Russian Technological Journal.
2024;12(6):7–19

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

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

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.

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.

ВВЕДЕНИЕ

Современные электрические сети стремительно трансформируются в децентрализованные системы с внедрением смарт-сетей (Smart Grids) и распределенной генерации энергии. Эти сети, являясь киберфизическими системами, сталкиваются с новыми вызовами в области кибербезопасности, связанными с необходимостью защиты распределенных компонентов и реализацией многоуровневых атак [1–5]. Защита таких сетей только традиционным антивирусным обеспечением не приносит положительного результата, поэтому в последнее время все больше внимания профессиональным сообществом уделяется вопросу защиты конечных точек, в т.ч. с помощью системы безопасности Endpoint Detection and Response (EDR) [6].

Особенностью EDR-системы является то, что она позволяет осуществлять поведенческий анализ в выявлении подозрительной активности и обнаружении изменений в конфигурации конечных точек – узлов электрической сети и непосредственно электротехнического оборудования. Например, действия злоумышленников с применением бесфайловых методов могут проявляться в изменении параметров электрической энергии (напряжения, сопротивления) и ложных командах на переключение оборудования.

Для защиты смарт-сетей требуется разработка новых методов поведенческого анализа, учитывающих особенности их технологических режимов работы.

ИССЛЕДОВАНИЕ И КЛАССИФИКАЦИЯ ГАРМОНИЧЕСКИХ ИСКАЖЕНИЙ И АНОМАЛЬНЫХ СИГНАЛОВ, ВЫЗВАННЫХ КИБЕРАТАКАМИ

Основное внимание кибератак на смарт-сети может быть направлено на создание условий для нанесения максимального ущерба от нарушения их нормального функционирования.

Одним из вариантов кибератак, представляющих значительную угрозу, является вмешательство в систему управления регулированием напряжения. Для поддержания необходимого уровня напряжения в смарт-сетях используются трансформаторы с автоматическим регулированием напряжения. Наиболее распространенным способом регулирования является использование трансформаторов с регулированием под нагрузкой [7–9].

Необычные команды и действия в ходе кибератаки на электрическую сеть могут проявляться в различных формах, отличающихся от нормального поведения системы. Например, команда на изменение коэффициента трансформации трансформатора без видимой причины или попытки неоднократного входа в систему управления могут указывать на попытки атакующих вмешаться в работу системы. Такие аномальные действия требуют оперативного выявления и анализа для предотвращения возможных угроз.

Рассмотрим пример работы электрической сети во время кибератаки. Энергосистема работает в нормальном режиме, все параметры находятся в допустимых пределах. Трансформатор T1 стабильно функционирует, обеспечивая необходимое напряжение на подстанции с коэффициентом трансформации 35(10)/0.4 кВ. Внезапно поступает команда на изменение коэффициента трансформации трансформатора T1, хотя оператор не находит причин для таких изменений, т.к. параметры системы остаются в норме. Тем не менее, команда выполняется, и трансформатор начинает изменять коэффициент трансформации. Это вызывает колебания напряжения на стороне низкого напряжения трансформатора (0.4 кВ), что приводит к нарушению работы подключенных потребителей.

Этот процесс может спровоцировать веерное отключение автоматики и потери питания у конечных потребителей. На диспетчерском пульте появляются сигналы тревоги из-за отклонений параметров сети, и операторы принимают меры по восстановлению нормального режима работы. После устранения последствий инцидента проводится анализ для выявления причины отправки несанкционированной команды. Проверяются логи системы и сетевой трафик на предмет возможных кибератак или сбоев в системе управления.

Этот пример демонстрирует уязвимость электрических сетей в случае проникновения злоумышленников в систему управления, а также

необходимость раннего выявления аномалий (ложных команд).

Понимание аномалий в защите сетей электроснабжения невозможно без знаний особенностей технологического процесса. Кибератаки часто отличаются от обычных сбоев в системе тем, что они не связаны с очевидными причинно-следственными связями в цепочке нарушений. Такие атаки происходят внезапно, что делает их трудными для выявления с помощью традиционных методов [10–14].

В связи с этим задачей исследования являются проведение эксперимента, моделирующего отклонение напряжения в сети, и выбор такого метода анализа этой аномалии, который позволит максимально точно отличить ее от обычного аварийного режима работы электрической сети.

Для проведения исследований были сгенерированы синтетические данные, моделирующие электрическое напряжение в диапазоне от −0.9 кВ до +0.9 кВ (рис. 1). Эти данные охватывают три различных сценария: нормальную работу системы (без отклонений напряжения), резкое отклонение напряжения вследствие кибератаки (без изменения электрической нагрузки) и аварийный режим работы с продолжительным отклонением напряжения (с изменением электрической нагрузки).

В нормальных условиях напряжение описывается синусоидальной функцией времени $U = f(t)$ с добавлением случайного шума, отражающего реальные флуктуации (рис. 1а). Для моделирования кибератаки был искусственно введен внезапный скачок напряжения на 0.3 кВ (рис. 1б). Аварийный режим работы с отклонением напряжения был смоделирован увеличением амплитуды синусоиды на определенный промежуток времени (рис. 1в).

В рамках данного исследования использованы несколько алгоритмов машинного обучения для анализа синтетических данных, моделирующих поведение электрической сети в условиях кибератаки и аварийного режима отклонения электрической нагрузки. В отличие от нейронных сетей, которые требуют значительных вычислительных ресурсов, выбранные методы, такие как метод изолированного леса (Isolation Forest), локальный факторинг выбросов (local outlier factor, LOF), одноклассовая машина опорных векторов (one-class support vector machine, One-Class SVM) и кластеризация методом *k*-средних, обладают меньшей вычислительной сложностью и не требуют большого массива данных для обучения.

Рассмотрим каждый метод отдельно и проанализируем полученные результаты, чтобы оценить их эффективность в выявлении таких аномалий.

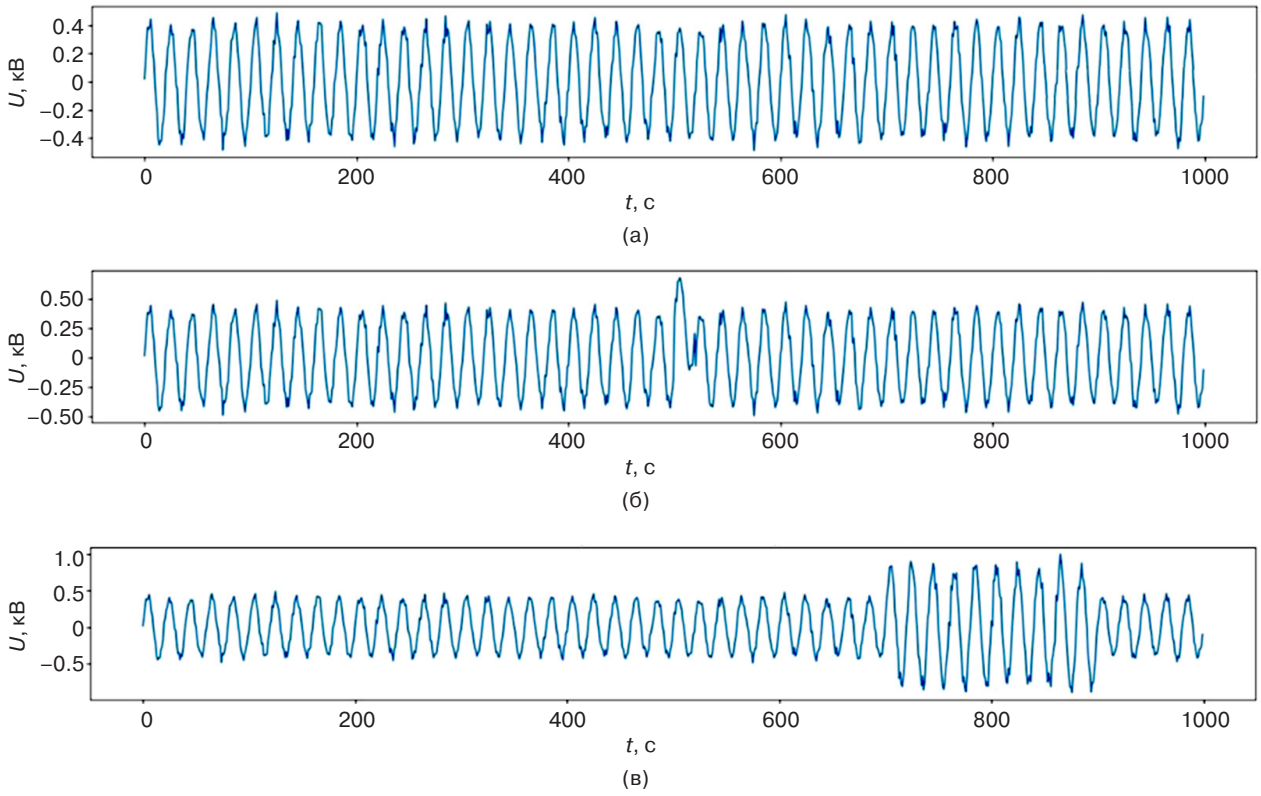

Рис. 1. Моделирование различных режимов работы электрической сети: нормальный режим работы (а); режим с кибератакой (б); обычный режим с отклонением напряжения (в)

Мультифрактальный анализ и метод Isolation Forest

Фрактальные методы позволяют выявлять аномалии в данных, которые могут указывать на изменение состояния системы или наличие внешних воздействий. Это делает их полезными для мониторинга и диагностики различных процессов [15–17].

Применим дискретное вейвлет-преобразование для напряжения и вычислим мультифрактальные признаки – среднее значение и дисперсию абсолютных значений коэффициентов. Вектор этих признаков будем использовать в модели Isolation Forest [18] для обнаружения аномалий.

Пусть $x(t)$ – временной ряд, представляющий данные (например, временной ряд напряжения). Для анализа временного ряда используется дискретное вейвлет-преобразование, которое разлагает сигнал на несколько уровней детализации.

Вейвлет-преобразование W_x сигнала $x(t)$ на уровне j можно записать как:

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

где $\psi_{j,k}(t)$ – функция-вейвлет, сдвинутая и масштабированная версия материнского вейвлета.

Для каждого уровня разложения j получаем набор коэффициентов c_j, которые описывают различные временные масштабы сигнала:

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

На каждом уровне j вейвлет-разложения вычисляются среднее значение и дисперсия абсолютных значений коэффициентов c_j:

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

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

где N_j – количество коэффициентов на уровне j.

Эти признаки составляют вектор признаков для каждого временного ряда:

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

Пусть $\mathbf{F}_i$ – вектор мультифрактальных признаков для i-го временного ряда, тогда множество признаков для всех временных рядов можно записать как матрицу:

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

Проведем обучение модели Isolation Forest [18] на матрице признаков $\mathbf{F}$, чтобы выявить аномалии. При этом модель строит несколько деревьев решений, в которых данные разрезаются на основе случайно выбранных признаков, и пытается изолировать аномальные точки данных с минимальной глубиной дерева.

Аномальные оценки (scores) для каждого временного ряда вычисляются с использованием функции принятия решений:

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

где S_i – оценка аномалии для i-го временного ряда.

Аномальная оценка S_i используется для определения степени отклонения временного ряда от нормального состояния. Низкие значения S_i указывают на сильную аномалию, тогда как высокие значения S_i соответствуют нормальному поведению.

На основе изложенных теоретических принципов была разработана компьютерная программа. С ее помощью и использованием модели Isolation Forest, основанной на мультифрактальных признаках, создана тепловая карта аномалий (рис. 2). Использование тепловых карт для визуализации аномалий обосновано тем, что они позволяют наглядно продемонстрировать повторяющиеся паттерны и отделить нормальные события от кибератак и аварийных режимов.

На тепловой карте горизонтальная ось представляет временные шаги (от 0 до 1000), отображающие последовательные измерения данных во времени, а вертикальная ось отражает оценки аномалий, предсказанные моделью. Градиентная шкала варьируется от черного, указывающего на высокие аномальные оценки (низкая вероятность нормальности), до белого, который свидетельствует о низких аномальных оценках (высокая вероятность нормальности).

Анализ тепловой карты

1. Период равен 0–500 с. Большая часть данных в этом периоде окрашена в белый цвет, что свидетельствует о низких аномальных оценках. Это указывает на то, что модель классифицирует эти данные как нормальные.
2. Период около временной отметки равен 500 с. В этом периоде наблюдается узкая черная полоса, что соответствует высокому аномальному скору.
3. Эта черная полоса явно указывает на кибератаку, которая была синтезирована для имитации резкого отклонения от нормы. Модель успешно идентифицировала это отклонение, что подтверждается наличием черного участка на тепловой карте.

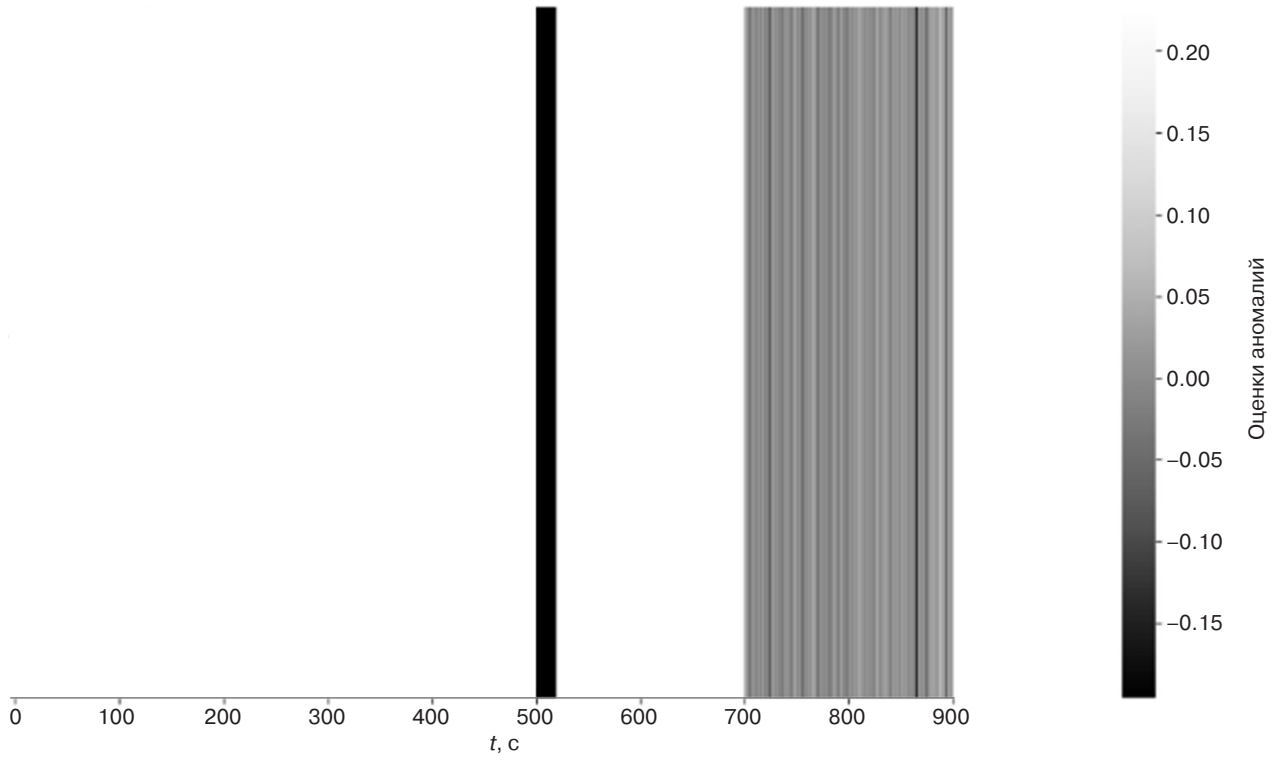

Рис. 2. Тепловая карта аномалий с использованием изолированного леса с мультифрактальными объектами

4. Период равен 700–900 с. На этом участке наблюдается значительная вариативность цветовой шкалы от черного до серого, что связано с аварийным режимом, в котором изменена амплитуда синусоидального сигнала. В отличие от узкой черной полосы, указывающей на кибератаку, здесь видна более сложная и градиентная картина, отражающая аномалию, связанную с рабочим режимом отклонения напряжения, а не с кибератакой.
5. Период равен 900–1000 с. На этом отрезке снова доминирует белый цвет, что указывает на нормальные данные, аналогичные начальному периоду.

LOF-метод

Метод LOF [19] позволяет выявлять локальные аномалии на основе сравнения плотности данных в окрестностях каждой точки.

Локальный фактор выброса для каждой точки x_i рассчитывается следующим образом:

1. Определяется расстояние до ближайших соседей:

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

где k – количество ближайших соседей.

2. Определяется локальная плотность достижимости lrd_k для точки x_i:

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

где $\mathrm{reach\_dist}_k(x_i, x_j)$ – это расстояние, на которое нужно переместиться от x_i к x_j, чтобы достичь плотности x_j.

3. Расчет LOF:

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

Значение $\mathrm{LOF}_k(x_i)$, значительно превышающее 1, указывает на то, что точка x_i является аномальной.

Для визуализации результатов оценки аномалий полученные значения LOF инвертируются:

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

где S_i – аномальная оценка для точки x_i.

На основе этих значений строится тепловая карта (рис. 3), где аномальные точки отображаются в градациях серого, соответствующих степени их отклонения от нормы.

Метод LOF продемонстрировал способность эффективно обнаруживать кибератаки, что отчетливо видно по черной полосе на тепловой карте в области около 500-й точки временного ряда. Однако LOF также

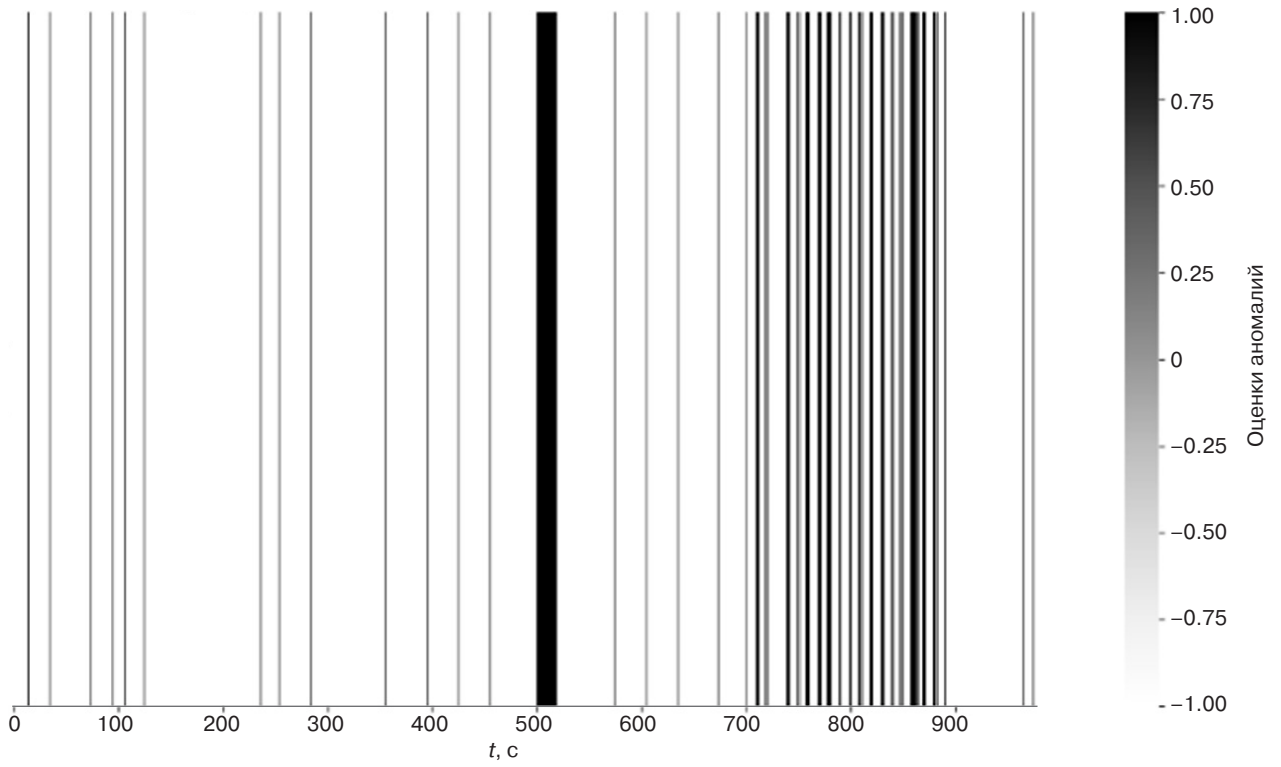

Рис. 3. Тепловая карта оценок аномалий с использованием локального коэффициента выбросов (LOF)

выявил аномалии по всей временной шкале, что может быть как преимуществом, так и недостатком. В частности, в области аварийного режима (700–900 с) наблюдаются значительные изменения, хотя их выделение не столь контрастное. Высокая чувствительность LOF к локальным отклонениям и мелким аномалиям позволяет детектировать тонкие изменения в данных, но вместе с тем может приводить к увеличению числа ложных срабатываний, что требует учета в процессе интерпретации результатов.

Метод кластеризации *k*-средних

Метод *k*-средних предназначен для разбиения набора данных на k кластеров, где каждый кластер характеризуется своим центром (центроидом) [20].

Цель метода заключается в минимизации суммы квадратов расстояний между точками данных и центрами кластеров.

Пусть у нас есть набор данных $\mathbf{X} = \{x_1, x_2, \ldots, x_n\}$, где каждая точка данных x_i является вектором признаков.

Расчет состоит из следующих шагов:

1. Выбирается число кластеров k, на которые нужно разбить данные.
2. Инициализация центроидов:

Инициализируются k начальных центроидов $\{\mu_1, \mu_2, \ldots, \mu_k\}$, которые могут быть выбраны случайным образом из точек данных или другими методами, например, методом *k*-средних++.

3. Назначение точек кластерам:

Для каждой точки данных x_i вычисляется расстояние до каждого из центроидов μ_j:

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

Точка x_i назначается кластеру с минимальным расстоянием:

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

где C_i – кластер, к которому относится точка x_i.

4. Обновление центроидов:

После назначения всех точек пересчитываются центроиды каждого кластера:

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

где $|C_j|$ – количество точек в j-м кластере, а μ_j – новое положение центроида.

5. Повторение шагов 3 и 4.

Шаги 3 и 4 повторяются до тех пор, пока не сойдется процесс (например, пока центроиды не перестанут изменяться или не будет достигнуто максимальное количество итераций).

Метод *k*-средних минимизирует следующую функцию стоимости (функцию потерь):

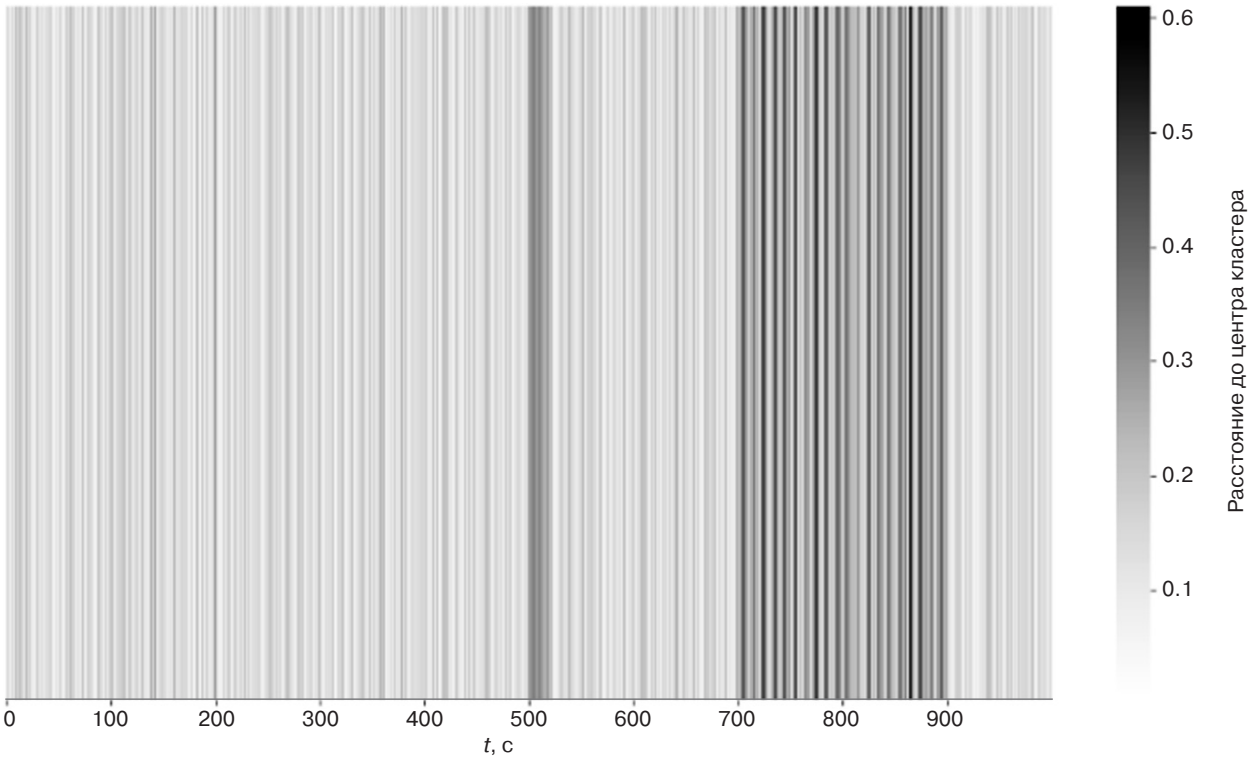

Рис. 4. Тепловая карта расстояний до центров кластеров с использованием кластеризации *k*-средних

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

где J – суммарное внутрикластерное отклонение, а $\left\| x_i - \mu_j \right\|^2$ – квадрат евклидова расстояния между точкой данных и центроидом ее кластера.

На тепловой карте (рис. 4) показаны расстояния до центров кластеров, вычисленные с использованием метода кластеризации *k*-средних. На горизонтальной оси отображены временные шаги, а на вертикальной оси – расстояния до центров кластеров. Градиентная шкала варьируется от светло-серого до черного, где черные области соответствуют максимальным значениям расстояний.

Результаты использования метода кластеризации *k*-средних показали, что метод эффективно справляется с крупными аномалиями, но при плавных изменениях может давать ошибки. Поэтому использование этого метода необходимо сочетать с другими методами для более комплексного анализа аномалий.

Метод One-Class SVM

Метод One-Class SVM [21] обладает рядом особенностей, которые делают его особенно подходящим для задач обнаружения аномалий в критически важных системах, таких как электрические сети. В отличие от других методов, One-Class SVM направлен на обучение модели, которая описывает распределение нормальных данных, и затем используется для выявления отклонений, которые не соответствуют этому распределению. Этот подход особенно полезен в условиях, где имеются ограниченные данные об аномальных состояниях или кибератаках, и основное внимание уделяется выявлению отклонений от нормального состояния системы.

Математически метод One-Class SVM строит гиперплоскость в пространстве признаков, которая отделяет все точки данных от начала координат, стремясь максимизировать расстояние между этой гиперплоскостью и наиболее близкими к ней точками данных. Цель состоит в том, чтобы все нормальные данные располагались по одну сторону гиперплоскости, а аномалии – по другую.

Формально, пусть $\mathbf{x}_i$ обозначает вектор признаков временного ряда, где $i = 1, 2, \ldots, n$. Модель One-Class SVM решает следующую задачу оптимизации:

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

при условии:

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

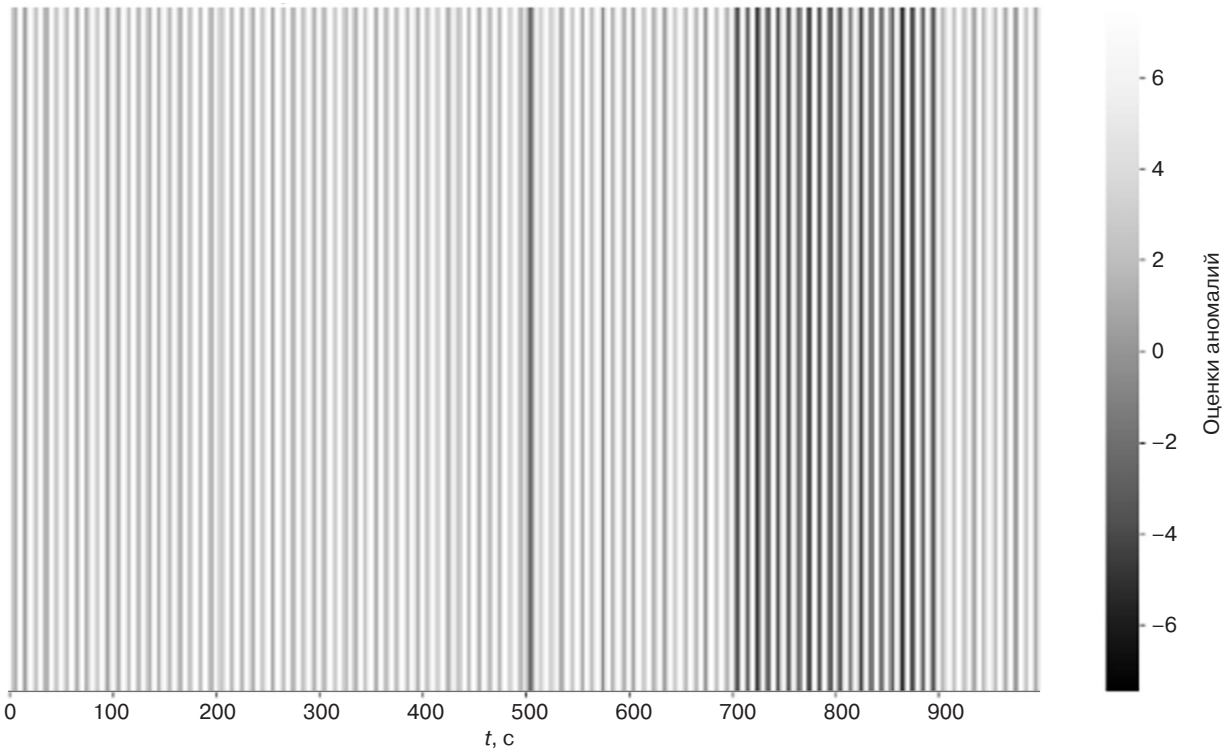

Рис. 5. Тепловая карта оценок аномалий с использованием метода One-Class SVM

Здесь **w** – вектор весов, ρ – смещение гиперплоскости, ξ_i – переменные разрывов (slack variables), $\phi(\mathbf{x}_i)$ – функция отображения в высокоразмерное пространство признаков, а v – гиперпараметр, контролирующий допустимую долю выбросов и сложность модели.

Результатом работы One-Class SVM является функция принятия решений:

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

Значения $f(\mathbf{x}) \geq 0$ указывают на потенциальные аномалии, тогда как значения $f(\mathbf{x}) < 0$ соответствуют нормальным данным.

Выполнив расчет с помощью метода One-Class SVM, получим результаты, которые показаны на тепловой карте (рис. 5).

Метод One-Class SVM продемонстрировал высокую эффективность в выявлении как резких, так и плавных аномалий в синтетических данных, моделирующих работу электрической сети. Способность этого метода обнаруживать различные типы отклонений подтверждается контрастными областями на тепловой карте, соответствующими как кибератаке, так и аварийному режиму. Данный подход может быть полезен для мониторинга критически важных инфраструктур, где важно своевременное выявление аномалий для предотвращения нарушений в работе системы.

ЗАКЛЮЧЕНИЕ

На основании проведенного анализа тепловых карт можно заключить, что различные методы обнаружения аномалий демонстрируют разную степень эффективности в контексте выявления киберугроз и других отклонений в электрических системах. Метод Isolation Forest показал наилучшие результаты в обнаружении резких изменений, связанных с кибератаками, выделяя такие аномалии с высокой точностью и минимальным числом ложных срабатываний. В то же время, метод LOF также продемонстрировал способность к выявлению кибератак, однако, его повышенная чувствительность к мелким отклонениям привела к увеличению числа ложных срабатываний, что требует дополнительного внимания при интерпретации результатов.

Методы кластеризации *k*-средних и One-Class SVM проявили себя менее контрастно по сравнению с Isolation Forest, но имеют свои преимущества. Метод кластеризации *k*-средних оказался полезным для общей кластеризации данных, однако, оказался менее эффективным в выявлении резких аномалий. Метод One-Class SVM, в свою очередь, продемонстрировал способность к обнаружению как резких, так и плавных изменений, но с меньшей контрастностью в выделении аномалий, что также требует учета при выборе подходящего метода для задач мониторинга и защиты критически важных инфраструктур. В целом Isolation Forest является наиболее предпочтительным методом

для выявления киберугроз, однако, для комплексного анализа аномалий рекомендуется использование нескольких методов в сочетании.

На основании проведенных исследований можно сделать вывод о необходимости сочетания различных методов в зависимости от характера изменения электрической нагрузки с целью эффективного предотвращения кибератак на смарт-сети.

Вклад авторов

С.В. Кочергин – общая концепция исследования, определение основных проблем, формулировка целей и задач, обзор литературы в области кибербезопасности интеллектуальных сетей, подготовка материалов для экспериментальной части исследования и проведение экспериментов.

С.В. Артемова – разработка методологии исследования, выбор подходов машинного обучения для сравнения, подготовка статьи и ее редактирование.

А.А. Бакаев – определение темы исследования и обсуждение финального текста статьи.

Е.С. Митяков – интерпретация результатов исследований, подготовка выводов.

Ж.Г. Вегера – математическая интерпретация исследований.

Е.А. Максимова – анализ существующих методов обнаружения аномалий и определение наиболее перспективных из них для сравнения.

Каждый из авторов внес свой уникальный вклад в подготовку этой научной статьи.

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.

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.

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.). Available from URL: https://doi.org/10.14529/secur210404, 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.

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 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