Russian Technological Journal.
2025;13(1):7–15

ISSN 2782-3210 (Print)
ISSN 2500-316X (Online)

УДК 621.311.1
https://doi.org/10.32362/2500-316X-2025-13-1-7-15
EDN DUNSTG

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.

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.

ВВЕДЕНИЕ

Современные киберугрозы представляют собой серьезную опасность для интеллектуальных энергетических сетей, известных как смарт-сети (Smart Grid). Эти угрозы включают атаки с использованием вредоносного программного обеспечения, фишинг, DDoS-атаки[1] и целенаправленные кибероперации, направленные на нарушение работы критически важных элементов энергетической инфраструктуры. Из-за того, что технология Smart Grid объединяет традиционные системы электроэнергетики с современными информационными и коммуникационными технологиями, она становится более подверженной различным угрозам. Это связано с ее зависимостью от цифровых технологий и сетевых подключений. В условиях роста числа кибератак обеспечение безопасности Smart Grid становится приоритетной задачей для сохранения стабильности и безопасности энергетической системы [1–6].

Характерной особенностью современного электроснабжения является наличие большого количества потребителей с нелинейными источниками питания, которые вызывают искажение синусоидальной характеристики напряжения и тока. Это приводит к негативным последствиям, ухудшает качество электрической энергии, вызывает дополнительные потери, в ряде случаев возможно появление резонансных явлений [7–9].

В тоже время кибератаки на электрические сети могут маскироваться под искажения естественного характера и оставаться незамеченными. Это осложняет процесс выявления подобных аномалий, существенно усложняет выявление и различение кибератак от нормальных эксплуатационных режимов, что представляет серьезную угрозу для стабильности и безопасности электрической сети.

ИССЛЕДОВАНИЕ И КЛАССИФИКАЦИЯ ГАРМОНИЧЕСКИХ ИСКАЖЕНИЙ И АНОМАЛЬНЫХ СИГНАЛОВ В КОНТЕКСТЕ КИБЕРБЕЗОПАСНОСТИ

Для проведения исследований был создан искусственный датасет, включающий в себя 100 электрических сигналов с гармоническими искажениями (на рис. 1 изображены сплошной линией), вызванными работой нелинейных источников питания с характерным преобладанием гармоник, кратных трем (инверторы, блоки питания и др.). Также были созданы 100 сигналов со случайными аномальными искажениями, особенностью которых являются случайные всплески (на рис. 1 изображены штриховой линией),

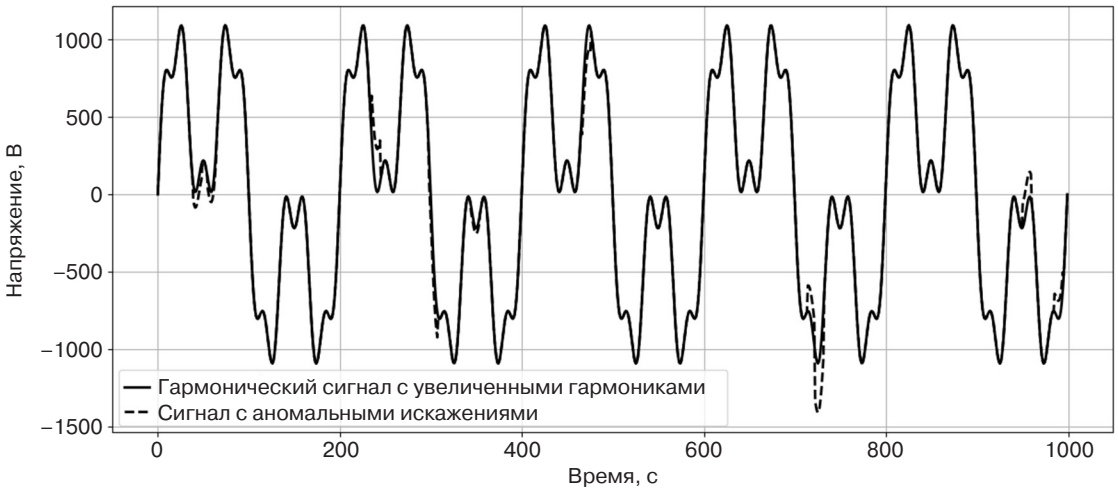

Рис. 1. Сравнение гармонического сигнала и сигнала с аномалиями

[1] Distributed denial of service – распределенная атака, которая создает нагрузку на сервер и приводит к отказу системы. [Distributed denial of service is a distributed attack that creates a load on the server and leads to a system failure.]

отличающиеся от повторяющихся сигналов естественного происхождения.

Аномальные искажения отличаются от гармонических не только формой, но и характером изменений: они могут быть более непредсказуемыми и хаотичными, что усложняет их обнаружение и классификацию. На графике (рис. 1) видно, что, хотя оба сигнала имеют похожие элементы, аномальные искажения более выражены и могут существенно отличаться по амплитуде и фазе от гармонических искажений.

Ввиду того, что гармонические искажения в электрических сетях часто демонстрируют сложную динамику и самоподобие, проведем оценку этих сигналов с использованием фрактальных методов.

Выполним расчет фрактальной размерности и коэффициента Херста, которые вместе позволяют количественно оценить степень сложности, самоподобия и корреляционной структуры сигнала. Одним из наиболее распространенных методов определения фрактальной размерности является метод коробочного подсчета (box-counting) [10]. Для одномерного временного ряда фрактальная размерность D определяется по следующей формуле:

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

где $N(\varepsilon)$ – количество коробок (отрезков длины ε), необходимых для покрытия всей кривой сигнала.

Коэффициент Херста H представляет собой важный фрактальный параметр, характеризующий степень долговременной зависимости и корреляции в сигнале. Он вычисляется по формуле:

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

где R – размах (range) накопленного отклонения сигнала от среднего значения, S – стандартное отклонение, а n – размер выборки.

Результаты расчета (таблица) фрактальных характеристик для гармонических и аномальных сигналов, представленных в нашем исследовании, показали, что оба типа сигналов имеют схожие значения как фрактальной размерности, так и коэффициента Херста. Среднее значение коэффициента Херста для аномальных сигналов оказалось незначительно выше, что может свидетельствовать о более выраженной автокорреляции или «запоминаемости» в этих сигналах по сравнению с гармоническими. Однако это различие минимально и, возможно, недостаточно для четкого разграничения двух типов сигналов.

Анализ фрактальной размерности показал: оба типа сигналов имеют схожие значения, что говорит о том, что на малых масштабах они имеют похожую структуру. Это может усложнить задачу различения гармонических и аномальных искажений на основе только фрактальных параметров.

Таблица. Сравнение фрактальных характеристик для гармонических и аномальных сигналов

Параметр	Тип сигнала	Среднее значение
Коэффициент Херста	Гармонические сигналы	0.643
	Аномальные сигналы	0.652
Фрактальная размерность	Гармонические сигналы	0.988
	Аномальные сигналы	0.988

Результаты исследования показывают, что, несмотря на различия в природе сигналов, их фрактальные характеристики оказались очень схожими, что затрудняет точное их различение. Для более точной классификации аномальных и гармонических искажений проведем мультифрактальный анализ [11, 12]. Выбор мультифрактального спектра объясняется его способностью более глубоко характеризовать сложные и неоднородные структуры сигналов, которые недостаточно описываются традиционными монофрактальными методами.

В результате выполненного расчета мультифрактального спектра была получена зависимость (рис. 2), которая отображает показатель Херста $H(q)$ в зависимости от параметра масштабирования q.

Для достижения этой цели сигнал был разложен на поддиапазоны, используя различные значения параметра масштабирования q, который связан с моментами сигнала. В процессе декомпозиции была рассчитана обобщенная кумулятивная функция $Z(q, s)$, определяемая как:

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

где $X(i, s)$ представляет собой амплитуду сигнала на масштабе s, а N_s – количество элементов на этом масштабе.

Было проведено масштабное преобразование для каждого значения q, чтобы вычислить зависимость кумулятивной функции $Z(q, s)$ от масштаба s. Установлено, что для сигналов с мультифрактальными свойствами эта зависимость подчиняется степенному закону:

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

где $\tau(q)$ – спектральная функция, описывающая мультифрактальные характеристики сигнала.

В результате были вычислены значения показателя Херста $H(q)$ для каждого значения q с использованием соотношения:

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

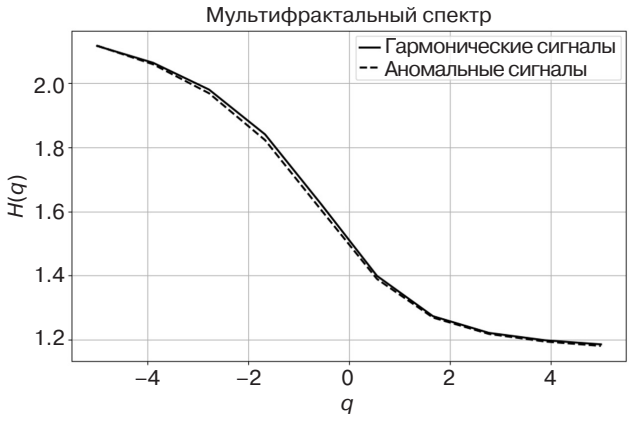

Рис. 2. Зависимость показателя Херста от параметра масштабирования

Результаты мультифрактального анализа (рис. 2) показывают, что спектры сложности гармонических и аномальных сигналов очень похожи. Это означает, что похожи сложность и структура этих сигналов на разных масштабах. Несмотря на то, что природа этих сигналов различна, их мультифрактальные свойства очень похожи. Это ограничивает возможность использования мультифрактального анализа для различения гармонических и аномальных сигналов.

Для более точной классификации и выявления различий между этими типами сигналов возникает необходимость в использовании дополнительных методов анализа. Одним из таких методов является энтропия Шеннона [13, 14], которая была выбрана для дальнейшего исследования благодаря своей способности количественно оценивать уровень неопределенности и сложности в системе. Энтропия Шеннона позволяет анализировать изменения в распределении вероятностей различных событий, связанных с сигналом, что может быть особенно полезным при исследовании сигналов с аномалиями. В контексте электрических сетей этот метод может выявить скрытые аномалии или нестабильности, которые остаются незамеченными при использовании только мультифрактального анализа.

Чтобы сравнить гармонические и аномальные сигналы, использован метод оценки энтропии Шеннона. Он помогает измерить уровень неопределенности в сигнале. Энтропия Шеннона H показывает, насколько равномерно распределены значения сигнала. Ее можно рассчитать по формуле:

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

где $p(x_i)$ – вероятность того, что сигнал примет значение x_i, а n – количество возможных значений сигнала.

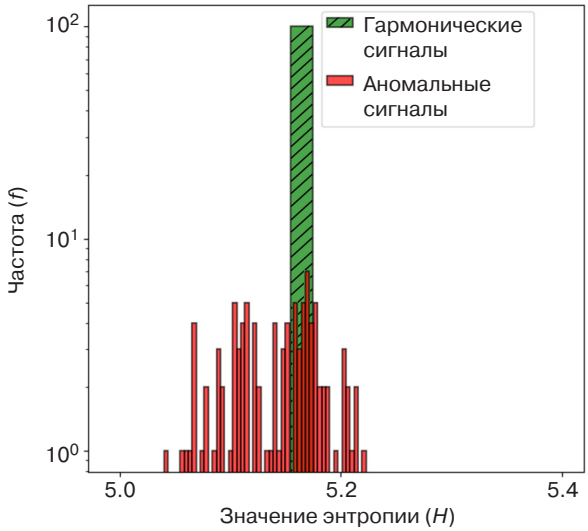

Рис. 3. Энтропия Шеннона (логарифмическая шкала)

График (рис. 3) демонстрирует распределение значений энтропии Шеннона для двух типов сигналов: гармонических (зеленый цвет, штриховка) и аномальных (красный цвет). Частота f по оси ординат показывает, как часто различные значения энтропии H встречаются в выборке данных. Гармоническим сигналам свойственны значения энтропии, сосредоточенные в узком диапазоне около ~5.2, что образует высокий и узкий пик на гистограмме. Это свидетельствует о высокой степени упорядоченности и предсказуемости гармонических сигналов, отражающейся в их стабильных и относительно низких значениях энтропии.

Аномальные сигналы, напротив, имеют более широкое распределение энтропии, варьирующееся от 5 до ~5.4, с более низким и размытым пиком. Это указывает на большую хаотичность и неупорядоченность в их структуре, что приводит к повышенной вариативности энтропии. Частичное перекрытие распределений гармонических и аномальных сигналов показывает, что некоторые аномальные сигналы имеют энтропию, схожую с энтропией гармонических сигналов.

Хотя энтропия Шеннона предоставляет важную информацию о степени неопределенности сигнала, для полного понимания природы гармонических и аномальных сигналов требуется также анализ их частотных характеристик.

С целью выявления ключевых частотных характеристик сигналов в работе использован метод расчета спектральной плотности мощности (power spectral density, PSD) [15, 16]. Особенностью этого метода является то,

что он позволяет обнаружить скрытые периодичности и аномалии, которые могут остаться незамеченными при анализе только временных характеристик сигнала.

Метод PSD дает более полное представление о спектральной структуре сигналов, анализируя распределение энергии по частотам. Это важно для дифференциации гармонических и аномальных сигналов, особенно в сложных временных рядах. Применение PSD позволяет не только качественно, но и количественно оценивать различия между сигналами, обеспечивая более точную их классификацию и выявление скрытых аномалий.

Расчет PSD был выполнен с использованием метода Уэлча (Welch) [17], который представляет собой улучшенный метод оценки спектра мощности, снижающий шум путем разбиения сигнала на перекрывающиеся сегменты и усреднения их спектров.

Спектральная плотность мощности $P(\omega)$ сигналов была рассчитана по следующей формуле:

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

где ω – частота, $X_k(\omega)$ – дискретное преобразование Фурье k-го сегмента сигнала, а N – количество сегментов.

Метод Уэлча используют для более точного определения спектра мощности. При этом сигнал разделяют на несколько частей, которые могут перекрываться. Затем для каждой части применяют преобразование Фурье. После этого вычисляют среднее значение спектров мощности всех сегментов. Это позволяет снизить влияние случайных помех и повысить стабильность оценки:

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

где M – количество сегментов, а $P_m(\omega)$ – спектральная плотность мощности для m-го сегмента.

На рис. 4 представлено сравнение распределения спектральной плотности мощности гармонических и аномальных сигналов. На низких частотах гармонические сигналы демонстрируют более концентрированное распределение энергии. Для аномальных сигналов характерен более широкий спектр.

Чтобы глубже проанализировать спектральные характеристики и точно оценить разницу между гармоническими и аномальными сигналами, нужно вычислить интегральную энергию сигналов. Это делается путем интегрирования значений PSD по всему диапазону частот. Интегральная энергия сигнала, которая определяется как площадь под кривой PSD, служит количественной мерой общей энергии, распределенной по частотам. Она может предоставить дополнительные сведения о различиях между типами сигналов.

Интегральная энергия сигнала E вычисляется путем интегрирования значений PSD $P(\omega)$ по всему диапазону частот ω:

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

где $\omega_{\max}$ – максимальная частота, до которой выполняется интегрирование.

Этот переход к интегральной оценке энергии позволяет не только выявить, как энергия распределена по частотам, но и количественно оценить общую энергетическую составляющую сигналов, что является важным для более глубокого понимания их природы и для точной их классификации.

Результаты расчета спектральной плотности мощности выявили значительное различие в энергетическом распределении между аномальными и гармоническими сигналами в диапазоне частот 200–300 Гц. В частности, энергия в этом диапазоне для аномальных данных составила 224.53 единицы, что существенно

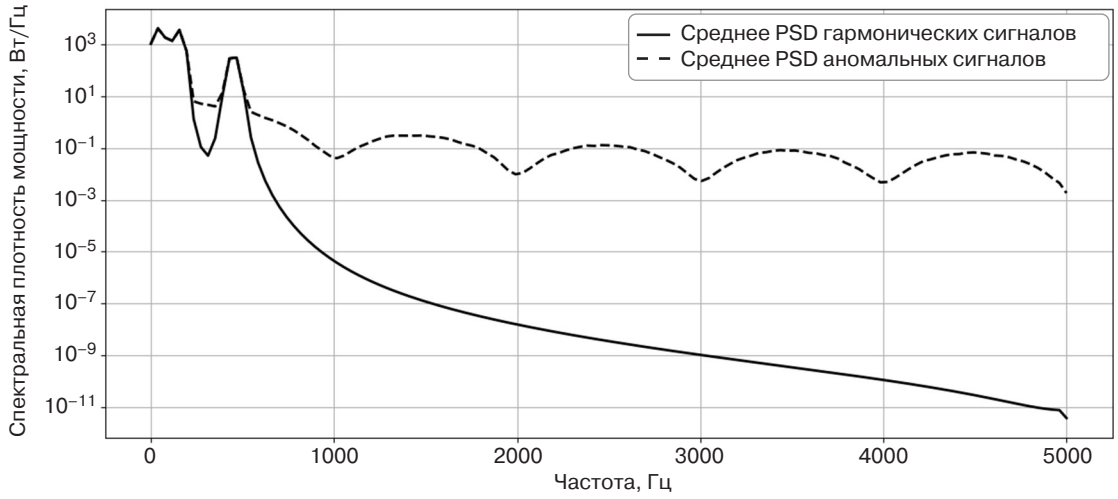

Рис. 4. Сравнение распределения PSD гармонических и аномальных сигналов

превышает энергию гармонических данных, равную 27.51 единицам. Это различие указывает на то, что в аномальных данных в диапазоне 200–300 Гц присутствует значительное увеличение энергии, что может свидетельствовать о наличии дополнительных частотных компонентов или повышенной активности, характерной для аномальных сигналов.

Рост энергии может быть вызван дополнительными шумами, негармоническими составляющими или другими факторами, которые отсутствуют в гармонических сигналах. Это подчеркивает значимость частотного анализа, особенно метода PSD, для обнаружения аномалий, которые могут быть незаметны при анализе сигналов во временной области.

ВЫВОДЫ

Результаты исследования демонстрируют, что метод PSD является эффективным инструментом для выявления и численной оценки различий между гармоническими и аномальными сигналами. Это позволяет использовать данный метод для обнаружения кибератак, связанных с искажением гармонических сигналов, и более точной классификации паттернов, характерных для вредоносных воздействий. Применение такого подхода способствует повышению уровня безопасности и устойчивости энергосистем, обеспечивая своевременное обнаружение и нейтрализацию угроз.

Вклад авторов

С.В. Кочергин – разработка основной концепции исследования, формулирование ключевых целей и задач, проведение обзора литературы в соответствующей области, подготовка материалов для исследований и координация экспериментальных работ.

С.В. Артемова – разработка и оптимизация методологии исследования, проведение сравнительного анализа и участие в редактировании и подготовке статьи.

А.А. Бакаев – определение темы исследования, координация обсуждения результатов и завершающих этапов подготовки статьи.

Е.С. Митяков – анализ и интерпретация результатов, подготовка выводов и участие в обсуждении данных.

Ж.Г. Вегера – математическое и статистическое сопровождение, обеспечение точности методов анализа и проверка целостности данных.

Е.А. Максимова – исследование существующих методов обнаружения аномалий и определение наиболее перспективных подходов для сравнительного анализа.

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.

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

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

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

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