ОБЕСПЕЧЕНИЕ ФУНКЦИОНАЛЬНОСТИ ЦИФРОВЫХ УСТРОЙСТВ РЕЛЕЙНОЙ ЗАЩИТЫ ПРИ КИБЕРАТАКАХ НА МИКРОСЕТИ С РАСПРЕДЕЛЕННЫМИ ЭНЕРГЕТИЧЕСКИМИ РЕСУРСАМИ

Гурина Л. А.[1], Томин Н. В.[2]

DOI: 10.21681/2311-3456-2025-4-55-64

Цель исследования: *разработка метода достоверизации данных, используемых в цифровых системах релейной защиты, автоматики и управления микросетями с распределенными энергетическими ресурсами.*

Методы исследования: *вероятностные методы, методы машинного обучения.*

Результат исследования: *рассмотрено информационное обеспечение схем релейной защиты микросетей, проанализированы возможные кибератаки, при успешной реализации которых может стать нарушение функциональности цифровых устройств релейной защиты микросетей. Разработан метод достоверизации данных с использованием методов обучения без учителя, включая изоляционный лес и метод k-ближайших соседей, который эффективно выявляет и корректирует ошибки в измерениях при атаках внедрения ложных данных на информационную инфраструктуру систем защиты микросетей.*

Научная новизна *состоит в том, что предложен подход, обеспечивающий устойчивость систем релейной защиты микросетей при кибератаках и, тем самым, не допускающий ложных срабатываний и отказов устройств защиты.*

Ключевые слова: *активные системы распределения электроэнергии, схемы защиты, кибербезопасность, достоверизация данных, случайные процессы, машинное обучение.*

Введение

В настоящее время наблюдается постепенное сокращение доли традиционных источников энергии, что сопровождается массовым внедрением генерирующих объектов на основе возобновляемых источников энергии (ВИЭ) [1, 2]. Процессы декарбонизации и интеллектуализации энергетических систем позволяют эффективно использовать всевозможные вилы источников энергии [3]. Одним из путей развития активных систем распределения электрической энергии, включающих высокий уровень объектов распределенной энергетики, является интеграция в них микросетей (МС). Такие МС в силу внедрения объектов распределенной энергетики и ВИЭ с привлечением устройств силовой электроники имеют достаточно сложную информационную инфраструктуру, отказы и сбои в которой могут оказывать существенное влияние на надежность и безопасность не только МС, но и всей распределительной сети. Кроме того, при цифровой трансформации МС становятся более уязвимыми к кибератакам [4, 5].

Активные системы распределения электроэнергии отличаются от традиционных распределительных сетей тем, что могут иметь двунаправленные потоки мощности, широкое внедрение распределенных энергетических ресурсов (РЭР), возможности хранения электрической энергии, сложные стратегии управления и обладают высокой зависимостью от информационной инфраструктуры, увеличивая их уязвимости к киберугрозам.

Концепцией построения современных распределительных сетей, включающих РЭР, является интеграция в них МС, позволяющим повысить наблюдаемость и управляемость, а также обеспечить надежное электроснабжение потребителей. МС с РЭР все чаще развертываются для повышения операционной гибкости, устойчивости, возможностей скоординированного управления. Созданная на основе интеллектуальных технологий информационная инфраструктура активных систем распределения электрической энергии позволяет расширить перечень решаемых технологических задач и повысить эффективность управления МС с РЭР. К информационной инфраструктуре относятся в первую очередь каналы передачи данных от локальных контроллеров до центрального контроллера в случае централизованного управления или сеть передачи

1 Гурина Людмила Александровна, кандидат технических наук, доцент, старший научный сотрудник лаборатории управления функционированием электроэнергетических систем Института систем энергетики им. Л. А. Мелентьева СО РАН, Иркутск, Россия. E-mail: gurina@isem.irk.ru

2 Томин Никита Викторович, кандидат технических наук, заведующий лабораторией управления функционированием электроэнергетических систем Института систем энергетики им. Л. А. Мелентьева СО РАН, Иркутск, Россия. E-mail: tomin.nv@gmail.com

данных между соседними контроллерами при распределенном управлении МС. С расширением возможностей злоумышленников для проведения успешных кибератак, связанных с ростом уязвимостей в информационной инфраструктуре, требуется разработка методов своевременного обнаружения кибератак и устранения их влияния на функциональность систем релейной защиты (РЗ), автоматики и управления МС с РЭР.

В зависимости от типа активной системы распределения электроэнергии МС подразделяются на сети постоянного тока, переменного тока и гибридные [6]. Для обеспечения надежной работы МС с РЭР важно решение таких задач, как управление режимами, распределение мощности, сохранение устойчивости и эффективной работы средств РЗ. Причем, зашита МС с РЭР становится первостепенной для сохранения их безопасной работы в условиях новых вызовов и угроз [7]. Функционирований МС с РЭР зависит от ее информационной инфраструктуры из-за большого числа коммуникаций [8]. При успешной реализации кибератак несвоевременное принятие мер по их обнаружению и подавлению последствий может привести к всевозможным сбоям и отказам в технологической подсистеме МС с РЭР [9]. Надежная работа МС с РЭР требует достоверных измерений и защищенных от кибератак систем РЗ, автоматики и управления [10].

Обнаружение неисправностей и защита от них МС с РЭР – сложная проблема из-за переменных по величине и двунаправленных потоков мощности, а также различных типов распределенных источников энергии и мест их подключения. В последнее время, наряду с применением традиционных средств РЗ, в МС с РЭР внедряются инновационные защиты, например, адаптивные РЗ, защита на основе IoT, мультиагентные РЗ, РЗ на основе машинного обучения, искусственного интеллекта и др. Наряду с преимуществами применения таких РЗ возникают проблемы, связанные с нарушениями функциональности схем защиты, целостности и доступности данных в результате кибератак на информационную инфраструктуру МС с РЭР.

Использование современных устройств и датчиков для мониторинга, защиты и управления МС с РЭР также может привести к нарушению их кибербезопасности. Срабатывания устройств РЗ зависят от каналов передачи данных, которые могут быть подвержены множеству кибератак. В результате успешной кибератаки может произойти изменение настроек не только РЗ, но и всего комплекса контролирующих устройств. Современные системы РЗ различных видов требуют наличия информационно-коммуникационной инфраструктуры, на которую могут воздействовать злоумышленники. Таким образом, инновационные защиты МС с РЭР могут оказаться неэффективными в условиях кибератак, последствиями которых могут быть отказы объектов информационной системы, каналов связи, а также нарушение качества данных. Обеспечение кибербезопасности цифровых защит МС с РЭР становится актуальным.

В статье рассмотрены проблемы в области кибербезопасности схем РЗ и возможные пути их решения для осуществления безопасной и надежной работы МС РЭР.

Стратегии защиты МС с РЭР и их информационное обеспечение

В [11] представлен обзор технических достижений, направленных на улучшение традиционных механизмов РЗ, используемых в пассивных распределительных сетях, а также разработку современных схем РЗ, основанных на инновационных подходах и новых методах. Подчеркивается, что адаптивные системы защиты, разработанные как для децентрализованных, так и для централизованных структур, в целом обеспечивают надежную защиту для МС с РЭР. Современные устройства РЗ, которые интегрируют передовые функциональные возможности защиты, демонстрируют лучшие показатели в таких областях, как надежность, чувствительность, селективность и скорость работы.

Во время работы МС с РЭР могут возникать аномальные и аварийные ситуации из-за таких факторов, как токовые перегрузки и короткие замыкания. Обнаружение этих условий и определение неисправных компонентов в МС является сложной задачей. В результате в МС с отключаемыми объектами распределенной генерации требуется тщательный анализ влияния информации, прежде всего, содержащей «плохие данные», для предотвращения сбоев в работе, а также нежелательных или ложных срабатываний РЗ [12] в случае кибератак. В исследовании [13] предлагается объединить централизованную защиту, дистанционную и многоагентную РЗ в единую категорию, известную как распределенные системы РЗ, с использованием протокола беспроводных приложений (WAP). Такие распределенные системы имеет высокий потенциал благодаря достижениям в области информационно-коммуникационной инфраструктуры в МС с РЭР, что позволяет эффективно обмениваться большими объемами данных [14].

Внедрение дистанционного управления для выключателей, развертывание дополнительных датчиков тока и напряжения [15], а также использование устройств РЗ на основе современных интеллектуальных алгоритмов и возможности удаленной настройки параметров защиты способствуют возрастанию восприимчивости систем РЗ к киберугрозам.

Существуют две основные методологии для построения адаптивных систем РЗ: децентрализованная и централизованная. Централизованный подход включает архитектуру управления, которая взаимодействует с каждым устройством РЗ, настраивая их конфигурации в зависимости от текущего режима МС с РЭР. В отличие от этого, децентрализованный подход основывается на обмене данными между цифровыми устройствами РЗ, когда каждое такое устройство может независимо изменять свои настройки на основе информации, полученной от других устройств. Значительная часть исследований в области адаптивной защиты сосредоточена на использовании интеллектуальных аналитических методов, таких как мультиагентные методы, которые способны обрабатывать большие объемы данных [16].

Система, которая объединяет отдельных агентов, работающих на достижение общей цели с использованием данных от каждого агента для выработки решений, называется мультиагентной системой (МАС). Применение МАС при реализации защиты МС с РЭР является достаточно эффективным, поскольку вводит новые методы для оптимизации целевой функции, тем самым улучшая селективность и скорость реакции. В [17] предлагается схема дифференциальной защиты с использованием МАС с регулируемыми временными задержками срабатывания. Агенты оснащены слоями первичной, резервной и шиной защиты, которые применяются как для первичной, так и для резервной защиты. В [18] вводится схема защиты, включающая алгоритм Q-обучения и МАС. Агенты обучаются с использованием алгоритма Q-обучения для выявления и устранения неисправностей. Кроме того, агенты общаются через децентрализованные сети на основе блокчейна. В [19] представлена схема защиты, использующая надежные интеллектуальные агенты. Обнаружение неисправностей осуществляется путем измерения напряжения и тока. Компоненты функционируют как агенты, передающие решения вышестоящим управляющим слоям и смежным компонентам для повышения общей производительности.

Основной и ключевой функцией схем защиты является распознавание и обнаружение возникновения неисправностей. Для предотвращения аварийных ситуаций в МС с РЭР в системах релейной защиты и автоматики заложены схемы обнаружения и классификации неисправностей, которые могут быть основаны на обработке сигналов, знаниях и моделях.

В активных системах распределения электроэнергии, в том числе и в МС с РЭР, широкое распространение получили методы обнаружения неисправностей, основанные на обработке сигналов. При возникновении аварийных ситуаций параметры системы отклоняются от значений при нормальной функционировании системы. Для обнаружения неисправностей в активных системах распределения электроэнергии на основе обработки сигналов применяют вейвлет-анализ данных [20], Фурье-анализ сигналов [21], оконное преобразование Фурье [22], метод эмпирической модовой декомпозиции сигналов и преобразование Гильберта-Хуанга [23].

Наряду с методами обнаружения неисправностей, основанных на обработке сигналов, в системах релейной защиты и автоматики применяются такие методы искусственного интеллекта и машинного обучения, как искусственные нейронные сети, глубокое обучение, алгоритмы обучения с подкреплением, нечеткая логика, адаптивные системы нечеткого вывода, метод опорных векторов и т.д. [24–27].

Методы обнаружения неисправностей в МС с РЭР на основе модели используют аналитические знания для оценки параметров системы. Авторами [28] предложен метод на основе инверторов, применение которого позволяет обнаруживать неисправности независимо от режима работы МС с РЭР и от уровней токов короткого замыкания.

В [29] определено понятие обнаружение локализации неисправности, представляющего собой определение местоположения неисправности с максимальной точностью и достоверностью. Сами методы определения локализации неисправностей подразделяются на основе сигналов напряжения и тока на основной частоте [30].

Метод восстановления качества данных при кибератаках на информационную инфраструктуру систем защиты МС с РЭР

Развертывание МС с РЭР требует применения адаптивных схем защиты, устройства которых могут изменять свои настройки при каких-либо изменениях, обусловленных внутренними и внешними угрозами. Даже незначительные неисправности в информационной инфраструктуре могут иметь катастрофические последствия для физической части МС с РЭР. Внедрение цифровых устройств измерений, датчиков, устройств РЗ, использование многочисленных каналов связи и применение различных методов обнаружения неисправностей на основе искусственного интеллекта, машинного обучения и требующих большого многообразия данных для реализации схем защиты без соответствующих мер по обеспечению кибербезопасности может привести к отказам функционирования МС с РЭР при кибератаках [31].

Функциональность устройств и каналов связи информационной инфраструктуры являются важным для реализации современных алгоритмов адаптивной защиты.

Возможные кибератаки и их последствия для схем защиты могут быть следующими:

- Атака, направленные на целостность. Данная кибератака может быть в виде ложной команды, последствиями которой являются изменение логики управления и неправильная работа цифровых объектов релейной защиты.
- Атака «человек по середине». При атаке «человек по середине» противником может быть получена экстренная информации об изменении режима работы устройства релейной защиты и, в дальнейшем, заменена нужной для злоумышленника информацией.
- Атака повторного воспроизведения. При получении доступа к передаче данных по каналам связи противники могут повторять отправку данных из ранее отправленных, имитируя появление нарушений, которые имели место быть.
- Атака внедрения ложных данных. При данной кибератаке противники могут сымитировать ложные изменения в конфигурациях микропроцессорных устройств релейной защиты для отключения их функций при возникновении аварийных ситуаций.
- Атака отказа в обслуживании. При атаке отказа в обслуживании противник может вызвать сбои в каналах связи, переполнение буфера и, тем самым, нарушить передачу потоков данных. При этом возникает потеря информации, используемая в схемах защиты.
- Вредоносный код. При внедрении вредоносного кода в цифровое устройство РЗ может произойти переполнение буфера.

В области защиты МС с РЭР мультиагентные системы являются эффективными платформами связи в реальном времени. Модульная структура агентов обеспечивает более тесное взаимодействие между информационной инфраструктурой и технологической частью МС для реализации их деятельности с помощью сложных программных платформ.

Ранее авторами [32] была разработана двухэтапная процедура обнаружения и восстановления качества данных при кибератаках с использованием методов машинного обучения без учителя: изоляционный лес (англ. Isolation Forest) и k-ближайших соседей (англ. k-nearest neighbors algorithm, k-NN) при вторичном регулировании напряжения на основе МАС. Важно заметить, что обнаружение аномалий с помощью ансамблевой модели (алгоритм изоляционного леса) не требует разметки данных и эффективно выявляет отклонения в параметрах системы. Кроме того, при восстановлении данных с помощью метода k-ближайших соседей, используется информация о соседних нормальных измерениях для предполагаемых аномалий. На рис. 1 показана архитектура этой процедуры, где s_1, s_2, ..., s_N являются измеренными значениями, полученными физическим объектом (выход датчика), переменные f_1, f_2, ..., f_N – двоичные переменные, выводимыми моделью изоляционного леса и указывающие на присутствие сбоя и/или грубого измерения датчика, s_1, s_2, ..., s_N – «восстановленные» данные, в случае если грубое измерение было обнаружено в модели изоляционного леса и N – количество датчиков.

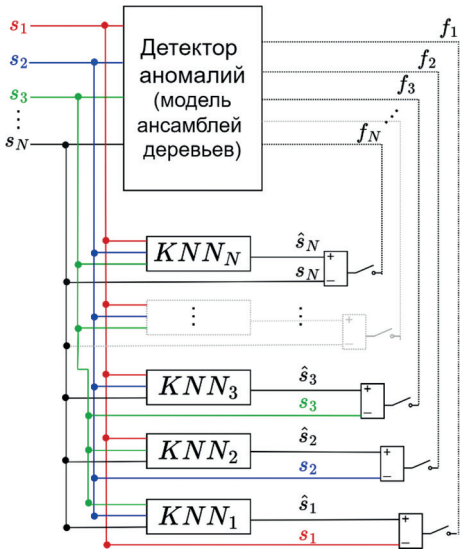

Рис. 1. Схема достоверизации данных на основе моделей машинного обучения

Данная процедура была развита и адаптирована и для схем защиты МС. Рассмотрим систему из N взаимосвязанных МС, где каждая i-ая МС характеризуется следующими параметрами: измеренные датчиками напряжение $V(t)$ и ток $I(t)$, значения которых изменяются во времени t. Пусть в примере взаимосвязанная система будет состоять из трех МС ($N = 3$). Смоделировать измерения процессов изменения напряжения и тока можно с учетом нормальной работы цифровых датчиков и случайного шума:

$$V(t) = V_0 + A_V \sin(\omega t) + \epsilon_V(t), \quad (1)$$

$$I(t) = I_0 + A_I \sin(\omega t + \phi) + \epsilon_I(t), \quad (2)$$

где V_0 и I_0 – средние значения напряжения и тока; A_V и A_I – амплитуды колебаний; ω – угловая частота; ϕ – фазовый сдвиг между напряжением и током; $\epsilon_V(t)$ и $\epsilon_I(t)$ – случайный шум, распределенный по нормальному закону.

Для оценки влияния кибератаки на цифровые устройства РЗ была смоделирована атака внедрения ложных данных в виде ошибок измерений случайного процесса изменения напряжения и тока [33],

которая моделируется как мультипликативное искажение:

$$V_i^{\text{атака}}(t_k) = V_i(t_k) \cdot k_{Vi}(t_k), \quad k_{Vi} \sim U(0.5,1.5), \tag{3}$$

$$I_i^{\text{атака}}(t_k) = I_i(t_k) \cdot k_{Ii}(t_k), \quad k_{Ii} \sim U(0.5,1.5), \tag{4}$$

где k_{Vi} и k_{Ii} – случайные коэффициенты искажения, применяемые к выбранным моментам времени t_i.

Для обнаружения аномалий используется алгоритм изоляционного леса, который идентифицирует точки, резко отличающиеся от общей структуры данных. Алгоритм основывается на построении множества случайных деревьев решений, где аномальные точки изолируются на меньшей глубине дерева по сравнению с нормальными данными. Для каждой i-ой МС алгоритм изоляционного леса может быть записан следующим образом:

$$s_i(V_i,I_i) = \frac{1}{M} \sum_{m=1}^{M} h_m(V_i,I_i), \tag{5}$$

h_m – глубина изоляции в дереве m, M – количество деревьев.

Помимо алгоритма изоляционного леса для детектирования аномалий используется координационный механизм между агентами МАС:

$$s_i^{glob} = \alpha s_i + \beta \frac{1}{|N_i|} \sum_{j \in N_i} s_j, \tag{6}$$

где N_i – соседние МС, $\alpha + \beta = 1$ – веса локальных и глобальных показателей.

После выявления аномальных измерений производится восстановление корректных значений с использованием метода k-ближайших соседей. Для каждого аномального измерения напряжения $V_{\text{КА}}(t_i)$ находим k-ближайших соседей среди нормальных данных по признакам времени и тока $[t, I(t)]$. Восстановленное значение напряжения вычисляется как среднее значение напряжения этих соседей:

$$V_{\text{восст}}(t_i) = \frac{1}{k} \sum_{j=1}^{k} V_j, \tag{7}$$

где V_j – значения напряжения у k-ближайших соседей.

Алгоритм работы МАС для координации киберзащиты цифровых средств РЗ микросетей на основе двухуровневой процедуры может быть описан следующим образом. Каждый агент A_i независимо обнаруживает аномалии в своей МС. Агенты обмениваются показателями аномальности s_i. При превышении порога $S_i^{glob} > S$ запускается процедура восстановления. Восстановленные значения используются для корректировки уставок защит.

Результаты достоверизации измерений тока и напряжения на основе предлагаемого метода при смоделированных кибератаках на устройства РЗ представлены на рис. 2. На рис. 3 показаны результаты восстановления качества данных с использованием предложенной процедуры. Хорошо видно, что категория «attacked», которая указывает на искаженные, но невосстановленные данные, фактически равна нулю, что свидетельствует о высокой эффективности предложенного подхода.

В результате моделирования была количественно оценена эффективность как модели обнаружения аномалий, так и модели восстановления качества данных. Полученные результаты, представленные в табл. 1, демонстрирует высокую эффективность алгоритма изоляционного леса в идентификации

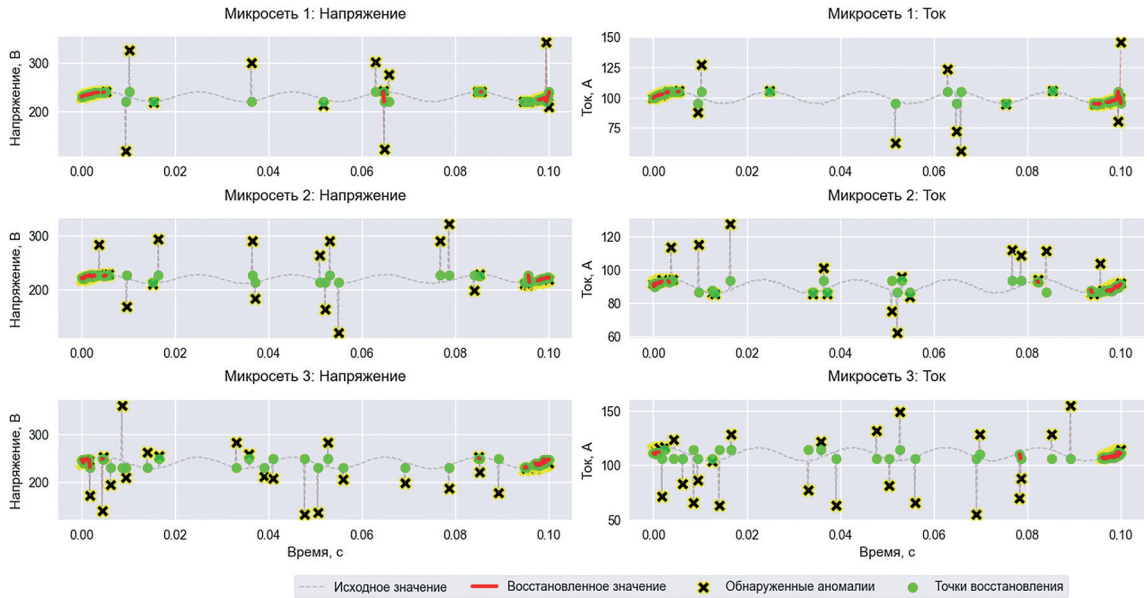

Рис. 2. Восстановление данных измерений при атаке внедрения ложных данных на устройства мультиагентной РЗ для взаимосвязанных микросетей

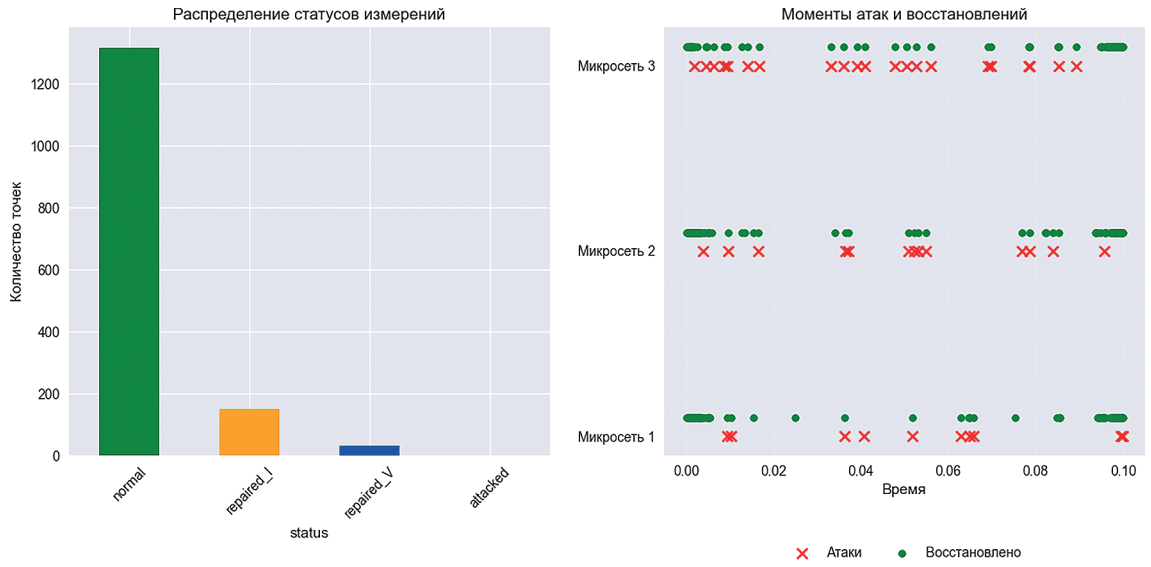

Рис. 3. Результат процесса восстановления качества данных цифровых устройств РЗ микросетей, связанных МАС для координации и регулирования: а) распределение статусов измерений (normal – нормальные измерения, $repaired_I$ и $repaired_V$ – восстановленные измерения тока и напряжения соответственно, attacked – искаженные, невосстановленные измерения); б) моменты атак и восстановлений

аномальных измерений. Модель достигла точности и полноты 98–100 % для обоих классов, что свидетельствует о практически безошибочном распознавании как нормальных данных (класс 0), так и аномалий (класс 1). Общая точность составляет 100 %, а средние значения метрик (macro avg и weighted avg) подтверждают стабильность и надежность модели [34]. Эти результаты указывают на то, что предложенный подход обеспечивает эффективное обнаружение аномалий, что существенно повышает устойчивость схем защиты МС с РЭР в условиях возможных кибератак.

Таблица 1.

Обнаружение аномалий на базе алгоритма изоляционного леса

	precision	**recall**	**f1-score**	**support**
0	1.00	1.00	1.00	950
1	0.98	0.98	0.98	50
accuracy			1.00	1000
macro avg	0.99	0.99	0.99	1000
weighted avg	1.00	1.00	1.00	1000

Для оценки восстановления качества данных на базе алгоритма k-ближайших соседей были вычислены следующие метрики: среднеквадратическая ошибка (MSE), средняя абсолютная ошибка (MAE) и средняя абсолютная процентная ошибка (MAPE) [35]. Результаты оценки этих показателей представлены в табл. 2. Низкие значения MSE и MAE указывают на то, что восстановленные значения очень близки к истинным в абсолютных единицах. Низкий MAPE (менее 1-2 %) свидетельствует о высокой относительной точности восстановления по сравнению с истинными значениями.

Таблица 2.

Оценка эффективности восстановления качества данных

Параметр	**Показатели**		
	MSE	**MAE**	**MAPE, %**
Напряжение	0.53	0.58	0.26
Ток	0.03	0.15	1.48

Выводы

Проанализированы стратегии защиты МС с РЭР. Показано, что современные виды защит требуют наличия информационно-коммуникационной инфраструктуры, что увеличивает уязвимости схем защиты к кибератакам. Выявлены возможные последствия реализованных кибертак на функциональность схем защиты МС с РЭР. Разработан подход к достоверизации данных, позволяющий обнаруживать ошибки в измерениях и восстанавливать данные, требуемые для цифровых систем релейной защиты МС с РЭР, тем самым, предотвращая ложные срабатывания и сбои в работе устройств релейной защиты при кибератаках. Результаты демонстрируют высокую точность обнаружения аномалий в измерениях напряжения и тока (до 98–100 % успешных

обнаружений) и их восстановления (средняя ошибка не превышает 1-2 %). Система успешно масштабируется для нескольких взаимосвязанных микросетей, сохраняя стабильность работы при различных типах атак. Реализация данного метода способствует повышению кибербезопасности схем релейной защиты, позволяя обеспечить надежность и безопасность функционирования МС с РЭР.

Работа выполнена в рамках научного проекта «Теоретические основы, модели и методы управления развитием и функционированием интеллектуальных электроэнергетических систем», № FWEU-2021-0001.

Литература

1. Воропай Н. И. Направления и проблемы трансформации электроэнергетических систем // Электричество. 2020. № 7. С. 12–21. DOI: 10.24160/0013-5380-2020-7-12-21.
2. Илюшин П. В. Интеграция электростанций на основе возобновляемых источников энергии в Единой энергетической системе России: обзор проблемных вопросов и подходов к их решению // Вестник Московского энергетического института. 2022. № 4. С. 98–107. DOI: 0.24160/1993-6982-2022-4-98-107.
3. Ilyushin P., Filippov S., Kulikov A., Suslov K. and Karamov D. Intelligent Control of the Energy Storage System for Reliable Operation of Gas-Fired Reciprocating Engine Plants in Systems of Power Supply to Industrial Facilities // Energies. 2022. Vol. 15, 6333. DOI: 10.3390/en15176333.
4. Гурина Л. А. Показатели киберустойчивости компонентов информационно-коммуникационной инфраструктуры при управлении киберфизическими энергетическими системами // Методические вопросы надежности больших систем энергетики. 2022. Выпуск 73. С. 279–288.
5. Дураковский А. П., Марков А. С. Актуальные вопросы кибербезопасности в энергетике // Безопасные информационные технологии. 2024. С. 94–98.
6. Shaukat N. et al. Decentralized, Democratized, and Decarbonized Future Electric Power Distribution Grids: A Survey on the Paradigm Shift From the Conventional Power System to Micro Grid Structures // in IEEE Access. 2023. Vol. 11. Pp. 60957–60987. DOI: 10.1109/ACCESS.2023.3284031.
7. Lu H., Biyawerwala H. and Thakrawala H. Polarized Distribution Protection Coordination Strategy Under the Impact from Various Distributed Energy Resources (DER) Generation Points // 2022 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), New Orleans, LA, USA. 2022. Pp. 1–5. DOI: 10.1109/TD43745.2022.9816925.
8. S. K. T, Jadoun V. K., J. N. S and S. S. A Systematic Study on the Intelligent Cyber Security for Smart Microgrid // 2024 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER), Mangalore, India. 2024. Pp. 237–242. DOI: 10.1109/DISCOVER62353.2024.10750634.
9. Canaan B., Colicchio B., Abdeslam D. O. Microgrid Cyber-Security: Review and Challenges toward Resilience // Applied Sciences. 2020. Vol. 10, no. 16. Pp. 5649. DOI: 10.3390/app10165649.
10. Ding D., Han Q. -L., Ge X. and Wang J. Secure State Estimation and Control of Cyber-Physical Systems: A Survey // in IEEE Transactions on Systems, Man, and Cybernetics: Systems. Jan. 2021. Vol. 51, No. 1. Pp. 176–190. DOI: 10.1109/TSMC.2020.3041121.
11. Илюшин П. В., Вольный В. С. Обзор методов решения проблемных вопросов функционирования устройств защиты в microgrid напряжением до 1 кВ с распределенными источниками энергии // Релейная защита и автоматизация. 2022. № 4(49). С. 6–21.
12. Zheng Dehua, Zhang Wei, Netsanet Solomon, Wang Ping, Bitew Girmaw Teshager, Wei Dan, Yue Jun. Key technical challenges in protection and control of microgrid // Microgrid Protection and Control. 2021. Pp. 45–56. DOI: 10.1016/B978-0-12-821189-2.00007-3.
13. Patnaik B., Mishra M., Bansal R. C., Jena R. K. AC microgrid protection – A review: Current and future prospective // Applied Energy. 2020. Vol. 271. Pp. 115210. DOI: 10.1016/J.APENERGY.2020.115210.
14. Abd el-Ghany H. A. Optimal PMU allocation for high-sensitivity wide-area backup protection scheme of transmission lines // Electric Power Systems Research. 2020. Vol. 187. Pp. 106485. DOI: 10.1016/J.EPSR.2020.106485.
15. Kulikov A., Loskutov A., Bezdushniy D. Relay Protection and Automation Algorithms of Electrical Networks Based on Simulation and Machine Learning Methods // Energies. 2022. Vol. 15(18). Pp. 6525. DOI: 10.3390/en15186525.
16. Shobole A. A., Wadi M. Multiagent systems application for the smart grid protection // Renewable and Sustainable Energy Reviews. 2021. Vol. 149. Pp. 111352. DOI: 10.1016/J.RSER.2021.111352.
17. Verma R., Gawre S. K., Patidar N. P. An Analytical Review on Measures of Microgrid Protection // 2022 IEEE International Conference on Power Electronics, Drives and Energy Systems (PEDES), Jaipur, India. 2022. Pp. 1–6. DOI: 10.1109/PEDES56012.2022.10080291.
18. Cui S., Zeng P., Wang Z., Song C. Research on Intelligent Protection Technology for Distribution Network with Distributed Generation // 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China. 2021. Pp. 1549–1554. DOI: 10.1109/IAEAC50856.2021.9390692.
19. Fawzy N., Habib H. F., Mohammed O., Brahma S. Protection of Microgrids with Distributed Generation based on Multiagent System // 2020 IEEE International Conference on Environment and Electrical Engineering and 2020 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe), Madrid, Spain. 2020. Pp. 1–5. DOI: 10.1109/EEEIC/ICPSEurope49358.2020.9160827.
20. Chaitanya B. K., Anamika Yadav. Empirical Wavelet Transform-Based Differential Protection Scheme for Micro-Grid // Journal of The Institution of Engineers (India): Series B. 2023. 104. Pp. 1–10. DOI: 10.1007/s40031-023-00869-0.
21. Uddin M. N., Arifin M. S., Rezaei N. A Novel Neuro-Fuzzy Based Direct Power Control of a DFIG based Wind Farm Incorporated with Distance Protection Scheme and LVRT Capability // 2022 IEEE Industry Applications Society Annual Meeting (IAS), Detroit, MI, USA. 2022. Pp. 01–08. DOI: 10.1109/IAS54023.2022.9939684.

22. Chaitanya B. K., Anamika Yadav, Mohammad Pazoki. High Impedance Fault Detection Scheme for Active Distribution Network Using Empirical Wavelet Transform and Support Vector Machine // 2020 15th International Conference on Protection and Automation of Power Systems (IPAPS). 2020. Pp. 149–152. DOI:10.1109/IPAPS52181.2020.9375620.
23. Shaik M., Shaik A. G., Yadav S. K. Hilbert–Huang transform and decision tree based islanding and fault recognition in renewable energy penetrated distribution system // Sustainable Energy, Grids and Networks. 2022. 30. Pp. 100606. DOI: 10.1016/j.segan.2022.
24. Raad Salih Jawad, Hafedh Abid. HVDC Fault Detection and Classification with Artificial Neural Network Based on ACO-DWT Method // Energies. 2023. Vol. 16. Pp. 1064. DOI: 10.3390/en16031064.
25. Chandran L. R., A. Parvathy V S, I. K, Nair M. G. Adaptive Over Current Relay Protection in a PV Penetrated Radial Distribution System With Fuzzy GA Optimisation // 2022 IEEE 19th India Council International Conference (INDICON), Kochi, India. 2022. Pp. 1–7. DOI: 10.1109/INDICON56171.2022.10040021.
26. Nasir M., Bansal R., Elnady A. A Review of Various Neural Network Algorithms for Operation of AC Microgrids // 2022 Advances in Science and Engineering Technology International Conferences (ASET), Dubai, United Arab Emirates. 2022. Pp. 1–7. DOI: 10.1109/ASET53988.2022.9734899.
27. Vincent Nsed Ogar, Sajjad Hussain, Kelum A. A. Gamage. The use of artificial neural network for low latency of fault detection and localisation in transmission line // Heliyon. 2023. Vol. 9. Pp. e13376. DOI: 10.1016/j.heliyon.2023.
28. Wang J. et al. Microgrid Fault Analysis Method Based on Inverter-Type DG with Different Control // 2022 4th International Conference on Smart Power & Internet Energy Systems (SPIES), Beijing, China. 2022. Pp. 1397–1402. DOI: 10.1109/SPIES55999.2022.10082157.
29. Xu Y. et al. A Novel Distribution Network Fault Location Method Based on Improved Convolutional Neural Network // 2024 IEEE 7th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chongqing, China. 2024. Pp. 837–841. DOI: 10.1109/ITNEC60942.2024.10733085.
30. Conte F., D'Agostino F., Gabriele B., Schiapparelli G. -P. and Silvestro F. Fault Detection and Localization in Active Distribution Networks Using Optimally Placed Phasor Measurements Units // in IEEE Transactions on Power Systems. 2023. Vol. 38, no. 1. Pp. 714–727. DOI: 10.1109/TPWRS.2022.3165685.
31. Гурина Л. А. Оценка рисков кибербезопасности энергетического сообщества микросетей // Вопросы кибербезопасности. 2024. № 1(59). С. 101–107. DOI: 10.21681/2311-3456-2024-1-101-107.
32. Гурина Л. А., Томин Н. В. Интеллектуальные методы обеспечения кибербезопасности мультиагентных систем управления микросетями // Вопросы кибербезопасности. 2024. № 6(64). С. 53–64. DOI: 10.21681/2311-3456-2024-6-53-64.
33. Колосок И. Н., Гурина Л. А. Идентификация кибератак на системы SCADA и СМПР в ЭЭС при обработке измерений методами оценивания состояния // Электричество. 2021. № 6. С. 25–32. DOI: 10.24160/0013-5380-2021-6-25-32.
34. Opitz J. A Closer Look at Classification Evaluation Metrics and a Critical Reflection of Common Evaluation Practice // Transactions of the Association for Computational Linguistics. 2024. Vol. 12. Pp. 820–836. DOI: 10.1162/tacl_a_00675.
35. Hodson T. Root-mean-square error (RMSE) or mean absolute error (MAE): when to use them or not // Geoscientific Model Development. 2022. Vol. 15. Pp. 5481–5487. DOI: 10.5194/gmd-15-5481-2022.

ENSURING THE FUNCTIONALITY OF DIGITAL PROTECTION DEVICES IN THE EVENT OF CYBER-ATTACKS ON MICROGRIDS WITH DISTRIBUTED ENERGY RESOURCES

Gurina L. A.[3], Tomin N. V.[4]

Keywords: *active power distribution systems, protection schemes, cybersecurity, data verification, random processes, machine learning.*

The research aims *to develop method for method for verifying data used in digital systems for protection, automation and control of microgrids with distributed energy resources.*

The research relies *on the probabilistic methods, machine learning methods.*

Research result: *the information support of microgrids protection schemes is considered, possible cyber attacks are analyzed, the successful implementation of which may result in a violation of the functionality of digital protection devices of microgrids. A data verification method has been developed using unsupervised learning methods, including isolation forest and the k-nearest neighbors method, which effectively identifies and corrects measurement errors during attacks on the information infrastructure of microgrids protection systems under false data injection attacks.*

The scientific novelty *lies in the fact that an approach has been proposed that ensures the stability of microgrids protection systems during cyber attacks and, thereby, prevents false alarms and failures of protection devices.*

3 Liudmila A. Gurina, Ph.D. in engineering, Associate Professor, Senior Research Fellow, Laboratory for Control of Electric Power Systems at Melentiev Energy Systems Institute, SB RAS, Irkutsk, Russia. E-mail: gurina@isem.irk.ru
4 Nikita N. Tomin, Ph.D. in engineering, Head of Laboratory for Control of Electric Power Systems at Melentiev Energy Systems Institute, SB RAS, Irkutsk, Russia. E-mail: tomin.nv@gmail.com

References

1. Voropai, N. I. (2020). Prospects and Problems of Electric Power System Transformations. Elektrichestvo, 7, 12–21. DOI: 10.24160/0013-5380-2020-7-12-21.
2. Ilyushin, P. V. (2022). Integration of RES-based Power Plants into the Unified Energy System of Russia: Problematic Issues and Approaches to Solving Them. Bulletin of MPEI, 4, 98–107. DOI: 0.24160/1993-6982-2022-4-98-107.
3. Ilyushin, P., Filippov, S., Kulikov, A., Suslov, K., and Karamov, D. (2022). Intelligent Control of the Energy Storage System for Reliable Operation of Gas-Fired Reciprocating Engine Plants in Systems of Power Supply to Industrial Facilities. Energies, 15, 6333. DOI: 10.3390/en15176333.
4. Gurina, L. A. (2022). Pokazateli kiberustojchivosti komponentov informacionno-kommunikacionnoj infrastruktury pri upravlenii kiberfizicheskimi energeticheskimi sistemami // Methodological problems in reliability study of large energy systems, 73, 279–288.
5. Durakovsky, A. P., Markov, A. S. (2024). Current issues of cyber security in the energy sector. Secure Information Technologies, 94–98.
6. Shaukat, N. et al. (2023). Decentralized, Democratized, and Decarbonized Future Electric Power Distribution Grids: A Survey on the Paradigm Shift From the Conventional Power System to Micro Grid Structures. In IEEE Access, 11, 60957–60987. DOI: 10.1109/ACCESS.2023.3284031.
7. Lu, H., Biyawerwala, H. and Thakrawala, H. (2022). Polarized Distribution Protection Coordination Strategy Under the Impact from Various Distributed Energy Resources (DER) Generation Points. 2022 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), New Orleans, LA, USA, 1–5. DOI: 10.1109/TD43745.2022.9816925.
8. S. K. T, Jadoun V. K., J. N. S and S. S. (2024). A Systematic Study on the Intelligent Cyber Security for Smart Microgrid. 2024 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER), Mangalore, India, 237–242. DOI: 10.1109/DISCOVER62353.2024.10750634.
9. Canaan, B., Colicchio, B., Abdeslam, D. O. (2020). Microgrid Cyber-Security: Review and Challenges toward Resilience. Applied Sciences, 10, 16, 5649. DOI: 10.3390/app10165649.
10. Ding, D., Han, Q. -L., Ge, X. and Wang, J. (2021). Secure State Estimation and Control of Cyber-Physical Systems: A Survey. In IEEE Transactions on Systems, Man, and Cybernetics: Systems, 51, 1, 176-190. DOI: 10.1109/TSMC.2020.3041121.
11. Ilyushin, P. V., Volnyi, V. S. (2022). Review of methods for addressing challenging issues in the operation of protection devices in microgrids with voltage up to 1 kV that integrate distributed energy resources. Relay protection and automation, 4(49), 6–21.
12. Zheng, Dehua, Zhang, Wei, Netsanet, Solomon, Wang, Ping, Bitew Girmaw, Teshager, Wei, Dan, Yue, Jun. (2021). Key technical challenges in protection and control of microgrid. Microgrid Protection and Control, 45–56. DOI: 10.1016/B978-0-12-821189-2.00007-3.
13. Patnaik, B., Mishra, M., Bansal, R. C., Jena, R. K. (2020) AC microgrid protection – A review: Current and future prospective. Applied Energy, 271, 115210. DOI: 10.1016/J.APENERGY.2020.115210.
14. Abd el-Ghany, H. A. (2020). Optimal PMU allocation for high-sensitivity wide-area backup protection scheme of transmission lines. Electric Power Systems Research, 187, 106485. DOI: 10.1016/J.EPSR.2020.106485.
15. Kulikov, A., Loskutov, A., Bezdushniy, D. (2022). Relay Protection and Automation Algorithms of Electrical Networks Based on Simulation and Machine Learning Methods. Energies, 15(18), 6525. DOI: 10.3390/en15186525.
16. Shobole, A. A., Wadi, M. (2021). Multiagent systems application for the smart grid protection. Renewable and Sustainable Energy Reviews, 149, 111352. DOI: 10.1016/J.RSER.2021.111352.
17. Verma, R., Gawre, S. K., Patidar, N. P. (2022). An Analytical Review on Measures of Microgrid Protection. 2022 IEEE International Conference on Power Electronics, Drives and Energy Systems (PEDES), Jaipur, India, 1–6. DOI: 10.1109/PEDES56012.2022.10080291.
18. Cui, S., Zeng, P., Wang, Z., Song, C. (2021). Research on Intelligent Protection Technology for Distribution Network with Distributed Generation. 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, 1549–1554. DOI: 10.1109/IAEAC50856.2021.9390692.
19. Fawzy, N., Habib, H. F., Mohammed, O., Brahma, S. (2020). Protection of Microgrids with Distributed Generation based on Multiagent System // 2020 IEEE International Conference on Environment and Electrical Engineering and 2020 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe), Madrid, Spain, 1–5. DOI: 10.1109/EEEIC/ICPSEurope49358.2020.9160827.
20. Chaitanya, B. K., Anamika, Yadav. (2023). Empirical Wavelet Transform-Based Differential Protection Scheme for Micro-Grid. Journal of The Institution of Engineers (India): Series B, 104, 1–10. DOI: 10.1007/s40031-023-00869-0.
21. Uddin, M. N., Arifin, M. S., Rezaei, N. (2022). A Novel Neuro-Fuzzy Based Direct Power Control of a DFIG based Wind Farm Incorporated with Distance Protection Scheme and LVRT Capability. 2022 IEEE Industry Applications Society Annual Meeting (IAS), Detroit, MI, USA, 01–08. DOI: 10.1109/IAS54023.2022.9939684.
22. Chaitanya, B. K., Anamika, Yadav, Mohammad, Pazoki. (2020). High Impedance Fault Detection Scheme for Active Distribution Network Using Empirical Wavelet Transform and Support Vector Machine. 2020 15th International Conference on Protection and Automation of Power Systems (IPAPS), 149–152. DOI:10.1109/IPAPS52181.2020.9375620.
23. Shaik, M., Shaik, A. G., Yadav, S. K. (2022). Hilbert–Huang transform and decision tree based islanding and fault recognition in renewable energy penetrated distribution system. Sustainable Energy, Grids and Networks, 30, 100606. DOI: 10.1016/j.segan.2022.
24. Raad Salih, Jawad, Hafedh, Abid. (2023). HVDC Fault Detection and Classification with Artificial Neural Network Based on ACO-DWT Method. Energies, 16, 1064. DOI: 10.3390/en16031064.
25. Chandran, L. R., A. Parvathy, V S, I. K, Nair, M. G. (2022). Adaptive Over Current Relay Protection in a PV Penetrated Radial Distribution System With Fuzzy GA Optimisation. 2022 IEEE 19th India Council International Conference (INDICON), Kochi, India, 1–7. DOI: 10.1109/INDICON56171.2022.10040021.
26. Nasir, M., Bansal, R., Elnady, A. (2022). A Review of Various Neural Network Algorithms for Operation of AC Microgrids. 2022 Advances in Science and Engineering Technology International Conferences (ASET), Dubai, United Arab Emirates, 1–7. DOI: 10.1109/ASET53988.2022.9734899.
27. Vincent Nsed, Ogar, Sajjad, Hussain, Kelum A.A., Gamage (2023). The use of artificial neural network for low latency of fault detection and localisation in transmission line. Heliyon, 9, e13376. DOI: 10.1016/j.heliyon.2023.
28. Wang, J. et al. (2022). Microgrid Fault Analysis Method Based on Inverter-Type DG with Different Control. 2022 4th International Conference on Smart Power & Internet Energy Systems (SPIES), Beijing, China, 1397–1402. DOI: 10.1109/SPIES55999.2022.10082157.

29. Xu, Y. et al. (2024). A Novel Distribution Network Fault Location Method Based on Improved Convolutional Neural Network. 2024 IEEE 7th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chongqing, China, 837–841. DOI: 10.1109/ITNEC60942.2024.10733085.
30. Conte, F., D'Agostino, F., Gabriele, B., Schiapparelli, G. -P. and Silvestro, F. (2023). Fault Detection and Localization in Active Distribution Networks Using Optimally Placed Phasor Measurements Units. In IEEE Transactions on Power Systems, 38, 1, 714–727. DOI: 10.1109/TPWRS.2022.3165685.
31. Gurina, L. A. (2024). Assessment of cyber security risk of microgrids energy community. Cybersecurity issues, 1(59), 101–107. DOI: 10.21681/2311-3456-2024-1-101-107.
32. Gurina, L. A., Tomin, N. V. (2024). Intelligent methods of ensuring cybersecurity multi-agent control system of microgrid. Cybersecurity issues, 6(64), 53–64. DOI: 10.21681/2311-3456-2024-6-53-64.
33. Kolosok, I. N., Gurina, L. A. (2021). Identification of Cyberattacks on SCADA and WAMS Systems in Electric Power Systems when Processing Measurements by State Estimation Methods. Elektrichestvo, 6, 25–32. DOI: 10.24160/0013-5380-2021-6-25-32.
34. Opitz, J. (2024). A Closer Look at Classification Evaluation Metrics and a Critical Reflection of Common Evaluation Practice. Transactions of the Association for Computational Linguistics, 12, 820–836. DOI: 10.1162/tacl_a_00675.
35. Hodson, T. (2022). Root-mean-square error (RMSE) or mean absolute error (MAE): when to use them or not. Geoscientific Model Development, 15, 5481–5487. DOI: 10.5194/gmd-15-5481-2022.