Information systems. Computer sciences. Issues of information security
Информационные системы. Информатика. Проблемы информационной безопасности

UDC 621.311.1
https://doi.org/10.32362/2500-316X-2024-12-6-7-19
EDN LEDVEZ

RESEARCH ARTICLE

Cybersecurity of smart grids: Comparison of machine learning approaches training for anomaly detection

Sergey V. Kochergin [@], Svetlana V. Artemova, Anatoly A. Bakaev, Evgeny S. Mityakov, Zhanna G. Vegera, Elena A. Maksimova

MIREA – Russian Technological University, Moscow, 119454 Russia
[@] Corresponding author, e-mail: kochergin_s@mirea.ru

Abstract

Objectives. The transformation of modern electric grids into decentralized smart grids presents new challenges in the field of cybersecurity. The purpose of this work is to conduct research and analysis into the effectiveness of different machine-learning methods for identifying anomalies in decentralized smart networks, including cyberattacks and emergency modes, as well as to develop recommendations on the optimal combination of these methods for ensuring effective cybersecurity under conditions of changing electrical loads.

Methods. We consider several machine learning methods for identifying anomalies in power systems that simulate network behavior under conditions of cyberattacks and emergency modes. The relative effectiveness of such methods as multifractal analysis using wavelets, the Isolation Forest model, local outlier factor (LOF), *k*-means clustering, and one-class support vector machine (One-Class SVM), is analyzed.

Results. The comparison of machine learning methods reveals the varying effectiveness of anomaly detection methods used to detect cyber threats and deviations in electrical systems. Isolation Forest is best at detecting abrupt changes related to cyberattacks with high accuracy and a minimum of false positives. While LOF can also be effective in detecting cyberattacks, its increased sensitivity to minor deviations increases the number of false positives. *K*-means and One-Class SVMs are less effective in detecting abrupt anomalies but are useful for general clustering of data and detecting both abrupt and smooth changes, respectively.

Conclusions. The obtained research results indicate the advantages of using a combination of machine learning algorithms to ensure the reliable protection of smart networks from cyberattacks taking into account the nature of the electrical load.

Keywords: smart grids, cybersecurity, machine learning, anomaly detection, Isolation Forest, cyberattacks

• **Submitted:** 12.09.2024 • **Revised:** 25.09.2024 • **Accepted:** 01.10.2024

For citation: Kochergin S.V., Artemova S.V., Bakaev A.A., Mityakov E.S., Vegera Zh.G., Maksimova E.A. Cybersecurity of smart grids: Comparison of machine learning approaches training for anomaly detection. *Russ. Technol. J.* 2024;12(6):7–19. https://doi.org/10.32362/2500-316X-2024-12-6-7-19

Financial disclosure: The authors have no financial or proprietary interest in any material or method mentioned.

The authors declare no conflicts of interest.

НАУЧНАЯ СТАТЬЯ

Кибербезопасность смарт-сетей: сравнение подходов машинного обучения для обнаружения аномалий

С.В. Кочергин [@], **С.В. Артемова**, **А.А. Бакаев**, **Е.С. Митяков**, **Ж.Г. Вегера**, **Е.А. Максимова**

МИРЭА – Российский технологический университет, Москва, 119454 Россия
[@] *Автор для переписки, e-mail: kochergin_s@mirea.ru*

Резюме

Цели. Современные электрические сети, трансформирующиеся в децентрализованные смарт-сети, сталкиваются с новыми вызовами в области кибербезопасности. Цель работы – провести исследование и анализ эффективности различных методов машинного обучения для выявления аномалий в децентрализованных смарт-сетях, включая кибератаки и аварийные режимы, для разработки рекомендаций по оптимальному сочетанию этих методов для обеспечения эффективной кибербезопасности в условиях изменяющейся электрической нагрузки.

Методы. Рассматриваются различные методы машинного обучения для выявления аномалий в энергосистемах, моделирующих поведение сети в условиях кибератак и аварийных режимов. Проведен анализ эффективности таких методов, как мультифрактальный анализ с использованием вейвлетов и модель изолированного леса (Isolation Forest), локальный коэффициент выбросов (local outlier factor, LOF), кластеризация методом *k*-средних и одноклассовая машина опорных векторов (One-Class SVM).

Результаты. Рассмотрены различные методы машинного обучения для выявления аномалий в энергосистемах, моделирующих поведение сети в условиях кибератак и аварийных режимов. Методы обнаружения аномалий показали разную эффективность в выявлении киберугроз и отклонений в электрических системах. Метод Isolation Forest лучше всего обнаруживает резкие изменения, связанные с кибератаками, высокой точностью и минимумом ложных срабатываний. Метод LOF также может выявлять кибератаки, но его повышенная чувствительность к мелким отклонениям увеличивает число ложных срабатываний. Методы *k*-средних и One-Class SVM менее эффективны в выявлении резких аномалий, но полезны для общей кластеризации данных и обнаружения как резких, так и плавных изменений соответственно.

Выводы. Полученные результаты исследований указывают на то, что для обеспечения надежной защиты смарт-сетей от кибератак следует использовать комбинацию алгоритмов машинного обучения с учетом характера электрической нагрузки.

Ключевые слова: смарт-сети, кибербезопасность, машинное обучение, выявление аномалий, Isolation Forest, кибератаки

• **Поступила:** 12.09.2024 • **Доработана:** 25.09.2024 • **Принята к опубликованию:** 01.10.2024

Для цитирования: Кочергин С.В., Артемова С.В., Бакаев А.А., Митяков Е.С., Вегера Ж.Г., Максимова Е.А. Кибербезопасность смарт-сетей: сравнение подходов машинного обучения для обнаружения аномалий. *Russ. Technol. J*. 2024;12(6):7–19. https://doi.org/10.32362/2500-316X-2024-12-6-7-19

Прозрачность финансовой деятельности: Авторы не имеют финансовой заинтересованности в представленных материалах или методах.

Авторы заявляют об отсутствии конфликта интересов.

INTRODUCTION

Modern power grids are being rapidly transformed into decentralized systems with the introduction of smart grids and distributed power generation. Such grids, comprising cyberphysical systems, face new cybersecurity challenges related to the need to protect distributed components from potential multilayered attacks [1–5]. Due to the inadequacy of using traditional antivirus software for protecting such networks, the professional community has been paying more attention to the issue of endpoint protection, including Endpoint Detection and Response (EDR) [6].

A special feature of the EDR system lies in its capability to use behavioral analysis for detecting suspicious activity and detecting changes in the configuration of endpoints and nodes of the electrical network and directly connected electrical equipment. For example, the actions of intruders using fileless methods can manifest themselves in changes in electrical energy parameters (voltage, resistance) and false commands to switch equipment.

Smart grids protection requires the development of new behavioral analysis methods that take into account the peculiarities of their technological modes of operation.

STUDY AND CLASSIFICATION OF HARMONIC DISTORTIONS AND ANOMALOUS SIGNALS CAUSED BY CYBERATTACKS

The primary focus of cyberattacks on smart grids is to create the conditions to maximize the damage of disruption. One cyberattack approach that poses a significant threat consists in tampering with the voltage regulation control system. This exploits a vulnerability connected with the use of transformers with automatic voltage regulation to maintain the required voltage level. The most common regulation method involves the use of load-side regulation transformers [7–9].

Unusual commands and actions during a cyberattack on the electric grid can manifest themselves in a variety of ways that differ from normal system behavior. For example, a command to change a transformer's transformer ratio for no apparent reason or attempts to repeatedly log into the control system may indicate that the attackers are attempting to interfere with the system. Such anomalous actions require prompt detection and analysis to prevent possible threats.

Let us consider an example of power grid operation during a cyberattack. Here the power system is operating in normal mode with all parameters within acceptable limits. Transformer T1 functions stably, providing the necessary voltage at the substation with a transformation ratio of 35(10)/0.4 kV. Suddenly a command is received to change the T1 transformer ratio, although the operator finds no reason for such a change, as the system parameters remain within normal limits. Nevertheless, the command is executed to change the transformer ratio. This causes voltage fluctuations on the low voltage side of the transformer (0.4 kV), which leads to disruption of the connected consumers' operation.

This process can trigger a rolling shutdown of automation and consequent loss of power supply to end consumers. Alarms due to deviations of network parameters appear on the dispatch panel, and operators take measures to restore normal operation. After the incident is eliminated, analysis is performed to identify the cause of sending an unauthorized command. System logs and network traffic are examined for possible cyberattacks or control system failures.

This example demonstrates the vulnerability of electrical grids in the case of intruders penetrating the control system, along with the need for early detection of anomalies (false commands).

Understanding anomalies in power grid protection is not possible without process knowledge. Cyberattacks typically differ from normal system failures due to their lack of association with obvious causal links in the fault chain. Additionally, such attacks occur suddenly, making them difficult to detect using traditional methods [10–14].

In this regard, the task of the present study is to conduct an experiment simulating the deviation of voltage in the network according to a selected anomaly analysis method, allowing it to be distinguished as accurately as possible from the normal emergency mode of operation of the electrical network.

In order to conduct the studies, synthetic data were generated to simulate electrical voltages ranging from −0.9 kV to +0.9 kV (Fig. 1). These data cover three different scenarios: normal system operation (no voltage deviation), sudden voltage deviation due to a cyberattack (no change in electrical load), and emergency operation with prolonged voltage deviation (with change in electrical load).

Under normal conditions, the voltage is described by a sinusoidal time function $U = f(t)$ with the addition of random noise reflecting real fluctuations (Fig. 1a). To simulate a cyberattack, a sudden voltage spike of 0.3 kV was artificially introduced (Fig. 1b). Emergency operation mode with voltage deviation was simulated by increasing the amplitude of the sinusoid for a finite period of time (Fig. 1c).

In this study, several machine learning algorithms were used for the analysis of synthetic data simulating the behavior of the electric grid under cyberattack and emergency mode of electric load deviation. Unlike neural networks, which require significant computational resources, the selected methods such as Isolation Forest method, local outlier factor (LOF), one-class support vector machine (One-Class SVM), and *k*-means clustering, have less computational complexity and do not require a large dataset for learning.

Let us consider each method separately and analyze the results obtained to evaluate their effectiveness in detecting such anomalies.

Multifractal analysis and Isolation Forest method

Fractal methods can be used to detect anomalies in the data, which may indicate a change in the state of the system or the presence of external influences. This makes them useful for monitoring and diagnostics of various processes [15–17].

We apply the discrete wavelet transform for the voltage and calculate multifractal features, including the mean value and the variance of the absolute values of the coefficients. The vector of these features will be used in the Isolation Forest model [18] to detect anomalies.

Let $x(t)$ be a time series representing data (e.g., a voltage time series). In order to analyze the time series, a discrete wavelet transform is used, which decomposes the signal into several levels of detail.

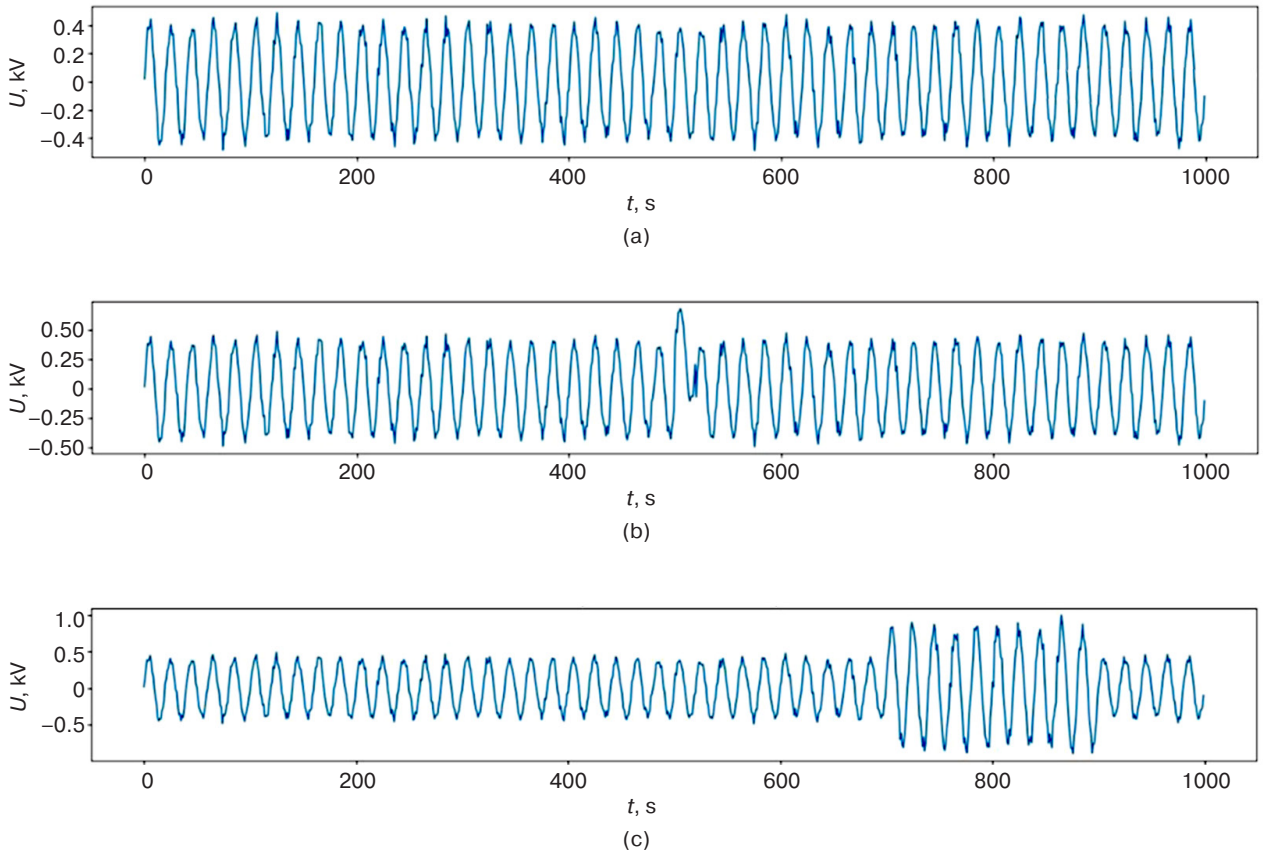

Fig. 1. Simulation of various operation modes of the power grid: normal operation mode (a); mode with cyberattack (b); normal mode with voltage deviation (c)

Wavelet transform W_x of the signal $x(t)$ at the level j can be written as:

$$W_x(t, j) = \Sigma_t x(t)\psi_{j,k}(t), \quad (1)$$

where $\psi_{j,k}(t)$ is a wavelet function, a shifted and scaled version of the mother wavelet.

For each decomposition level j, we obtain a set of coefficients c_j that describe different time scales of the signal:

$$\boldsymbol{c}_j = W_x(t, j). \quad (2)$$

At each level j of the wavelet decomposition, the mean and variance of the absolute values of the coefficients c_j are calculated:

$$\boldsymbol{\mu}_j = \frac{1}{N_j}\sum_{k=1}^{N_j} |\mathbf{c}_{j,k}|, \quad (3)$$

$$\boldsymbol{\sigma}_j^2 = \frac{1}{N_j}\sum_{k=1}^{N_j} (|\mathbf{c}_{j,k}| - \boldsymbol{\mu}_j)^2, \quad (4)$$

where N_j is the number of coefficients at the level j.

These features make up the feature vector for each time series:

$$\mathbf{features} = [\boldsymbol{\mu}_1, \boldsymbol{\sigma}_1^2, \boldsymbol{\mu}_2, \boldsymbol{\sigma}_2^2, ..., \boldsymbol{\mu}_m, \boldsymbol{\sigma}_m^2]. \quad (5)$$

Let $\mathbf{F}_i$ be a vector of multifractal features for the ith time series, then the set of features for all-time series can be written as a matrix:

$$\mathbf{F} = [\mathbf{F}_1, \mathbf{F}_2, \ldots, \mathbf{F}_n]^{\mathrm{T}}. \quad (6)$$

In order to identify anomalies, the Isolation Forest model [18] is trained on the feature matrix $\mathbf{F}_i$. In so doing, the model builds several decision trees according to which the data are sliced based on randomly selected features in an attempt to isolate anomalous data points with the minimum tree depth.

The abnormal scores for each time series are calculated using a decision function:

$$S_i = \text{decision\_function}(\mathbf{F}_i), \quad (7)$$

where S_i is the anomaly estimate for the ith time series.

Abnormal S_i score is used to determine the extent to which a time series deviates from the normal state. Low S_i values indicate a strong anomaly, while high S_i values correspond to normal behavior.

Based on the outlined theoretical principles, a computer program was developed to create a heat map of anomalies using the Isolation Forest model based on multifractal features (Fig. 2). The use of heat maps to visualize anomalies enables visual demonstration of the recurring patterns and the separation of normal events from cyberattacks and emergency modes.

Within the heat map, the horizontal axis represents time steps (0 to 1000) representing successive measurements of the data over time, while the vertical axis represents the anomaly estimates predicted by the model. The gradient scale ranges from black, indicating high anomaly estimates (low probability of normality), to white, which indicates low anomaly estimates (high probability of normality).

Heat map analysis

1. The period is 0–500 s. Most of the data in this period is colored white, indicating low abnormal estimates. This indicates that the model classifies this data as normal.
2. The period near the time mark is equal to 500 s. Within this period, a narrow black band is observed, which corresponds to a high anomalous score.
3. This black band clearly indicates a cyberattack that was synthesized to simulate an abrupt deviation from the norm. The model successfully identified this deviation, as confirmed by the presence of a black area in the heat map.
4. The period is equal to 700–900 s. This section shows a significant variation of the color scale from black to gray, which is associated with the emergency mode in which the amplitude of the sinusoidal signal is changed. In contrast to the narrow black band indicating a cyberattack, a more complex and gradient pattern is seen here, reflecting an anomaly associated with the operating mode of voltage deviation rather than a cyberattack.
5. The period is equal to 900–1000 s. This segment is again dominated by white color, indicating normal data similar to the initial period.

LOF method

The LOF method [19] identifies local anomalies based on a comparison of the data density in the neighborhood of each point.

The LOF for each point x_i is calculated as follows:

1. The distance to the nearest neighbors is determined:

$$d_k(x_i, x_j) = \left\| x_i - x_j \right\|, \quad (8)$$

where k is the number of nearest neighbors.

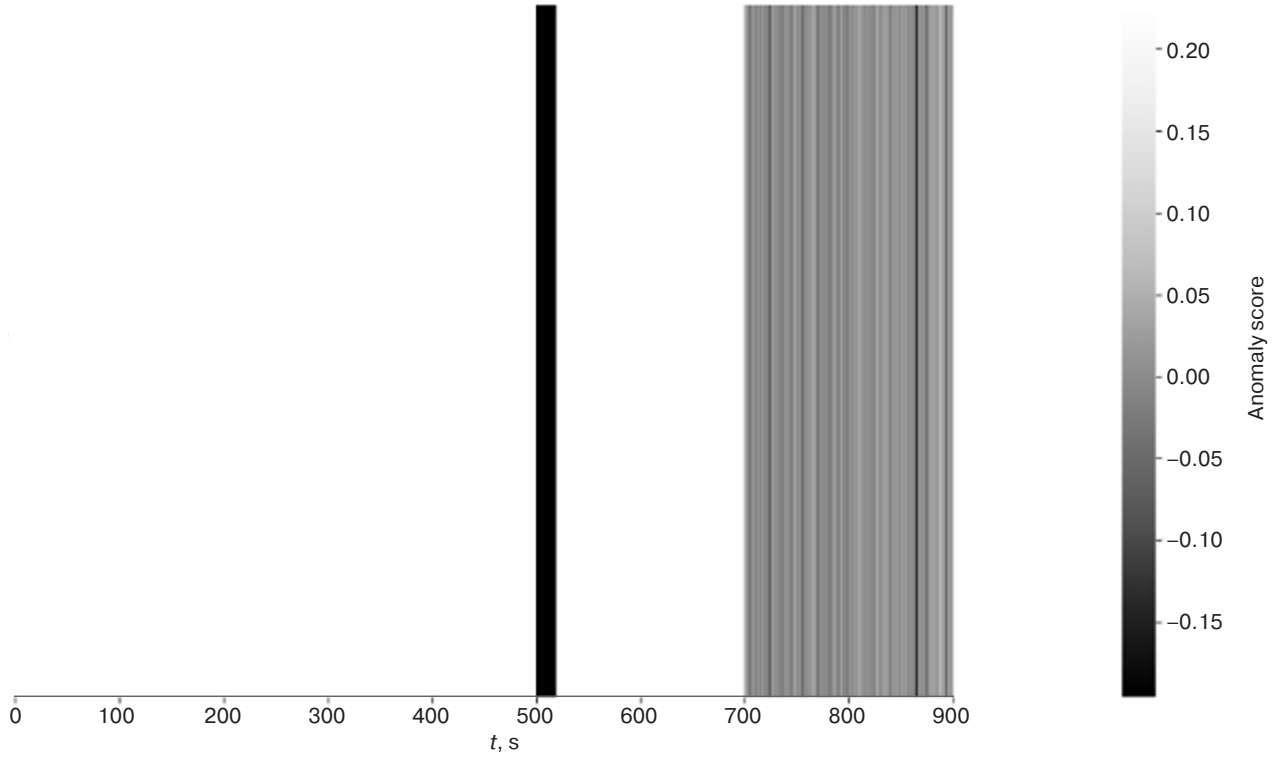

Fig. 2. Thermal anomaly map using the Isolation Forest model with multifractal objects

2. The local reachability density lrd_k for point x_i is determined:

$$\mathrm{lrd}_k(x_i) = \left(\frac{\sum_{j=1}^{k} \mathrm{reach\_dist}_k(x_i, x_j)}{k} \right)^{-1}, \quad (9)$$

where $\mathrm{reach\_dist}_k(x_i, x_j)$ is the distance one has to move from x_i to x_j in order to reach the density of x_j.

3. LOF calculation:

$$\mathrm{LOF}_k(x_i) = \frac{\sum_{j=1}^{k} \frac{\mathrm{lrd}_k(x_j)}{\mathrm{lrd}_k(x_i)}}{k}. \quad (10)$$

A value of $\mathrm{LOF}_k(x_i)$ significantly greater than 1 indicates that point x_i is anomalous.

In order to visualize the results of anomaly estimation, the obtained LOF values are inverted:

$$S_i = -\mathrm{LOF}_k(x_i), \quad (11)$$

where S_i is the anomalous estimate for the point x_i.

Based on these values, a heat map is constructed (Fig. 3), in which anomalous points are displayed in grayscale corresponding to the degree of their deviation from the norm.

The LOF method demonstrated the ability to effectively detect cyberattacks, as can be clearly seen by the black band on the heat map in the region around the 500th point of the time series. However, LOF also detected anomalies across the entire time scale, which can be both an advantage and a disadvantage. In particular, significant changes are observed in the emergency region (700–900 s), although their highlighting is not as contrastive. While the high sensitivity of LOF to local deviations and minor anomalies enables the detection of subtle changes in the data, at the same time it can lead to an increase in the number of false positives, which needs to be taken into account in the interpretation of the results.

K-means clustering method

The *k*-means method is designed to partition a dataset into *k* clusters, in which each cluster is characterized by its center (centroid) [20].

The objective of the method is to minimize the sum of squares of the distances between data points and cluster centers.

Let us have a dataset $\mathbf{X} = \{x_1, x_2, \ldots, x_n\}$, where each data point x_i is a feature vector.

The calculation consists of the following steps:

1. The number of clusters *k*into which the data should be divided is selected.

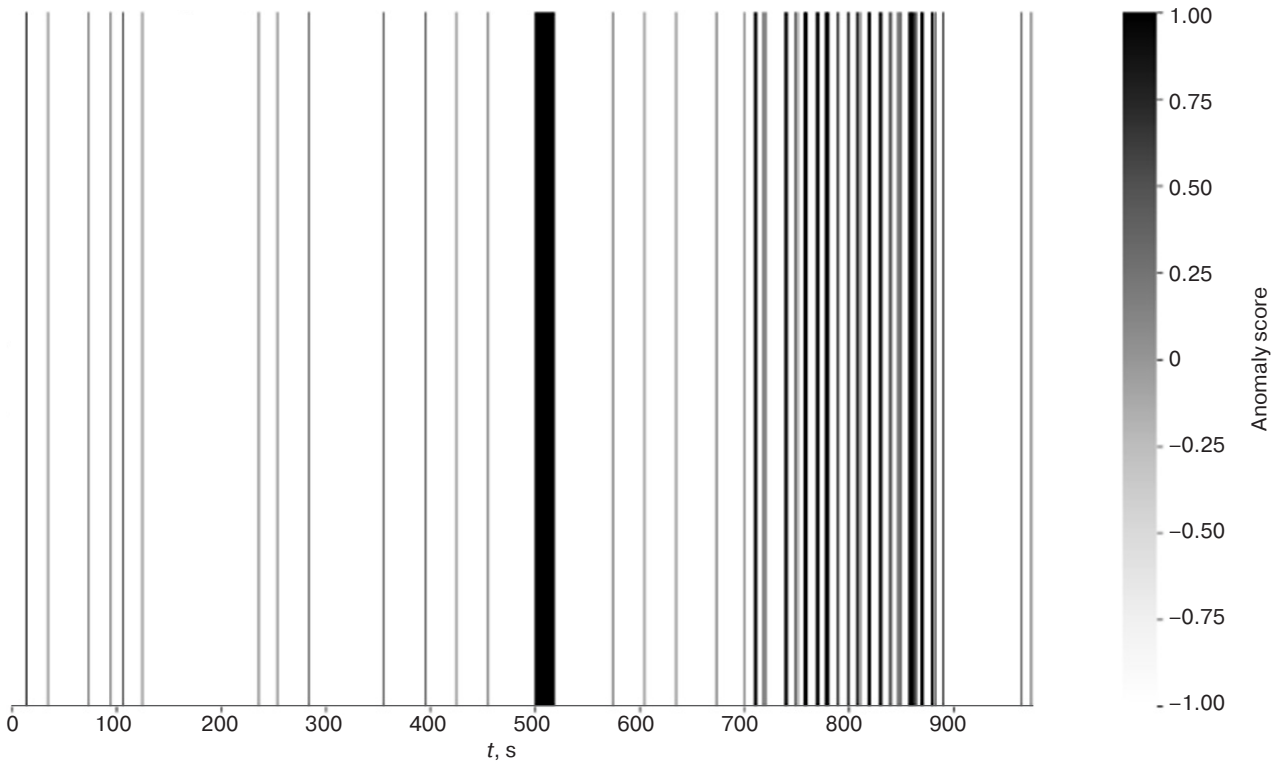

Fig. 3. Heat map of anomaly estimates using LOF

2. Initialization of centroids:

K initial centroids $\{\mu_1, \mu_2, \ldots, \mu_k\}$ are initialized, either chosen randomly from the data points or by other methods such as the *k*-means++.

3. Assigning points to clusters:

For each data point x_i, the distance to each of the centroids μ_j is calculated:

$$d(x_i, \mu_j) = \left\| x_i - \mu_j \right\|. \quad (12)$$

Point x_i is assigned to the cluster with minimum distance:

$$C_i = \arg\min_j d(x_i, \mu_j), \quad (13)$$

where C_i is the cluster to which point x_i belongs.

4. Centroid renewal:

After assigning all points, the centroids for each cluster are recalculated:

$$\mu_j = \frac{1}{|C_j|} \sum_{x_i \in C_j} x_i, \quad (14)$$

where $|C_j|$ is the number of points in the *j*th cluster, and μ_j is the new centroid position.

5. Repeat steps 3 and 4.

Steps 3 and 4 are repeated until the process converges (e.g., until the centroids stop changing or the maximum number of iterations is reached).

K-means method minimizes the following cost function (loss function):

$$J = \sum_{j=1}^{k} \sum_{x_i \in C_j} \left\| x_i - \mu_j \right\|^2, \quad (15)$$

where *J* is the total intra-cluster deviation, and $\left\| x_i - \mu_j \right\|^2$ is the square of the Euclidean distance between a data point and the centroid of its cluster.

The heat map (Fig. 4) shows the distances to cluster centers calculated using the *k*-means clustering method. Time steps are plotted on the horizontal axis are plotted on the vertical axis along with distances to cluster centers. The gradient scale ranges from light gray to black, where black areas correspond to the maximum values of the distances.

While the results obtained via *k*-means clustering method demonstrate its effectiveness in dealing with large anomalies, the approach can produce errors for smooth changes. Therefore, the use of this method should be combined with other methods for a more comprehensive analysis of anomalies.

One-Class SVM method

The One-Class SVM method [21] has a number of features that make it particularly suitable for anomaly detection tasks in critical systems such as electrical

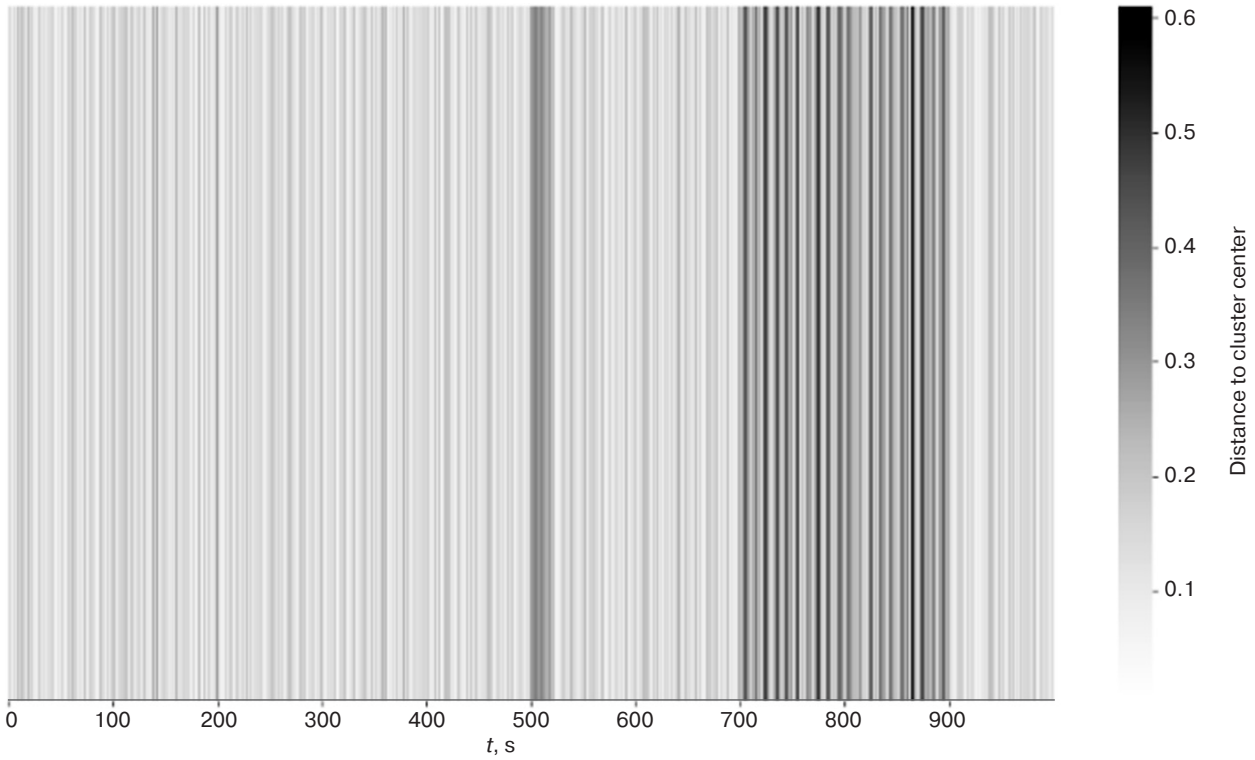

Fig. 4. Heat map of distances to cluster centers using *k*-means clustering

grids. Unlike other methods, One-Class SVM aims to train a model that describes the distribution of normal data and can then be used to detect outliers that do not follow this distribution. This approach is particularly useful in environments where there is limited data on abnormal states or cyberattacks and where the focus is on detecting deviations from the normal state of the system.

In mathematical terms, the One-Class SVM method constructs a hyperplane in feature space that separates all data points from the origin and seeks to maximize the distance between this hyperplane and the closest data points to it. The goal is to have all normal data on one side of the hyperplane and anomalies on the other side.

Formally, let $\mathbf{x}_i$ denote a vector of time series features, where $i = 1, 2, \ldots, n$. One-Class SVM model solves the following optimization problem:

$$\min_{\mathbf{w},\rho,\xi_i} \frac{1}{2}\|\mathbf{w}\|^2 + \frac{1}{\nu n}\sum_{i=1}^{n}\xi_i - \rho \qquad (16)$$

provided:

$$(\mathbf{w} \cdot \phi(\mathbf{x}_i)) \geq \rho - \xi_i,\ \xi_i \geq 0,\ i = 1, 2, \ldots, n. \qquad (17)$$

Here $\mathbf{w}$ is the vector of weights; ρ is the hyperplane offset; ξ_i are the slack variables; $\phi(\mathbf{x}_i)$ is the mapping function to the high-dimensional feature space; ν is a hyperparameter controlling the allowable proportion of outliers and model complexity.

The result of the One-Class SVM is a decision-making function:

$$f(\mathbf{x}) = (\mathbf{w} \cdot \phi(\mathbf{x})) - \rho. \qquad (18)$$

Values of $f(\mathbf{x}) \geq 0$ indicate potential anomalies, whereas values of $f(\mathbf{x}) < 0$ correspond to normal data.

By performing the calculation using the One-Class SVM method, we obtain the results that are shown in the heat map (Fig. 5).

The One-Class SVM method demonstrated high efficiency in detecting both sharp and smooth anomalies in synthetic data modeling the operation of the electrical grid. The ability of this method to detect different types of abnormalities is confirmed by contrasting regions in the heat map corresponding to both cyberattack and fault mode. This approach can be useful for monitoring critical infrastructures, where it is important to detect anomalies in time to prevent system disturbances.

CONCLUSIONS

Based on the heat map analysis, different anomaly detection methods can be concluded to have varying degrees of effectiveness in the context of detecting cyber threats and other abnormalities in electrical systems. The Isolation Forest method performed best in detecting

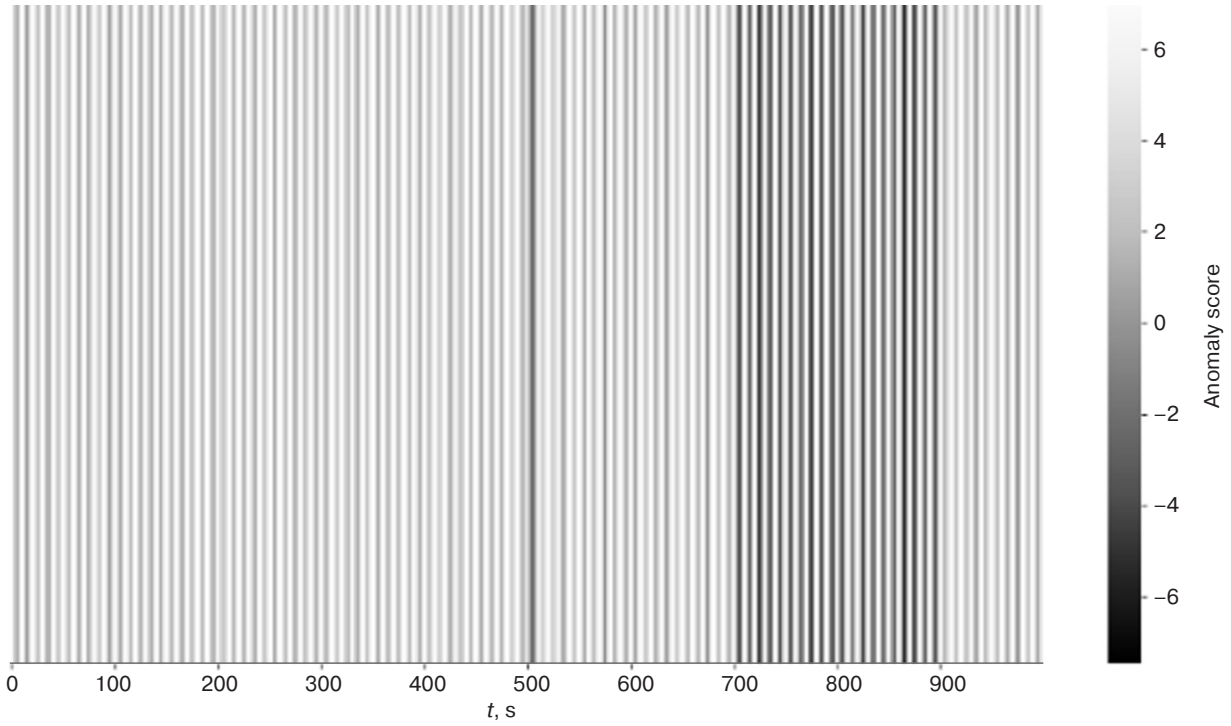

Fig. 5. Heat map of anomaly estimations using the One-Class SVM method

abrupt changes associated with cyberattacks, highlighting such anomalies with high accuracy and producing minimal false positives. While the LOF method also demonstrated an ability to detect cyberattacks, its increased sensitivity to small deviations led to an increased number of false positives, which requires additional attention when interpreting the results.

While the *k*-means clustering and One-Class SVM methods were shown to be less contrastive than Isolation Forest, they also have certain advantages. The *k*-means clustering method proved useful for general clustering of the data but was less effective in detecting sharp anomalies. The One-Class SVM method, on the other hand, demonstrated the ability to detect both abrupt and smooth changes, but with less contrast in highlighting anomalies, which also needs to be considered when selecting the appropriate method for the task of monitoring and protecting critical infrastructures. In general, Isolation Forest can be recommended for detecting cyber threats; however, in order to provide comprehensive anomaly analysis, it is recommended to use several methods in combination.

The presented research confirms the need to combine different methods depending on the nature of electrical load variation in order to effectively prevent cyberattacks on smart grids.

Authors' contributions

S.V. Kochergin—developing the research concept, identifying the main problems, formulating aims and objectives; literature review in cybersecurity for smart grids; preparing the materials for experiments and conducting the experiments.

S.V. Artemova—developing the research methodology, selecting approaches of machine learning for comparison; preparing the article and its editing.

A.A. Bakaev—determining the research topic and discussing the final text of the article.

E.S. Mityakov—interpreting the research results and preparing conclusions.

Zh.G. Vegera—mathematical interpretation of the research.

E.A. Maksimova—analysis of existing anomaly detection methods and identification of the most promising ones for comparison.

Each author uniquely contributed to preparing the research article.

REFERENCES

1. Ihsanov I.I. Security in the electric power industry: current threats and protective measures. In: *Youth and Knowledge – Guarantee of Success – 2023: Collection of Scientific Articles of the 10th International Youth Scientific Conference*. Kursk, September 19–20, 2023. Kursk: Universitetskaya kniga; 2023. V. 2. P. 472–474 (in Russ.). URL: https://elibrary.ru/tfyddx
2. Papkov B.V., Osokin L.V., Kuchin N.N. Cyber security of distribution facilities electrical networks. *Sel'skii mekhanizator = Selskiy Mechanizator*. 2024;5:3–7 (in Russ.). Available from URL: https://elibrary.ru/tfmvhi
3. Kolosok I.N., Korkina E.S. Analysis of cybersecurity of power facilities taking into account the mechanism and kinetics of undesirable processes. *Energetik*. 2024;2:3–8 (in Russ.). http://doi.org/10.34831/EP.2024.60.27.001, available from URL: https://elibrary.ru/ecxvjp
4. Abdrakhmanov I.I. Dangers and threats to cybersecurity in the electric power industry: analysis of modern threats and protection mechanisms. *Nauchnyi Aspekt*. 2024;31(3):3970–3973 (in Russ.). Available from URL: https://elibrary.ru/lrouni
5. Gurina L.A. Assessment of cyber resilience of the operational dispatch control system of EPS. *Voprosy kiberbezopasnosti = Cybersecurity Issues*. 2022;3(49):23–31 (in Russ.). Available from URL: https://elibrary.ru/sapiyh
6. Smetanin D.I. Studying the structure of the System for detecting and countering attacks of ransomware viruses based on Endpoint Detection and Response. In: *Topical Issues of Modern Science: Collection of articles of the 7th International Scientific and Practical Conference*: in 2 v. Penza: Nauka i Prosveshchenie; 2023. V. 1. P. 60–64 (in Russ.). Available from URL: https://elibrary.ru/vuvfpa
7. Lezhnyuk P.D., Rubanenko A.E., Kazmiruk O.I. Optimal control of normal modes of the EES, taking into account the technical condition of transformers with RPN. *Nauchnye trudy Vinnitskogo natsional'nogo tekhnicheskogo universiteta = Scientific Works of Vinnytsia National Technical University*. 2012;4:2 (in Russ.). Available from URL: https://elibrary.ru/pyqugn
8. Kopylova V.V., Parkachev K.N., Tiguntsev S.G. Transformer with thyristor on-load RPN changers. *Elektrooborudovanie: ekspluatatsiya i remont.* 2019;12:35–39 (in Russ.). Available from URL: https://elibrary.ru/vgfudv
9. Arzhannikov B.A., Baeva I.A., Tarasovskii T.S. Thyristor devices for voltage regulation of transformers under load RPN. *Transport Aziatsko-Tikhookeanskogo regiona = Transport of the Asia-Pacific Region*. 2020;4(25):32–38 (in Russ.). Available from URL: https://elibrary.ru/lxmknj
10. Ragozin A.N. Forming a forecast of multicomponent time series of data using digital filtering methods and a predictive auto-encoder in order to detect anomalies in the operation of automated process control systems under the influence of cyberattacks. *Vestnik UrFO. Bezopasnost' v informatsionnoi sfere = Journal of the Ural Federal District. Information Security.* 2021;2(40):44–58 (in Russ.). https://doi.org/10.14529/secur210205, available from URL: https://elibrary.ru/khwhfq
11. Pletenkova A.D. Detection of anomalies caused by cyber attacks in the observed processes of automated control systems using a self-organizing Kohonen map. In: *Security of the Information Space: Proceedings of the 22nd All-Russian Scientific and Practical Conference of Students, Postgraduates and Young Scientists*. Chelyabinsk, November 30, 2023. Chelyabinsk: SUSU Publishing Center; 2024. P. 267–274 (in Russ.). Available from URL: https://www.elibrary.ru/ctpuyj
12. Bukharev D.A., Sokolov A.N., Ragozin A.N. Application of hierarchical cluster analysis for clustering data of ICS information processes affected by cyberattacks. *Vestnik UrFO. Bezopasnost' v informatsionnoi sfere = Journal of the Ural Federal District. Information Security.* 2023;1(47):59–68 (in Russ.). https://doi.org/10.14529/secur230106, Available from URL: https://elibrary.ru/fycuhe
13. Asyaev G.D., Sokolov A.N. Predictive information protection models of automated water management system based on the series using machine learning technologies. *Vestnik UrFO. Bezopasnost' v informatsionnoi sfere = Journal of the Ural Federal District. Information Security.* 2021;4(42):39–45 (in Russ.). https://doi.org/10.14529/secur210404, available from URL: https://elibrary.ru/yjkbtz
14. Sokolov A.N., Ragozin A.N., Barinov A.E., et al. Development of models and methods for early detection of cyber attacks on energy facilities of a metallurgical enterprise. *Vestnik UrFO. Bezopasnost' v informatsionnoi sfere = Journal of the Ural Federal District. Information Security.* 2021;3(41):65–87 (in Russ.). https://doi.org/10.14529/secur210308, available from URL: https://elibrary.ru/kzggpj
15. Shtyrkina A.A., Zegzhda P.D., Lavrova D.S. Detection of anomalies in the traffic of Internet backbone networks using multifractal analysis. *Metody i Tekhnicheskie Sredstva Obespecheniya Bezopasnosti Informatsii.* 2018;27:14–15 (in Russ.). Available from URL: https://elibrary.ru/ypuxqd
16. Basarab M.A., Stroganov I.S. Anomaly detection in information processes based on multifractal analysis. *Voprosy kiberbezopasnosti*. 2014;4(7):30–40 (in Russ.). Available from URL: https://elibrary.ru/tcssen
17. Zegzhda P.D., Lavrova D.S., Shtyrkina A.A. Multifractal analysis of backbone network traffic for denial of service attacks detection. *Problemy informatsionnoi bezopasnosti. Komp'yuternye sistemy = Information Security Problems. Computer Systems.* 2018;2:48–58 (in Russ.). Available from URL: https://elibrary.ru/xtktfz
18. Liu F.T., Ting K.M., Zhou Z.-H. Isolation Forest. In: *Proceedings of the 2008 IEEE International Conference on Data Mining*. IEEE; 2008. P. 413–422. https://doi.org/10.1109/ICDM.2008.17

19. Breunig M.M., Kriegel H.-P., Ng R.T., Sander J. LOF: Identifying Density-based Local Outliers. In: *Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data* 2000. P. 93–104. https://doi.org/10.1145/342009.335388
20. Steinhaus H. Sur la division des corps materiels en parties. *Bull. Acad. Polon. Sci*. 1966;4(12):801–804 (in French.).
21. Oliveri P. Class-modelling in food analytical chemistry: Development, sampling, optimisation and validation issues – A tutorial. *Analytica Chimica Acta*. 2017;982:9–19. https://doi.org/10.1016/j.aca.2017.05.013, hdl:11567/881059. PMID 28734370.

СПИСОК ЛИТЕРАТУРЫ

1. Ихсанов И.И. Безопасность в электроэнергетике: актуальные угрозы и защитные меры. *Юность и знания – гарантия успеха – 2023: Сборник научных статей 10-й Международной молодежной научной конференции*. Курск, 19–20 сентября 2023 г. Курск: Университетская книга; 2023. Т. 2. С. 472–474. URL: https://elibrary.ru/tfyddx
2. Папков Б.В., Осокин Л.В., Кучин Н.Н. Кибербезопасность объектов распределительных электрических сетей. *Сельский механизатор*. 2024;5:3–7. URL: https://elibrary.ru/tfmvhi
3. Колосок И.Н., Коркина Е.С. Анализ кибербезопасности объектов энергетики с учетом механизма и кинетики нежелательных процессов. *Энергетик*. 2024;2:3–8. http://doi.org/10.34831/EP.2024.60.27.001, URL: https://elibrary.ru/ecxvjp
4. Абдрахманов И.И. Опасности и угрозы для кибербезопасности в электроэнергетике: анализ современных угроз и механизмов защиты. *Научный аспект*. 2024;31(3):3970–3973. URL: https://elibrary.ru/lrouni
5. Гурина Л.А. Оценка киберустойчивости системы оперативно-диспетчерского управления ЭЭС. *Вопросы кибербезопасности*. 2022;3(49):23–31. URL: https://elibrary.ru/sapiyh
6. Сметанин Д.И. Изучение структуры системы обнаружения и противодействия атакам вирусов-вымогателей на базе Endpoint Detection and Response. *Актуальные вопросы современной науки: Сборник статей VII Международной научно-практической конференции:* в 2-х ч. Пенза, 10 июня 2023 г. Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.); 2023. С. 60–64. URL: https://elibrary.ru/vuvfpa
7. Лежнюк П.Д., Рубаненко А.Е., Казьмирук О.И. Оптимальное управление нормальными режимами ЭЭС с учетом технического состояния трансформаторов с РПН. *Научные труды Винницкого национального технического университета*. 2012;4:2. URL: https://elibrary.ru/pyqugn
8. Копылова В.В., Паркачев К.Н., Тигунцев С.Г. Трансформатор с тиристорным РПН. *Электрооборудование: эксплуатация и ремонт*. 2019;12:35–39. URL: https://elibrary.ru/vgfudv
9. Аржанников Б.А., Баева И.А., Тарасовский Т.С. Тиристорные устройства регулирования напряжения трансформаторов под нагрузкой РПН. *Транспорт Азиатско-Тихоокеанского региона*. 2020;4(25):32–38. URL: https://elibrary.ru/lxmknj
10. Рагозин А.Н. Формирование прогноза многокомпонентных временных рядов данных с использованием методов цифровой фильтрации и прогнозирующего автокодировщика с целью обнаружения аномалий в работе автоматизированных систем управления технологическими процессами в условиях воздействия кибератак. *Вестник УрФО. Безопасность в информационной сфере.* 2021;2(40):44–58. https://doi.org/10.14529/secur210205, URL: https://elibrary.ru/khwhfq
11. Плетенкова А.Д. Обнаружение аномалий, вызванных кибератаками, в наблюдаемых процессах АСУ ТП с использованием самоорганизующейся карты Кохонена. *Безопасность информационного пространства: Сборник трудов XXII Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых*. Челябинск, 30 ноября 2023 г. Челябинск: Издательский центр ЮУрГУ; 2024. С. 267–274. URL: https://www.elibrary.ru/ctpuyj
12. Бухарев Д.А., Соколов А.Н., Рагозин А.Н. Применение иерархического кластерного анализа для кластеризации данных информационных процессов АСУ ТП, подвергающихся воздействию кибератак. *Вестник УрФО. Безопасность в информационной сфере.* 2023;1(47):59–68. https://doi.org/10.14529/secur230106, URL: https://elibrary.ru/fycuhe
13. Асяев Г.Д., Соколов А.Н. Модели предиктивной защиты информации автоматизированной системы управления водоснабжением на основе временных рядов с использованием технологий машинного обучения. *Вестник УрФО. Безопасность в информационной сфере*. 2021;4(42):39–45. https://doi.org/10.14529/secur210404, URL: https://elibrary.ru/yjkbtz
14. Соколов А.Н., Рагозин А.Н., Баринов А.Е., Уфимцев М.С., Пятницкий И.А., Бухарев Д.А. Разработка моделей и методов раннего обнаружения кибератак на объекты энергетики металлургического предприятия. *Вестник УрФО. Безопасность в информационной сфере*. 2021;3(41):65–87. https://doi.org/10.14529/secur210308, URL: https://elibrary.ru/kzggpj
15. Штыркина А.А., Зегжда П.Д., Лаврова Д.С. Обнаружение аномалий в трафике магистральных сетей Интернет с использованием мультифрактального анализа. *Методы и технические средства обеспечения безопасности информации*. 2018;27:14–15. URL: https://elibrary.ru/ypuxqd
16. Басараб М.А., Строганов И.С. Обнаружение аномалий в информационных процессах на основе мультифрактального анализа. *Вопросы кибербезопасности*. 2014;4(7):30–40. URL: https://elibrary.ru/tcssen

17. Зегжда П.Д., Лаврова Д.С., Штыркина А.А. Мультифрактальный анализ трафика магистральных сетей Интернет для обнаружения атак отказа в обслуживании. *Проблемы информационной безопасности. Компьютерные системы*. 2018;2:48–58. URL: https://elibrary.ru/xtktfz
18. Liu F.T., Ting K.M., Zhou Z.-H. Isolation Forest. In: *Proceedings of the 2008 IEEE International Conference on Data Mining*. IEEE; 2008. P. 413–422. https://doi.org/10.1109/ICDM.2008.17
19. Breunig M.M., Kriegel H.-P., Ng R.T., Sander J. LOF: Identifying Density-based Local Outliers. In: *Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data.* 2000. P. 93–104. https://doi.org/10.1145/342009.335388
20. Steinhaus H. Sur la division des corps materiels en parties. *Bull. Acad. Polon. Sci*. 1966;4(12):801–804 (in French.).
21. Oliveri P. Class-modelling in food analytical chemistry: Development, sampling, optimisation and validation issues – A tutorial. *Analytica Chimica Acta*. 2017;982:9–19. https://doi.org/10.1016/j.aca.2017.05.013, hdl:11567/881059. PMID 28734370.

About the authors

Sergey V. Kochergin, Cand. Sci. (Eng.), Associate Professor, "Information Protection" Department, Institute of Cybersecurity and Digital Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: kochergin_s@mirea.ru. https://orcid.org/0000-0002-3598-8149

Svetlana V. Artemova, Dr. Sci. (Eng.), Associate Professor, Head of the "Information Protection" Department, Institute of Cybersecurity and Digital Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: artemova_s@mirea.ru. Scopus Author ID 6508256085, RSCI SPIN-code 3775-6241, https://orcid.org/0009-0006-8374-8197

Anatoly A. Bakaev, Dr. Sci. (Hist.), Cand. Sci. (Juri.), Associate Professor, Director of the Institute of Cybersecurity and Digital Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: bakaev@mirea.ru. Scopus Author ID 57297341000, RSCI SPIN-code 5283-9148, https://orcid.org/0000-0002-9526-0117

Evgeny S. Mityakov, Dr. Sci. (Econ.), Professor, Acting Head of the "Subject-Oriented Information Systems" Department, Institute of Cybersecurity and Digital Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: mityakov@mirea.ru. Scopus Author ID 55960540500, RSCI SPIN-code 5691-8947, https://orcid.org/0000-0001-6579-0988

Zhanna G. Vegera, Cand. Sci. (Phys.-Math.), Associate Professor, Head of the Department of Higher Mathematics, Institute of Cybersecurity and Digital Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: vegera@mirea.ru. Scopus Author ID 57212931836, RSCI SPIN-code 9076-5678, https://orcid.org/0000-0001-7312-3341

Elena A. Maksimova, Dr. Sci. (Eng.), Associate Professor, Head of the Department "Intelligent Information Security Systems", Institute of Cybersecurity and Digital Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: maksimova@mirea.ru. Scopus Author ID 57219701980, RSCI SPIN-code 6876-5558, https://orcid.org/0000-0001-8788-4256

Об авторах

Кочергин Сергей Валерьевич, к.т.н., доцент, кафедра КБ-1 «Защита информации», Институт кибербезопасности и цифровых технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: kochergin_s@mirea.ru. https://orcid.org/0000-0002-3598-8149

Артемова Светлана Валерьевна, д.т.н., доцент, заведующий кафедрой КБ-1 «Защита информации», Институт кибербезопасности и цифровых технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: artemova_s@mirea.ru. Scopus Author ID 6508256085, SPIN-код РИНЦ 3775-6241, https://orcid.org/0009-0006-8374-8197

Бакаев Анатолий Александрович, д.и.н., к.ю.н., доцент, директор Института кибербезопасности и цифровых технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: bakaev@mirea.ru. Scopus Author ID 57297341000, SPIN-код РИНЦ 5283-9148, https://orcid.org/0000-0002-9526-0117

Митяков Евгений Сергеевич, д.э.н., профессор, и.о. заведующего кафедрой КБ-9 «Предметно-ориентированные информационные системы», Институт кибербезопасности и цифровых технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: mityakov@mirea.ru. Scopus Author ID 55960540500, SPIN-код РИНЦ 5691-8947, https://orcid.org/0000-0001-6579-0988

Вегера Жанна Геннадьевна, к.ф.-м.н., доцент, заведующий кафедрой высшей математики, Институт кибербезопасности и цифровых технологий ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: vegera@mirea.ru. Scopus Author ID 57212931836, SPIN-код РИНЦ 9076-5678, https://orcid.org/0000-0001-7312-3341

Максимова Елена Александровна, д.т.н., доцент, заведующий кафедрой КБ-4 «Интеллектуальные системы информационной безопасности», Институт кибербезопасности и цифровых технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: maksimova@mirea.ru. Scopus Author ID 57219701980, SPIN-код РИНЦ 6876-5558, https://orcid.org/0000-0001-8788-4256

Translated from Russian into English by Lyudmila O. Bychkova
Edited for English language and spelling by Thomas A. Beavitt