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-2025-13-1-7-15
EDN DUNSTG

RESEARCH ARTICLE

Improving Smart Grid security: Spectral and fractal analysis as tools for detecting cyberattacks

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. Cyberattacks are major potential sources of disturbances in modern electrical networks (Smart Grid). However, distinguishing between the various kinds of harmonic distortions and malicious interventions can be challenging. The objective of this work is to develop an effective tool for detecting and quantifying the differences between harmonic and anomalous signals. This will permit the identification of cyberattacks associated with harmonic signal distortions to provide a more accurate classification of patterns characteristic of malicious impacts.

Methods. A comparative analysis of various anomaly detection methods was conducted, including fractal analysis, multifractal analysis, Shannon entropy calculation, and power spectral density (PSD) analysis.

Results. Harmonic distortions and anomalous signals caused by cyberattacks may share similar fractal and multifractal characteristics, making it harder to distinguish between them. The use of the Shannon entropy method does not fully capture the complexity and uncertainty of harmonic and anomalous signals. To gain a deeper understanding of the nature of these signals, a comprehensive approach was applied, including analysis of their frequency characteristics and the use of other uncertainty assessment methods, such as multifractal analysis and PSD. Use of the PSD method revealed significant differences in energy distribution between these signals, permitting a more accurate identification of cyberattacks.

Conclusions. For the effective detection of cyberattacks associated with harmonic signal distortions in power systems, a comprehensive approach is required, including time series analysis, frequency analysis, and machine learning methods. This approach not only detects anomalies in signals but also provides their quantitative assessment to improve the accuracy of classifying malicious impacts. The integration of these methods enhances the reliability and security of power systems, making them less vulnerable to cyberattacks.

Keywords: Smart Grid, harmonic distortion, cyberattacks, multifractal analysis, spectral power density (PSD), anomaly detection

• **Submitted:** 12.09.2024 • **Revised:** 15.11.2024 • **Accepted:** 03.12.2024

For citation: Kochergin S.V., Artemova S.V., Bakaev A.A., Mityakov E.S., Vegera Zh.G., Maksimova E.A. Improving Smart Grid security: Spectral and fractal analysis as tools for detecting cyberattacks. *Russian Technological Journal.* 2025;13(1):7–15. https://doi.org/10.32362/2500-316X-2025-13-1-7-15, https://elibrary.ru/DUNSTG

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

Повышение безопасности смарт-сетей: спектральный и фрактальный анализ как инструменты выявления кибератак

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. В статье рассматриваются гармонические искажения и кибератаки как основные источники нарушений в смарт-сетях (Smart Grid). Цель работы – разработка эффективного инструмента для выявления и численной оценки различий между гармоническими и аномальными сигналами, что позволит обнаруживать кибератаки, связанные с искажением гармонических сигналов, и для более точной классификации паттернов, характерных для вредоносных воздействий.

Методы. Проведен сравнительный анализ различных методов обнаружения аномалий, таких как фрактальный анализ, мультифрактальный анализ, расчет энтропии Шеннона и плотности спектральной мощности (power spectral density, PSD).

Результаты. Полученные результаты показывают, что гармонические искажения и аномальные сигналы, вызванные кибератаками, обладают схожими фрактальными и мультифрактальными характеристиками, что затрудняет их различение. Использование метода энтропии Шеннона не позволило в полной мере оценить сложность и неопределенность гармонических и аномальных сигналов. Для более глубокого понимания природы этих сигналов был применен комплексный подход, включающий анализ их частотных характеристик и применение других методов оценки неопределенности, таких как мультифрактальный анализ и метод PSD. В результате метод PSD выявил значительные различия в распределении энергии между этими сигналами, что позволяет более точно идентифицировать кибератаки.

Выводы. Для эффективного обнаружения кибератак, связанных с искажением гармонических сигналов в энергетических системах, необходим комплексный подход, включающий методы анализа временных рядов, частотный анализ и методы машинного обучения. Такой подход позволяет не только выявлять аномалии в сигналах, но и проводить их численную оценку, что повышает точность классификации вредоносных воздействий. Интеграция этих методов обеспечивает повышение надежности и безопасности энергетических систем, делая их менее уязвимыми к кибератакам.

Ключевые слова: Smart Grid, гармонические искажения, кибератаки, мультифрактальный анализ, спектральная плотность мощности, обнаружение аномалий

• **Поступила:** 12.09.2024 • **Доработана:** 15.11.2024 • **Принята к опубликованию:** 03.12.2024

Для цитирования: Кочергин С.В., Артемова С.В., Бакаев А.А., Митяков Е.С., Вегера Ж.Г., Максимова Е.А. Повышение безопасности смарт-сетей: спектральный и фрактальный анализ как инструменты выявления кибератак. *Russian Technological Journal*. 2025;13(1):7–15. https://doi.org/10.32362/2500-316X-2025-13-1-7-15, https://elibrary.ru/DUNSTG

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

Авторы заявляют об отсутствии конфликта интересов.

INTRODUCTION

Today's cyber threats pose a serious risk to smart energy grids, known as smart grids. These threats include malware attacks, phishing, DDoS[1] attacks and targeted cyber operations aimed at disrupting critical elements of the energy infrastructure. As a result of its combination of traditional power systems with digital information and communication technologies, Smart Grid technology becomes more susceptible to various threats. With the growing number of cyberattacks, ensuring Smart Grid security becomes a priority for maintaining the stability and security of the power system [1–6].

A characteristic feature of modern power supply is the presence of a large number of consumers with nonlinear power supplies, which cause distortion of the sinusoidal characteristic of voltage and current. This leads to negative consequences, worsening the quality of electrical energy, causing additional losses, and in some cases resulting in various resonance phenomena [7–9]. Moreover, cyberattacks on the electric grid can masquerade as natural distortions and thus remain undetected. This complicates the process of detecting such anomalies, making it much more difficult to identify and distinguish cyberattacks from normal operating modes and posing a serious threat to the overall stability and security of the electric grid.

STUDY AND CLASSIFICATION OF HARMONIC DISTORTION AND ANOMALOUS SIGNALS IN THE CONTEXT OF CYBERSECURITY

In order to implement the research, an artificial dataset was created, including 100 electrical signals with harmonic distortions (depicted by a solid line in Fig. 1) caused by the operation of nonlinear power supplies predominantly characterized by harmonic multiples of three (inverters, power supplies, etc.). 100 signals with random anomalous distortions were additionally created, whose main characteristics are random bursts (in Fig. 1 depicted by a dashed line) distinguishable from repetitive signals of natural origin.

Anomalous distortions differ from harmonic distortions not only in terms of their shape, but also the nature of changes; however, their unpredictable and chaotic nature also complicates their detection and classification. As can be seen from the diagram (Fig. 1), while both signals have similar elements, the anomalous distortion is more pronounced and can differ significantly in amplitude and phase from harmonic distortion.

Due to the fact that harmonic distortions in electrical networks often demonstrate complex dynamics and self-similarity, we will evaluate these signals using fractal methods.

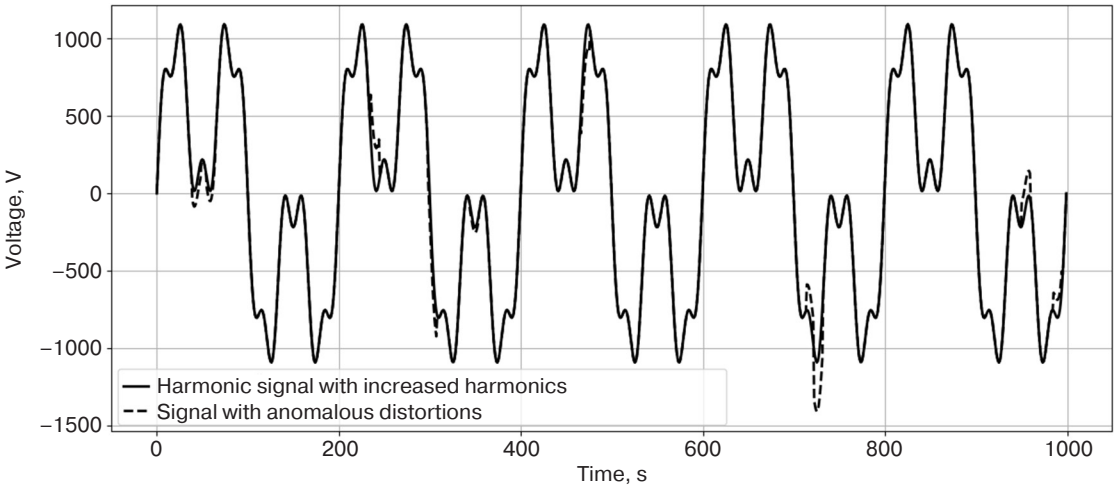

Fig. 1. Comparison of harmonic signal and signal with anomalies

[1] Distributed denial of service is a distributed attack that creates a load on the server and leads to a system failure.

Let us calculate the fractal dimension and the Hurst coefficient, which together allow us to quantify the degree of complexity, self-similarity and correlation structure of the signal. One of the most common methods for determining the fractal dimension is the box-counting method [10]. For a one-dimensional time series, the fractal dimension D is determined by the following formula:

$$D = \lim_{\varepsilon \to 0} \frac{\ln N(\varepsilon)}{\ln(1/\varepsilon)}, \quad (1)$$

where $N(\varepsilon)$ is the number of boxes (segments of length ε) required to cover the entire signal curve.

The Hurst coefficient H is an important fractal parameter that characterizes the degree of long-term dependence and correlation in the signal. It is calculated by the formula:

$$H = \frac{\ln(R/S)}{\ln n}, \quad (2)$$

where R is the range of the accumulated deviation of the signal from the average value; S is the standard deviation; n is the sample size.

The results of calculating (Table) fractal characteristics for harmonic and anomalous signals shows that both types of signals have similar values of both fractal dimensionality and Hurst coefficient. The average value of the Hurst coefficient for the anomalous signals was found to be slightly higher, which may indicate a more pronounced autocorrelation or "memorization" in these signals compared to the harmonic signals. However, this difference is minimal and may be insufficient for a clear distinction between the two types of signals.

The analysis of fractal dimensionality showed that both types of signals have similar values, indicating that they have a similar structure on small scales. This can complicate the task of distinguishing between harmonic and anomalous distortions on the basis of fractal parameters alone.

Table. Comparison of fractal characteristics for harmonic and anomalous signals

Parameter	Type of the signal	Average value
Hurst coefficient	Harmonic signals	0.643
	Anomalous signals	0.652
Fractal dimension	Harmonic signals	0.988
	Anomalous signals	0.988

The results of the study show that, despite the differences in the nature of the signals, their fractal characteristics turned out to be very similar, making it difficult to distinguish them accurately. For a more accurate classification of anomalous and harmonic distortions, it is necessary to conduct a multifractal analysis [11, 12]. The choice of multifractal spectrum is explained by its ability to more deeply characterize complex and heterogeneous signal structures, which are not sufficiently described by traditional monofractal methods.

The performed calculation of the multifractal spectrum resulted in the dependence (Fig. 2), which displays the Hurst exponent $H(q)$ as a function of the scaling parameter q.

In order to achieve this goal, the signal was decomposed into sub-bands using different values of the scaling parameter q, which is related to the signal moments. In the decomposition process, a generalized cumulative function $Z(q, s)$ was calculated according to the definition:

$$Z(q,s) = \sum_{i=1}^{N_s} |X(i,s)|^q, \quad (3)$$

where $X(i, s)$ represents the amplitude of the signal on the scale s, while N_s is the number of elements on this scale.

A scale transformation was performed for each value of q to calculate the dependence of the cumulative function $Z(q, s)$ on the scale s. It was found that for signals with multifractal properties this dependence follows a power law:

$$Z(q,s) \sim s^{\tau(q)}, \quad (4)$$

where $\tau(q)$ is a spectral function describing multifractal characteristics of the signal.

As a result, the values of the Hurst index $H(q)$ were calculated for each value of q using the ratio:

$$H(q) = \frac{\tau(q)}{q}. \quad (5)$$

The results of multifractal analysis (Fig. 2) show that the complexity spectra of harmonic and anomalous signals are very similar, including at different scales. Thus, although the nature of these signals is different, the similarity of their multifractal properties limits the ability to use multifractal analysis to distinguish between harmonic and anomalous signals.

In order to more accurately classify and identify the differences between these types of signals, it becomes necessary to use additional analysis methods. One such

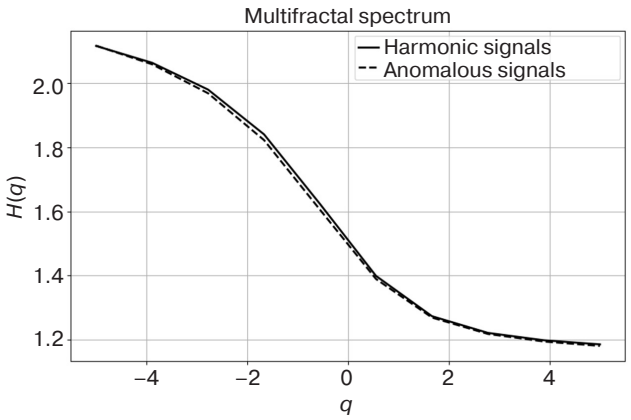

Fig. 2. Dependence of the Hurst index on the scaling parameter

method is Shannon entropy [13, 14], which was chosen for further study due to its ability to quantify the level of uncertainty and complexity in a system. The possibility of using Shannon entropy to analyze the changes in the probability distribution of different events associated with a signal makes it particularly useful in the study of signals with anomalies. In the context of electrical networks, this method can reveal hidden anomalies or instabilities that go undetected when using only multifractal analysis.

In order to compare harmonic and anomalous signals, the Shannon entropy estimation method is used to measure the level of uncertainty in the signal. Shannon entropy H, which shows how uniformly distributed the signal values are, can be calculated by the formula:

$$H = -\sum_{i=1}^{n} p(x_i) \lg p(x_i), \quad (6)$$

where $p(x_i)$ is the probability that the signal takes the value x_i, while n is the number of possible values of the signal.

The diagram (Fig. 3) shows the distribution of Shannon entropy values for two types of signals: harmonic (green color, lines) and anomalous (red color). The frequency f on the ordinate axis shows how often different values of entropy H occur in the data sample. Harmonic signals are characterized by entropy values concentrated in a narrow range around ~5.2 to form a high and narrow peak on the histogram. This indicates a high degree of orderliness and predictability of harmonic signals as reflected in their stable and relatively low entropy values.

In contrast, anomalous signals have a wider entropy distribution, which ranges from 5 to ~5.4 and is combined with a lower and fuzzier peak. This indicates greater randomness and disorder in their structure, resulting in increased entropic variation. The partial overlap of the distributions of harmonic and anomalous signals confirms that some anomalous signals have entropy similar to that of harmonic signals.

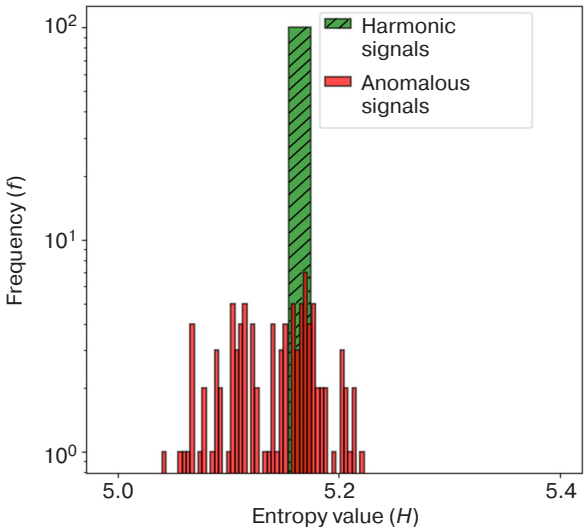

Fig. 3. Shannon entropy (logarithmic scale)

While Shannon entropy provides important information about the degree of uncertainty in a signal, a full understanding of the nature of harmonic and anomalous signals also requires an analysis of their frequency characteristics.

The described method for calculating the power spectral density (PSD) [15, 16] was used in this work to identify key frequency characteristics of signals. This method is suitable for detecting hidden periodicities and anomalies that may remain undetected when analyzing only the temporal characteristics of the signal.

The PSD method gives a more complete picture of the spectral structure of signals by analyzing the energy distribution over frequencies. This is important for differentiation of harmonic and anomalous signals, especially when dealing with complex time series. The application of PSD enables not only qualitative but also quantitative assessment of differences between signals, thus providing more accurate classification and detection of hidden anomalies.

PSD was calculated using the Welch method [17], an improved power spectrum estimation approach that reduces noise by splitting the signal into overlapping segments and averaging their spectra.

The power spectral density $P(\omega)$ of the signals was calculated using the following formula:

$$P(\omega) = \frac{1}{N} \sum_{k=1}^{N} |X_k(\omega)|^2, \quad (7)$$

where ω is the frequency; $X_k(\omega)$ is the discrete Fourier transform of the kth segment of the signal; N is the number of segments.

The Welch method is used to determine the power spectrum more accurately. The signal is divided into several parts, which may overlap. Then Fourier

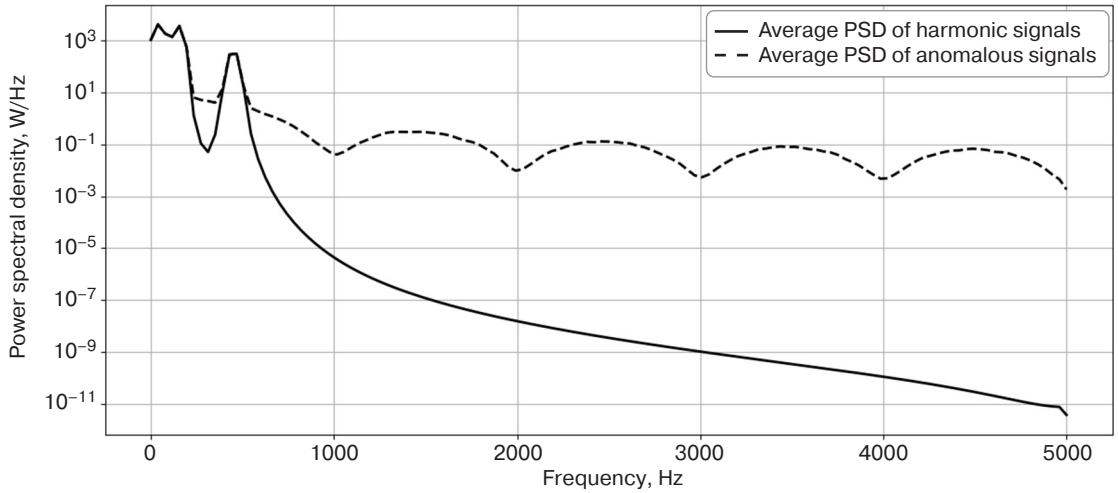

Fig. 4. Comparison of PSD distribution of harmonic and anomalous signals

transform is applied to each part. The average of the power spectra of all segments is then calculated. This reduces the influence of random noise and increases the stability of the estimation:

$$P_{\text{Welch}}(\omega) = \frac{1}{M}\sum_{m=1}^{M} P_m(\omega), \quad (8)$$

where M is the number of segments; $P_m(\omega)$ is the power spectral density for the mth segment.

Figure 4 compares the power spectral density distribution of harmonic and anomalous signals. At low frequencies, harmonic signals show a more concentrated energy distribution. Anomalous signals are characterized by a wider spectrum.

In order to further analyze the spectral characteristics and accurately evaluate the difference between harmonic and anomalous signals, it is necessary to calculate the integral energy of the signals. The integral energy of a signal, which is defined as the area under the PSD curve, serves as a quantitative measure of the total energy distributed across frequencies. It can provide additional insight into the differences between signal types.

The integral energy of the signal E is calculated by integrating the PSD values $P(\omega)$ over the entire frequency range ω:

$$E = \int_{0}^{\omega_{\max}} P(\omega)d\omega, \quad (9)$$

where $\omega_{\max}$ is the maximum frequency up to which the integration is performed.

This transition to integral energy estimation not only reveals how energy is distributed across frequencies, but also quantifies the overall energy content of signals, which is essential to better understand their nature and permit their more accurate classification.

The results of power spectral density calculations revealed a significant difference in the energy distribution between anomalous and harmonic signals in the frequency range of 200–300 Hz. In particular, the energy in this range for the anomalous data was 224.53 units, which is significantly higher than the energy of the harmonic data (27.51 units). This difference indicates that there is a significant increase in energy in the anomalous data in the 200–300 Hz range, which may indicate the presence of additional frequency components or increased activity characteristic of anomalous signals.

The increase in energy can be caused by additional noise, non-harmonic components, or other factors that are not present in harmonic signals. This emphasizes the importance of frequency analysis, especially the PSD method, for detecting anomalies that may not be noticeable when analyzing signals in the time domain.

CONCLUSIONS

The results of this study demonstrate that the PSD method is an effective tool for identifying and numerically evaluating the differences between harmonic and anomalous signals. The described approach can be used to detect cyberattacks involving distortion of harmonic signals and more accurately classify patterns characteristic of malicious attacks. The application of this method can contribute to improved security and resilience of power systems, ensuring timely detection and neutralization of threats.

Authors' contributions

S.V. Kochergin—development of the main research concept, formulation of key aims and objectives, conducting a literature review in the relevant field, preparation of research materials, and coordination of experimental studies.

S.V. Artemova—development and optimization of the research methodology, conducting comparative analyses, and participation in editing and preparing the article.

A.A. Bakaev—determination of the research topic, coordination of result discussions, and final stages of article preparation.

E.S. Mityakov—analysis and interpretation of results, preparation of conclusions, and participation in data discussions.

Zh.G. Vegera—mathematical and statistical support, ensuring the accuracy of quantitative analysis methods, and data integrity verification.

E.A. Maksimova—exploration of existing anomaly detection methods and identification of the most promising approaches for comparative analysis.

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.). 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.). 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, 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.). 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.). https://elibrary.ru/sapiyh
6. Gurina L.A., Aizenberg N.I. Search for an effective solution to protect microgrid community with interconnected information systems against cyber threats. *Voprosy kiberbezopasnosti = Cybersecurity Issues*. 2023;3(55):37–49 (in Russ.). https://www.elibrary.ru/qguytv
7. Semenov A.S., Bebikhov Yu.V., Egorov A.N., Fedorov O.V. Effect of higher harmonics on electric power quality in supply systems in mines. *Gornyi Zhurnal = Mining Journal*. 2024;2:84–91 (in Russ.). https://doi.org/10.17580/gzh.2024.02.14, https://www.elibrary.ru/nmssyq
8. Voronin M.S. The influence of higher harmonics in the power supply network of an enterprise on the quality of electricity. In: *Technologies, Machines and Equipment for the Design and Construction of Agricultural Facilities: collection of scientific articles of the 2nd International Scientific and Technical Conference of Young Scientists, Graduate Students, Masters and Bachelors.* Kursk: Universitetskaya kniga; 2024. P. 440–442 (in Russ.). https://www.elibrary.ru/wxelva
9. Ovechkin I.S., Puzina E.Yu. Development of technical solutions to reduce the distortion of the sinusoidal voltage curve of overhead lines supplying automatic blocking devices. *Sovremennye tekhnologii. Sistemnyi analiz. Modelirovanie = Modern Technologies. System Analysis. Modeling*. 2023;3(79):112–123 (in Russ.). https://www.elibrary.ru/smcqdv
10. Iannaccone P.M., Khokha M. *Fractal Geometry in Biological Systems: An Analytical Approach.* CRC Press; 1996. 366 p. ISBN 978-0-8493-7636-8.
11. Basarab M.A., Stroganov I.S. Anomaly detection in information processes based on multifractal analysis. *Voprosy kiberbezopasnosti = Cybersecurity Issues*. 2014;4(7):30–40 (in Russ.). https://www.elibrary.ru/tcssen
12. Shelukhin O.I., Pankrushin A.V. Detection of anomalous in real time by methods of multifractal analysis. *Nelineinyi mir = Nonlinear World*. 2016;14(2):72–82 (in Russ.). https://www.elibrary.ru/vtznth
13. Dobrovol'skii G.A., Todoriko O.A. Application of Shannon entropy for voice activity detection in noisy sound recordings. *Vestnik Khersonskogo natsional'nogo tekhnicheskogo universiteta = Bulletin of the Kherson National Technical University.* 2016;3(58):218–223 (in Russ.). https://www.elibrary.ru/xdsiyx
14. Shannon K. *Raboty po teorii informatsii i kibernetike* (*Works on Information Theory and Cybernetics*). Moscow: IL; 1963. 829 p. (in Russ.).
15. Goldenberg L.M., Matyushkin B.D., Polyak M.N. *Tsifrovaya obrabotka signalov*: Spravochnik (*Digital Signal Processing*: Handbook). Moscow: Radio i svyaz'; 1985. 256 p. (in Russ.).
16. Bespalov A.D., Mishagin K.G. Calculation of the spectral power density of phase noise with the allocation of discrete spectral components. In: *Proceedings of the 26th Scientific Conference on Radiophysics dedicated to the 120th anniversary of M.T. Grekhova: Conference materials.* Nizhny Novgorod: N.I. Lobachevsky National Research Nizhny Novgorod State University; 2022. P. 208–211 (in Russ.). https://www.elibrary.ru/xwykrc
17. Welch P.D. The use of Fast Fourier Transform for the estimation of power spectra: A method based on time averaging over short, modified periodograms. *IEEE Transactions on Audio and Electroacoustics.* 1967;15(2):70–73. https://doi.org/10.1109/TAU.1967.1161901

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 года. Курск: Университетская книга; 2023. Т. 2. С. 472–474. 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. 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, 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. https://elibrary.ru/lrouni
5. Гурина Л.А. Оценка киберустойчивости системы оперативно-диспетчерского управления ЭЭС. *Вопросы кибербезопасности*. 2022;3(49):23–31. https://elibrary.ru/sapiyh
6. Гурина Л.А., Айзенберг Н.И. Поиск эффективного решения по обеспечению защиты от киберугроз сообщества микросетей со взаимосвязанными информационными системами. *Вопросы кибербезопасности*. 2023;3(55):37–49. https://www.elibrary.ru/qguytv
7. Семенов А.С., Бебихов Ю.В., Егоров А.Н., Федоров О.В. Влияние высших гармоник на качество электроэнергии в системах электроснабжения горнодобывающих предприятий. *Горный журнал*. 2024;2:84–91. https://doi.org/10.17580/gzh.2024.02.14, https://www.elibrary.ru/nmssyq
8. Воронин М.С. Влияние высших гармоник в сети электроснабжения предприятия на качество электроэнергии. В сб.: *Технологии, машины и оборудование для проектирования, строительства объектов АПК: сборник научных статей 2-й Международной научно-технической конференции молодых ученых, аспирантов, магистров и бакалавров*. Курск: ЗАО «Университетская книга»; 2024. С. 440–442. https://www.elibrary.ru/wxelva
9. Овечкин И.С., Пузина Е.Ю. Разработка технических решений по уменьшению искажения синусоидальности кривой напряжения воздушных линий, питающих устройства автоблокировки. *Современные технологии. Системный анализ. Моделирование.* 2023;3(79):112–123. https://www.elibrary.ru/smcqdv
10. Iannaccone P.M., Khokha M. *Fractal Geometry in Biological Systems: An Analytical Approach.* CRC Press; 1996. 366 p. ISBN 978-0-8493-7636-8.
11. Басараб М.А., Строганов И.С. Обнаружение аномалий в информационных процессах на основе мультифрактального анализа. *Вопросы кибербезопасности*. 2014;4(7):30–40. https://www.elibrary.ru/tcssen
12. Шелухин О.И., Панкрушин А.В. Обнаружение аномальных выбросов в реальном масштабе времени методами мультифрактального анализа. *Нелинейный мир*. 2016;14(2):72–82. https://www.elibrary.ru/vtznth
13. Добровольский Г.А., Тодорико О.А. Использование энтропии Шеннона для детекции голосовой активности в зашумленных звукозаписях. *Вестник Херсонского национального технического университета*. 2016;3(58):218–223. https://www.elibrary.ru/xdsiyx
14. Шеннон К. *Работы по теории информации и кибернетике*. М.: ИЛ; 1963. 829 с.
15. Гольденберг Л.М., Матюшкин Б.Д., Поляк М.Н. *Цифровая обработка сигналов*: Справочник. М.: Радио и связь; 1985. 256 с.
16. Беспалов А.Д., Мишагин К.Г. Расчет спектральной плотности мощности фазового шума с выделением дискретных спектральных компонент. В: *Труды XXVI научной конференции по радиофизике, посвященной 120-летию М.Т. Греховой: Материалы конференции*. Нижний Новгород: Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского; 2022. С. 208–211. https://www.elibrary.ru/xwykrc
17. Welch P.D. The use of Fast Fourier Transform for the estimation of power spectra: A method based on time averaging over short, modified periodograms. *IEEE Transactions on Audio and Electroacoustics.* 1967;15(2):70–73. https://doi.org/10.1109/TAU.1967.1161901

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 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 Department "Subject-Oriented Information Systems," 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. (Phys.-Math.), Associate Professor, Head of 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