further research will involve conducting a computational experiment, followed by the analysis and interpretation of its results.

REFERENCE

[1] I. Burgetova, P. Matousek, and O. Rysavy, “Anomaly Detection of ICS Communication Using Statistical Models”, in *Proc. 17th Int. Conf. on Network and Service Management (CNSM)*, Izmir, Turkey, 2021, pp. 166-172.

[2] J. Hochenbaum, O.S. Vallis, and A. Kejariwal, “Automatic Anomaly Detection in the Cloud Via Statistical Learning”, *arXiv preprint arXiv:1704.07706*, Apr. 2017. [Online]. Available: https://arxiv.org/abs/1704.07706. Accessed on: Jan. 28, 2025.

[3] Y. Cissokho, S. Fadel, R. Millson, R. Pourhasan, and P. Boily, “Anomaly Detection and Outlier Analysis”, *Data Science Report Series*, University of Ottawa, Ottawa, Canada, 2020. [Online]. Available: https://www.data-action-lab.com/wp-content/uploads/2020/09/DSRS_ADOA.pdf. Accessed on: Feb. 02, 2025.

[4] S. Tschimben, and K. Gifford, “Anomaly Detection with Autoencoders for Spectrum Sharing and Monitoring”, in *Proc. 2022 IEEE Communications Quality and Reliability Workshop (CQR)*, Arlington, VA, USA, Sept. 13, 2022, pp. 37-42, doi: https://doi.org/10.1109/CQR54764.2022. 9918589.

[5] N. S. Senol, M. Baza, A. Rasheed, and M. Alsabaan, “Privacy-Preserving Detection of Tampered Radio-Frequency Transmissions Utilizing Federated Learning in LoRa Networks”, *Sensors*, vol. 24, no. 22, p. 7336, Nov. 2024, doi: https://doi.org/10.3390/s24227336.

[6] N. S. Senol, M. Baza, A. Rasheed, and M. Alsabaan, “Identifying Tampered Radio-Frequency Transmissions in LoRa Networks Using Machine Learning”, *Sensors*, vol. 24, no. 20, p. 6611, Oct. 2024, doi: https://doi.org/10.3390/s24206611.

[7] The scikit-learn developers, “sklearn.ensemble.IsolationForest”, *scikit-learn 1.6.1 documentation*, [Online]. Available: https://scikit-learn.org/stable/modules/generated/sklearn.ensemble.IsolationForest.html. Accessed on: Feb. 03, 2025.

[8] Y. Lim, “Unsupervised Outlier Detection with Isolation Forest”, *Medium*, Mar. 17, 2022. [Online]. Available: https://medium.com/@limyenwee_19946/unsupervised-outlier-detection-with-isolation-forest-eab398c593b2. Accessed on: Feb. 03, 2025.

[9] The scikit-learn developers, “sklearn.neighbors.LocalOutlierFactor”, *scikit-learn 1.6.1 documentation*, [Online]. Available: https://scikit-learn.org/stable/modules/generated/sklearn.neighbors.LocalOutlierFactor.html. Accessed on: Feb. 03, 2025.

[10] A. Athalye, C. Northcutt, and J. Mueller, “Class Imbalance, Outliers, and Distribution Shift”, *Introduction to Data-Centric AI*, MIT CSAIL, Jan. 19, 2024. [Online]. Available: https://dcai.csail.mit.edu/2024/imbalance-outliers-shift/. Accessed on: Feb. 05, 2025.

[11] O. Rainio, J. Teuho, and R. Klén, “Evaluation metrics and statistical tests for machine learning”, *Scientific Reports*, vol. 14, Art. no. 6086, Mar. 2024, doi: https://doi.org/10.1038/s41598-024-56706-x.

[12] J. Brownlee, “ROC Curves and Precision-Recall Curves for Imbalanced Classification”, *Machine Learning Mastery*, Oct. 12, 2019. [Online]. Available: https://machinelearningmastery.com/roc-curves-and-precision-recall-curves-for-imbalanced -classification/. Accessed on: Feb. 05, 2025.

[13] C.C. Aggarwal, *Outlier Analysis*, 2nd ed. Cham, Switzerland: Springer, 2017.

[14] T.L. Saaty, *Fundamentals of Decision Making and Priority Theory with the Analytic Hierarchy Process*, Pittsburgh, PA: RWS Publications, 2000.

The article was received 10.03.2025.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] I. Burgetova, P. Matousek, and O. Rysavy, “Anomaly Detection of ICS Communication Using Statistical Models”, in *Proc. 17th Int. Conf. on Network and Service Management (CNSM)*, Izmir, Turkey, 2021, pp. 166-172.

[2] J. Hochenbaum, O.S. Vallis, and A. Kejariwal, “Automatic Anomaly Detection in the Cloud Via Statistical Learning”, *arXiv preprint arXiv:1704.07706*, Apr. 2017. [Online]. Available: https://arxiv.org/abs/1704.07706. Accessed on: Jan. 28, 2025.

[3] Y. Cissokho, S. Fadel, R. Millson, R. Pourhasan, and P. Boily, “Anomaly Detection and Outlier Analysis”, *Data Science Report Series*, University of Ottawa, Ottawa, Canada, 2020. [Online]. Available: https://www.data-action-lab.com/wp-content/uploads/2020/09/DSRS_ADOA.pdf. Accessed on: Feb. 02, 2025.

[4] S. Tschimben, and K. Gifford, “Anomaly Detection with Autoencoders for Spectrum Sharing and Monitoring”, in *Proc. 2022 IEEE Communications Quality and Reliability Workshop*

(CQR), Arlington, VA, USA, Sept. 13, 2022, pp. 37-42, doi: https://doi.org/10.1109/CQR54764.2022. 9918589.

[5] N. S. Senol, M. Baza, A. Rasheed, and M. Alsabaan, “Privacy-Preserving Detection of Tampered Radio-Frequency Transmissions Utilizing Federated Learning in LoRa Networks”, *Sensors*, vol. 24, no. 22, p. 7336, Nov. 2024, doi: https://doi.org/10.3390/s24227336.

[6] N. S. Senol, M. Baza, A. Rasheed, and M. Alsabaan, “Identifying Tampered Radio-Frequency Transmissions in LoRa Networks Using Machine Learning”, *Sensors*, vol. 24, no. 20, p. 6611, Oct. 2024, doi: https://doi.org/10.3390/s24206611.

[7] The scikit-learn developers, “sklearn.ensemble.IsolationForest”, *scikit-learn 1.6.1 documentation*, [Online]. Available: https://scikit-learn.org/stable/modules/generated/sklearn. ensemble.IsolationForest.html. Accessed on: Feb. 03, 2025.

[8] Y. Lim, “Unsupervised Outlier Detection with Isolation Forest”, *Medium*, Mar. 17, 2022. [Online]. Available: https://medium.com/@limyenwee_19946/unsupervised-outlier-detection-with-isolation-forest-eab398c593b2. Accessed on: Feb. 03, 2025.

[9] The scikit-learn developers, “sklearn.neighbors.LocalOutlierFactor”, *scikit-learn 1.6.1 documentation*, [Online]. Available: https://scikit-learn.org/stable/modules/generated/sklearn. neighbors.LocalOutlierFactor.html. Accessed on: Feb. 03, 2025.

[10] A. Athalye, C. Northcutt, and J. Mueller, “Class Imbalance, Outliers, and Distribution Shift”, *Introduction to Data-Centric AI*, MIT CSAIL, Jan. 19, 2024. [Online]. Available: https://dcai.csail.mit.edu/2024/imbalance-outliers-shift/. Accessed on: Feb. 05, 2025.

[11] O. Rainio, J. Teuho, and R. Klén, “Evaluation metrics and statistical tests for machine learning”, *Scientific Reports*, vol. 14, Art. no. 6086, Mar. 2024, doi: https://doi.org/10.1038/s41598-024-56706-x.

[12] J. Brownlee, “ROC Curves and Precision-Recall Curves for Imbalanced Classification”, *Machine Learning Mastery*, Oct. 12, 2019. [Online]. Available: https://machinelearningmastery.com/roc-curves-and-precision-recall-curves-for-imbalanced -classification/. Accessed on: Feb. 05, 2025.

[13] C.C. Aggarwal, *Outlier Analysis*, 2nd ed. Cham, Switzerland: Springer, 2017.

[14] T.L. Saaty, *Fundamentals of Decision Making and Priority Theory with the Analytic Hierarchy Process*, Pittsburgh, PA: RWS Publications, 2000.

ВЯЧЕСЛАВ РЯБЦЕВ,
ПАВЛО ПАВЛЕНКО

МЕТОДИ МАШИННОГО НАВЧАННЯ У ЗАДАЧІ ВИЯВЛЕННЯ АНОМАЛІЙ У РАДІОЧАСТОТНОМУ СПЕКТРІ: МЕТОДИКА ДОСЛІДЖЕННЯ

Досвід останніх трьох років повномасштабної війни свідчить про динамічну трансформацію концептуальних засад бойових дій та зміни пріоритетності засобів їх ведення. Так, поява та все більш активне застосування різноманітних безпілотних систем, широке використання високоточних засобів ураження та новітніх засобів радіоелектронної протидії визначають стратегічний характер радіочастотного спектру. Забезпечення безперервного спектрального моніторингу та виявлення аномальної активності в ефірі стає критично важливою складовою систем радіоелектронної боротьби, радіо- та радіотехнічної розвідки, захищеного зв’язку. Традиційні підходи до аналізу сигналів, що ґрунтуються на фіксованих порогових значеннях, евристичних правилах або апріорних статистичних припущеннях, виявляють свою недостатню ефективність у високодинамічному та зашумленому середовищі сучасного радіоефіру.

У зв’язку з цим виникає потреба у дослідженні інноваційних підходів, зокрема методів машинного навчання, на здатність забезпечення автоматичного виявлення аномальних сигналів без потреби у маркованих даних. Такі рішення мають підвищити точність, адаптивність та швидкість реагування в системах спектрального моніторингу.

Запропоновано методику дослідження доцільності використання методів машинного навчання у задачі виявлення аномалій у радіочастотному спектрі з урахуванням складності структури даних, їх багатовимірності та обмеженості апріорної інформації про аномальні зразки. Ця методика дослідження включає етапи:

- постановки задачі експерименту;
- відбору методів виявлення аномалій для експериментального дослідження;
- вибору метрик оцінювання;
- вибору / формуванню наборів тестових даних (датасетів);
- безпосереднього проведення експериментального дослідження;
- аналізу та оцінки результатів;
- візуалізації та інтерпретації одержаних результатів;
- формування висновків за результатами експерименту.

Дана стаття присвячена теоретичній складовій експериментального дослідження. Практичні результати будуть опубліковані окремо.

Ключові слова: штучний інтелект, задача виявлення аномалій, машинне навчання, радіочастотний спектр, класифікація, метод аналізу ієрархій, *Isolation Forest*, *Autoencoder*, *Local Outlier Factor* (*LOF*), *One-Class SVM*, *Generative Adversarial Networks* (*GAN*).

Riabtsev Viacheslav, candidate of technical sciences, associate professor, associate professor at the cybersecurity and application of information systems and technologies academic department, Institute of special communications and information protection of National technical university of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine. ORCID 0000-0001-8331-0132, viacheslav.riabtsev@gmail.com.

Pavlenko Pavlo, cadet, Institute of special communications and information protection of National technical university of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine. ORCID 0009-0001-8825-0623, plamatag@gmail.com.

Рябцев Вячеслав Віталійович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки і застосування інформаційних систем і технологій, Інститут спеціального зв’язку та захисту інформації Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського”, Київ, Україна.

Павленко Павло Тарасович, курсант, Інститут спеціального зв’язку та захисту інформації Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського”, Київ, Україна.