РАЗРАБОТКА КОМПЛЕКСНОГО ПОДХОДА К ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ ВЗАИМОСВЯЗАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ПРИ ИНТЕЛЛЕКТУАЛЬНОМ УПРАВЛЕНИИ СООБЩЕСТВОМ МИКРОСЕТЕЙ[1]

Гурина Л.А.[2], Томин Н.В.[3]

Цель исследования: *разработка комплексного подхода к обеспечению кибербезопасности информационно-коммуникационной инфраструктуры энергетического сообщества.*

Методы исследования: *мультиагентное обучение с подкреплением, марковские процессы, вероятностные методы.*

Результат исследования: *рассмотрены способы формирования энергетических сообществ, проанализированы различные структуры управления такими сообществами, выявлены угрозы и уязвимости информационных систем, возможные отказы и сбои при кибератаках, которые могут привести к ошибкам при формировании управляющих воздействий. Разработан подход к обеспечению кибербезопасности взаимосвязанных информационных систем сообщества микросетей.*

Научная новизна *состоит в том, что для обеспечения кибербезопасности информационно-коммуникационной инфраструктуры при мультиагентном управлении энергетическим сообществом микросетей в работе предложен подход, методология которого заключается в моделировании энергетического сообщества, имитации кибератак, оценке последствий кибератак в разработке методов и средств защищенности взаимозависимых информационных систем от кибератак.*

Ключевые слова: *распределенная энергетика, энергетическое сообщество, микросеть, мультиагентное управление, риски кибербезопасности, модели кибератак.*

DOI:10.21681/2311-3456-2023-4-94-104

Введение

Агрегация микросетей в форме энергетического сообщества (например, группы удалённых поселков зон децентрализованного энергоснабжения, фермерские хозяйства, агрогородки, активные энергетические комплексы и т.п.) способствует эффективному использованию местных энергоресурсов между его участниками, сдерживанию роста тарифов на электроэнергию, а также повышению бесперебойности и надежности энергоснабжения потребителей [1-3].

Для реализации отмеченных преимуществ сообщество микросетей использует специальные цифровые автоматические системы управления, реализующие как функции оптимального управления доступными энергоисточниками, так и продвинутые рыночные функции торговли электроэнергии между субъектами сообщества. В этом отношении такое энергосообщество образует киберфизическую энергетическую систему (КФЭС) с внедрением, как правило, передовых информационных и коммуникационных технологий (искусственный интеллект, блокчейн, интернет вещей и пр.) для широкомасштабной многосторонней координации [4].

Общеизвестно, что технологическая часть КФЭС зависит от информационно-коммуникационной ин-

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

2 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

3 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

фраструктуры, как и функционирование информационно-коммуникационной инфраструктуры зависит от энергосистемы, т.е. системы взаимозависимы. Как правило, на энергосистему сильно влияют различные зависимости, существующие внутри самой системы, между энергосистемой и информационно-коммуникационной инфраструктурой, а также между энергосистемой и другими критически важными инфраструктурами или ее средой [5]. В [6] взаимозависимость определяется как «двунаправленная связь между двумя инфраструктурами, посредством которой состояние каждой инфраструктуры влияет или коррелирует с состоянием другой».

При формировании энергетических сообществ, а также при распределенном управлении объектами энергетики появляются взаимозависимости как между информационными системами микросетей, так и технологические взаимозависимости, которые вызывают новые потенциальные уязвимости, отказы по общей причине и другие взаимозависимые отказы, а также перебои в подаче электроэнергии. Взаимозависимости также подразумевают, что микросети более восприимчивы к кибератакам, даже если такие атаки не нацелены непосредственно на саму микросеть. Киберугрозы постоянно совершенствуются, и существует множество мер, которые можно предпринять, чтобы сделать информационные системы более защищенными. Однако многие из доступных мер лучше всего подходят для традиционных энергетических систем, но их может быть труднее применить к энергетическим сообществам, распределенные объекты которого тесно связаны между собой. Таким образом, в случае кибератак важно определить и проанализировать возможные сбои в взаимосвязанных информационных системах микросетей, чтобы обеспечить нормальное функционирование энергетического сообщества.

В связи с этим, для сообществ микросетей возникает комплексная задача сохранения свойств кибербезопасности информационных систем из-за роста используемых цифровых объектов, межсетевого взаимодействия, способствующих увеличению уязвимостей к кибератакам. Поэтому целью исследования является обеспечение кибербезопасности информационно-коммуникационной инфраструктуры сообществ микросетей, суть которого заключается в моделировании энергетического сообщества, имитации кибератак в разработке методов и средств защищенности взаимозависимых информационных систем от кибератак.

Структура управления сообществами микросетей

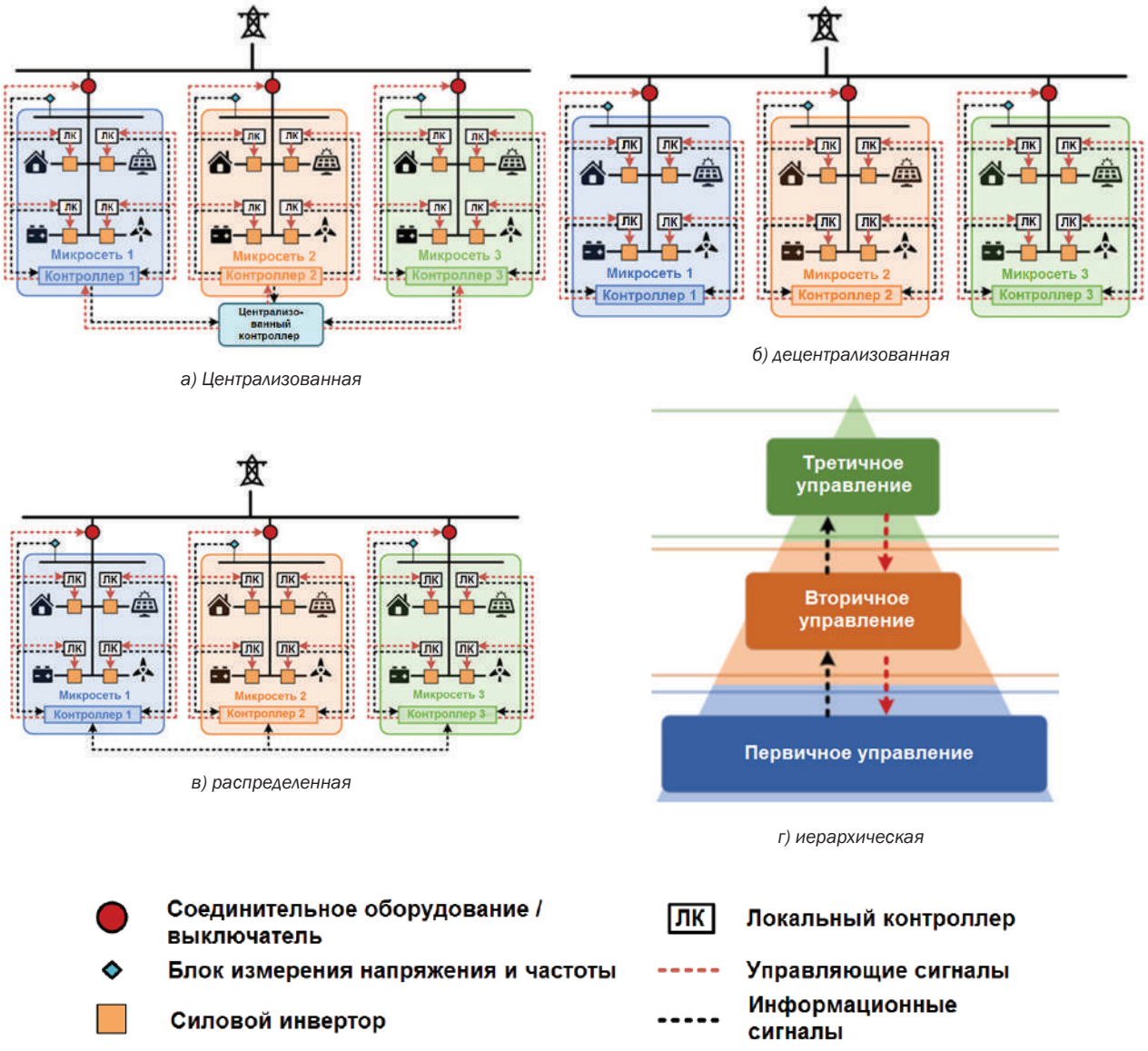
Управление сообществом микросетей включает в себя управление силовыми преобразователями, распределение активной/реактивной мощности между распределенными источниками генерации, управление уровнем заряда и зарядной/разрядной мощностью систем накопления энергии, синхронизацию нескольких микросетей, поддержание баланса напряжение-частота и генерация-нагрузка в микросетях и т.д. В [7] описаны принципы построения и режимы работы микросетей.

Управление микросетями фактически является многоцелевой задачей, охватывающей различные технические области, временные масштабы и физические уровни. Многоуровневое управление включает первичное управление, вторичное управление и третичное управление. На основе данной иерархии способ реализации уровней управления энергетическим сообществом может быть централизованным, децентрализованным, распределенным или иерархическим, как показано на рис. 1 [8].

В централизованной структуре существует центральный блок управления, который собирает и передает информацию на локальные источники генерации (рис. 1а). Децентрализованные и распределенные структуры не требуют центрального контроллера. Децентрализованное управление, как определено в [9], выполняет регулирование на основе локальных измерений, а распределенное управление основано как на локальном измерении, так и на соседней связи [10]. Иерархическая структура управления распределяет функции управления между локальными контроллерами и контроллерами верхнего уровня.

Централизованное управление требует сбора данных со всех основных компонентов микросети [11]. На основе собранной информации в контроллере могут выполняться процедуры мониторинга и управления для достижения правильной и эффективной работы. К преимуществам централизованного управления относятся высокая наблюдаемость и управляемость всем сообществом, а также простота реализации. Однако это влечет за собой проблему единой точки отказа, а выход из строя центрального контроллера приведет к потере всех функций [12].

Децентрализованное управление микросетью относится к методам управления, не требующим информации от других частей системы. Контроллер регулирует соответствующий блок, используя только локальную информацию. Преимущество децентрализованных схем в том, что они не требуют связи в режиме ре-



а) Централизованная

б) децентрализованная

в) распределенная

г) иерархическая

Рис. 1. Структуры управления энергетическим сообществом микросетей (адаптировано из [8])

ального времени, хотя отсутствие координации между местными регулирующими органами ограничивает возможность достижения глобального скоординированного поведения.

Функции, обеспечиваемые схемой централизованного управления, также могут быть реализованы распределенным способом, как показано на рис.1в. Между контроллерами осуществляется передача информации через линии связи, так что необходимая информация распределяется между каждой локальной системой, чтобы облегчить скоординированное поведение всех блоков. Основной проблемой полностью распределенной схемы управления является координация между распределенными блоками для выполнения целей управления. Обмен информацией между микросетями в составе энергосообщества позволяет контроллерам найти оптимальную стратегию работы для устойчивой и эффективной работы сообщества.

Распределенное вторичное управление, как новая стратегия управления, выполняет все функции централизованного контроллера с меньшими затратами на связь и вычисления, будучи устойчивым к сбоям к неизвестным системным параметрам. Идея состоит объединении первичных и вторичных элементов управления в один локальный контроллер. В отличие от децентрализованного первичного управления, для правильной работы встроенные вторичные контроллеры должны «общаться» со своими соседями. Каж-

дый агент (т. е. преобразователи, например, AC/DC инверторы) обменивается информацией с другими агентами в коммуникационной среде. Каждый локальный вторичный контроллер принимает решение в соответствии с информацией своих соседей [13].

Таким образом, для обеспечения кибербезопасности энергетического сообщества при централизованном и распределенном управлении следует учитывать взаимозависимости не только информационно-коммуникационных и физических подсистем, но и взаимозависимости информационных систем микросетей в составе сообщества.

Угрозы и уязвимости, обусловливающие возникновение рисков кибербезопасности сообщества микросетей

А. Уязвимости микросетей

Хотя интеграция киберсистем с технологической частью КФЭС дает преимущества, она также создает новый набор уязвимостей, которые могут подвергать систему различным угрозам. Эксплуатация таких кибер-уязвимостей может привести к сбоям и отказам в технологической части КФЭС. Микросеть, будучи КФЭС, наследует их общие киберуязвимости, добавленные к уязвимостям, обусловленным спецификой распределенной энергетики. Причинами появления уязвимостей могут являться:

1. Использование беспроводной связи. Риск таких атак, как перехват и вторжение, выше, чем в проводных сетях.

2. Использование гетерогенных коммуникационных технологий. Предполагается, что управление современными энергосистемами осуществляется посредством связи с использованием различных технологий. Сосуществование различных проводных или беспроводных технологий усложняет реализацию надежной и единой политики кибербезопасности для защиты коммуникационной инфраструктуры.

3. Увеличение подверженности внешним сетям. Микросети должны постоянно обмениваться данными с операторами основной сети и другими микросетями в составе энергетического сообщества с целью повышения общей производительности и гибкости основной сети и обеспечения безопасности ее операций. Такая связь с другими внешними сетями подвергает систему дополнительным внешним угрозам.

4. Воздействие Интернета. Микросети подвержены многочисленным атакам, проводимыми через Интернет.

5. Увеличение автоматизации системы. Обычно автоматизированное управление предназначено для повышения гибкости и эффективности работы системы за счет устранения возможности человеческой ошибки. Однако это порождает новые уязвимости, поскольку становится больше точек доступа к системе, и, следовательно, увеличивается риск атак.

6. Увеличение использования распределенных устройств управления и автоматизации. Сложное распределенное управление гибких активов и спроса в рамках микросетей обеспечивает их устойчивость. Вместе с тем, возросшее проникновение возможностей мониторинга и управления открывает возможности для нарушений безопасности.

7. Сосуществование между унаследованными и новыми системами. Поскольку распределительная сеть представляет собой общую инфраструктуру, используемую различными операторами, ожидается, что контроллер микросети будет постоянно контактировать с этими операторами для улучшения функционирования всей сети, что также создает новые уязвимости.

8. Использование нескольких независимых систем. Энергетические системы и, в частности, микросети состоят из таких устройств, как датчики, исполнительные механизмы, компьютеры, платежные системы, аварийные системы и т. д. Крайне важно, но сложно обеспечить плавное взаимодействие, связь и безопасность между такими независимыми и разнородными системами [14].

Таким образом, микросети могут быть подвержены различным киберугрозам.

Б. Возможные кибератаки на микросети

Основной целью кибератак обычно являются объекты управления и мониторинга [15]. Злоумышленники могут использовать уязвимости во всех активах, чтобы получить доступ к различным уровням управления и повлиять на функционирование сообщества микросетей, тем самым, обусловить возникновение рисков кибербезопасности.

Существуют различные типы кибератак на информационные системы, которые могут быть реализованы и для сообщества микросетей:

- Манипуляции с аппаратными средствами и программным обеспечением;
- Вредоносное программное обеспечение;
- Атаки внедрения ложных данных (FDI-атака);
- Атаки отказа в обслуживании (DoS-атака);
- Атаки захвата (Hijacking-атака) и т.д. [16, 17].

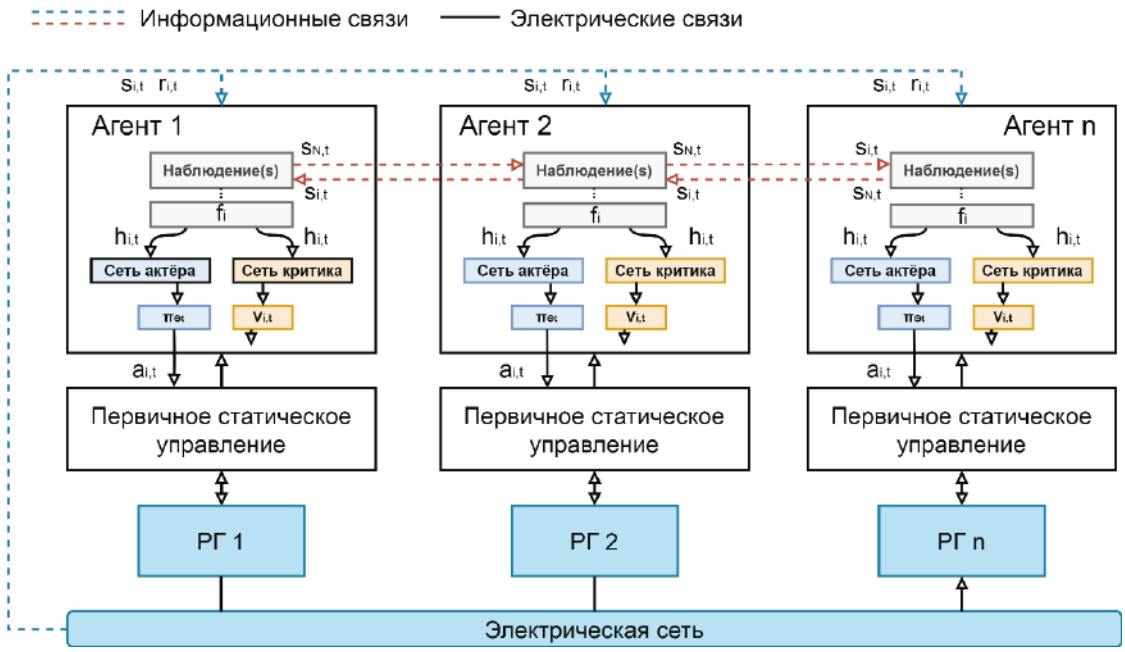


Рис. 2. Общая схема подхода к мультиагентному статическому регулированию напряжения через инверторы (адаптировано из [20])

FDI-атака может повлиять на целостность информации, DoS-атаки прервут доступ к передаваемым данным, атаки захвата позволят нарушить управление и «захватить» контроллеры распределенной системы управления [17]. При этом атака захвата контроллера разрывает канал связи и искажает данные, следовательно, прерывает процесс обновления полученного сигнала. В [18] показано, что атаки захвата контроллера могут снижать оптимальную производительность микросетей. Поскольку при таких атаках измерение с меткой времени заменяется постоянным вводом, алгоритм линейного консенсуса не может обновить свое эталонное состояние по отношению к соседним агентам, что, в конечном итоге, приводит к неизбежному небалансу мощности.

В этой связи предлагается подход к обеспечению кибербезопасности взаимосвязанных информационных систем микросетей, который заключается в следующем:

1. Моделирование энергетического сообщества микросетей.

2. Моделирование кибератак, оценка распространения и влияния их последствий на взаимосвязанные информационные системы микросетей в составе энергетического сообщества.

3. Разработка возможных мер, обеспечивающих защищенность информационных систем микросетей от кибератак.

Осведомленность о кибератаках и выявление их причин позволяет лучше оценить влияние сбоев на взаимосвязанные распределенные объекты. В [19] качестве возможной меры по защите взаимозависимых информационных систем от кибератак предложено объединение микросетей в коалиции, что позволит эффективнее использовать имеющиеся ресурсы для обеспечения кибербезопасности.

Мультиагентная система распределенного вторичного управления напряжением

В данной работе для реализации распределенного вторичного управления напряжением в сообществе микросетей была использована мультиагентная система управления, разработанная в [20] (рис. 2).

В этом подходе электрическая сеть рассматривается как мультиагентная $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, где каждый агент $i \in \mathcal{V}$ взаимодействует со своими соседями $N_i: \{j | \varepsilon_{ij} \in \mathcal{E}\}$. Под агентом здесь понимается контроллер вторичного управления DC/AC инвертором, используемый для подключения к сети переменного тока источников распределённой генерации (РГ) на постоянном токе, например, солнечные фотоэлектрические преобразователи, аккумуляторные батареи.

В представленной структуре в процессе обучения агент «изучает» стратегию управления, основанную на суб-глобальном вознаграждении, а также локальные состояния и закодированные коммуникационные сообщения от его соседей (других агентов). Поскольку каждый агент i в этой модели наблюдает только за частью среды (своё состояние и своих соседей), это приводит к частично марковскому процессу принятия

решений. Эта задача решается методом мультиагентного обучения с подкреплением, для которого определены следующие ключевые элементы:

— *Область действий:* управляющее действие для каждого агента — это уставка вторичного управления напряжением V_n. Были использованы 10 дискретных действий, равномерно распределенных между 1,02 и 1,12 о.е.

— *Пространство состояний*: состояние каждого агента i выбирается как $s_t = (\delta_i, P_i, Q_i, i_{odi}, i_{oqi}, i_{bdi}, i_{bqi}, v_{bdi}, v_{bqi})$ для характеристики режимов CIGs, где δ_i — измеренный опорный угол; P_i, Q_i – активная и реактивная мощности соответственно; $i_{odi}, i_{oqi}, i_{bdi}, i_{bqi}$ – выходные токи d-q CIG i и напрямую подключенные шины, соответственно; а v_{bdi}, v_{bqi} — выходные напряжения d-q подключенной шины соответственно.

— *Пространство наблюдений*: предполагается, что каждый агент может наблюдать только свое локальное состояние, а также сообщения от своих соседей, т.е. $o_{i,t} = S_{i,t} \cup m_{i,t}$, где $m_{i,t}$-коммуникационное сообщение, полученное от соседних агентов $j \in \mathcal{N}_i$, которое подробнее будет рассмотрено далее.

— *Функция вознаграждения*: целью всех агентов является максимизация общего вознаграждения $R_{i,t} = \sum_{k=o}^{T} \gamma^k \sum_{j \in v} \alpha(d_{i,j}) r_{i,t+k}$, где $\alpha(d_{i,j}) \in [0,1]$- пространственная функция дисконтирования; $d_{i,j}$ - расстояние между агентом i и j; $r_{i,t}$ – вознаграждение агента i на временном шаге t. Функция $r_{i,t}$ определяется следующим образом, для того чтобы напряжения в генераторных узлах быстро сходились к эталонным значениям (например, 1 о.е.):

$$r_{i,t} = \begin{cases} 0.05 - |1 - v_i|, \\ -|1 - v_i|, \\ -10. \end{cases} \quad (1)$$

$$v_i \in |0.95,1.05|,$$
$$v_i \in |0.8,0.95| \cup |1.05,1.25|$$
$$Otherwise$$

где $r_{i,t}$ — вознаграждение агента i на временном шаге t. Фактически, мы разделяем диапазон напряжений на 3 рабочие зоны: зона нормального режима ($|0.95,1.05|$ о.е.), зона утяжелённого режима $|0.8,0.95| \cup |1.05,1.25|$ о.е.) и аварийная зона ($|0, 0.8| \cup |1.25, \infty|$ о.е.). При сформулированном вознаграждении агент с «аварийными» напряжениями получат большой штраф, а агент с напряжением, близким к 1 о.е., получат положительное вознаграждение.

В рассматриваемой мультиагентной структуре информация от соседних агентов используется для повышения эффективности обучения. Таким образом, на основе структуры, предложенной в [20], агент *i* обновляет свое скрытое состояние $h_{i,t}$, на каждом шаге t

$$h_{i,t} = f_i\left(h_{i,t-1}, q_0\left(e_s(o_{i,t})\right), q_h(h_{\mathcal{N},t-1})\right) \quad (2)$$

где $h_{i,t-1}$ — скрытое состояние с предыдущего временного шага; $o_{i,t}$ — наблюдение агента *i,* сделанное в момент времени *t*, т.е. его внутреннее состояние и состояния его соседей; $h_{\mathcal{N},t-1}$ — интегрированное состояние от соседей; $e_S(o_{i,t})$ и q_h — дифференцируемые функции кодирования и извлечения сообщений. Вместо низкоразмерных индикаторов, здесь включены полные состояния соседнего агента в локальное наблюдение $o_{i,t} = s_{i,t} \cup s_{N,t}$ для улучшения наблюдаемости агента. При этом полученное коммуникационное сообщение $m_{i,t}$, *i*-го агента является комбинацией внутренних состояний и скрытых состояний его соседей.

Важно заметить, что в данной реализации мультиагентной системы скрытое состояние $h_{i,t}$, полученное из (2), используется затем в актёр-критических нейросетях для генерации случайных действий и прогнозирования функций ценности, соответственно, то есть $\pi_{\theta_i}(\cdot|h_{i,t})$ и $V_{\omega_i}(h_{i,t})$ (рис. 2). При этом используется централизованная схема обучения агентов с децентрализованным исполнением, где каждый агент имеет свои собственные актёр-критические нейросети, и их стратегия обновляется независимо, а не на основе алгоритмов консенсуса [21], который может снизить скорость сходимости решения. Такой подход позволяет создавать устойчивые системы интеллектуального управления к информационным сбоям, в том числе по причине кибератак на мультиагентные системы.

В следующем примере на базе вышеописанной мультиагентной системы вторичного управления напряжением в сообществе микросетей было исследовано влияние кибератак на агенты с поврежденными данными и влияние кибератак на соседние агенты.

Пример

Рассмотрим несколько сценариев, в которых злоумышленник искажает данные, например, текущие данные, которыми обмениваются агенты, вводя ложные данные в каналы связи или беспроводные каналы связи. Прежде всего рассмотрим FDI-атаку на

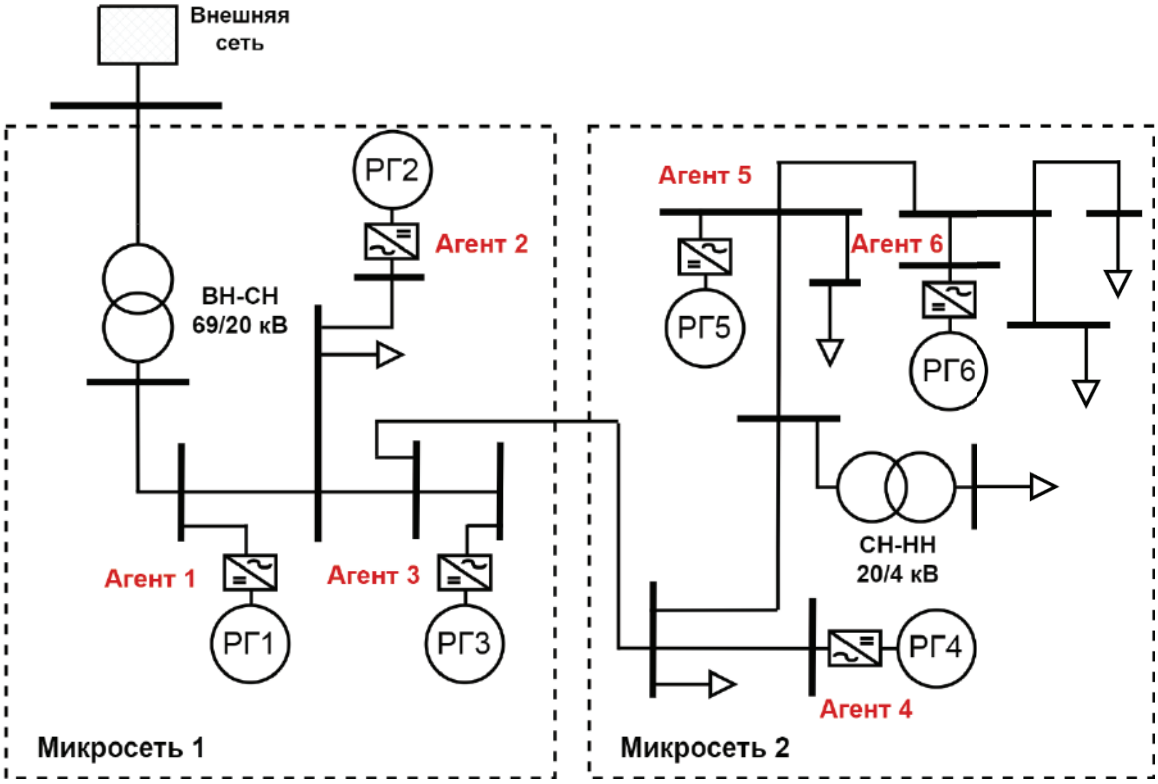


Рис. 3. Тестовая схема сообщества микросетей

нескольких агентов. Эта атака изменяет измеренную информацию от соседних агентов, добавляя ложные данные [17]. Фактическое текущее измерение (наблюдение) $o_{i,t} = S_{i,t} \cup m_{i,t}$ соседних агентов при этой атаке представлено как

$$o_{i,t}^{a} = o_{i,t} - \alpha x_{i,t}^{a} \quad (3)$$

где $x_{i,t}^{a}$ –ложные данные, заданные в виде случайного распределения в определённом диапазоне, $\alpha \in \{0, 1\}$ – коэффициент искажения данных, где $\alpha = 1$ означает FDI-атаку.

Также рассмотрим более тяжёлый вариант кибератаки, связанный с захватом контроллера. В случае такой атаки злоумышленник заменяет правильные данные вредоносными данными. Это может быть смоделировано следующим образом [22]:

$$o_{i,t}^{c} = (1 - \alpha) o_{i,t} - \alpha x_{i,t}^{a} \quad (4)$$

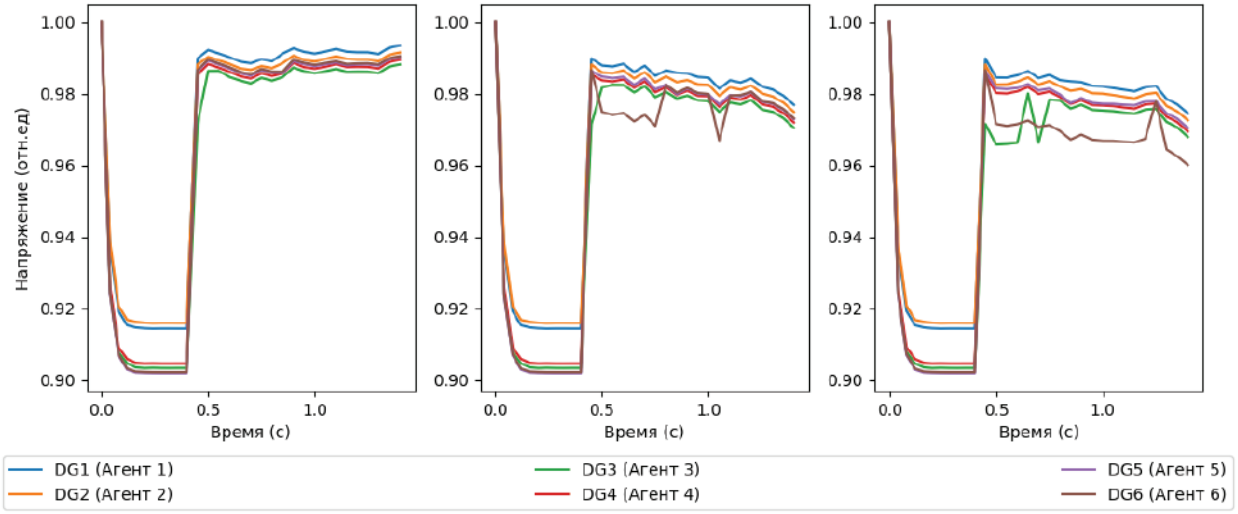
где $o_{i,t}^{c}$ – модифицированное наблюдение агента; $x_{i,t}^{a}$ – ложные данные, заданные в виде случайного распределения в определённом диапазоне, и $\alpha = 1$ означает атаку на инвертер с полной заменой корректных наблюдений.

В качестве тестирования мультиагентной системы с моделируемыми кибератаками, по аналогии с [22], была рассмотрена модель сообщества микросетей с распределенными источниками электроэнергии, полученная на основе модификации схемы IEEE 34 (рис. 3).

Для моделирования утяжелённых режимов, были добавлены случайные изменения нагрузки по всей сети с отклонениями ± 20% от номинальных значений, а также случайные возмущения в диапазоне ±5% для каждой нагрузки. Все агенты в рассматриваемых схемах контролировались со временем выборки 0,05 с, и каждый агент мог связываться со своими соседями через локальные границы связи. Первичное управление нижнего уровня реализовано по аналогии с [23].

Для схемы, показанной на рис. 3, рассматривались FDI-атака и атака захвата контроллеров на агенты 3, 5 и 6, согласно (3) и (4). На рис. 4. представлены результаты такого моделирования, где показано качество стабилизации напряжения после возмущения по нагрузке для различных сценариев.

Хорошо видно, что в отсутствие кибератак агенты-инверторы эффективно справляются с задачей согласованной стабилизации напряжения после возмущения (рис. 4а). Однако, при FDI-атаке и Hijacking-атаке на информационные системы, качество регулирования напряжения ухудшается (рис. 4б, 4в), особенно в плане регулирования напряжения инвертором рас-



а) Кибератаки отсутствуют *б) FDI-атака* *в) Атака захвата контроллеров*

Рис. 4. Результаты моделирования поведения агентов обученной системы регулирования напряжения при возмущении нагрузки при наличии и отсутствии кибератак

пределенного генератора №6 (агент 6). В случае атаки захвата контроллера последствия более критичные в отношении стабилизации профилей напряжения в генерирующих узлах.

Выводы

Рассмотрены различные структуры управления сообществами микросетей. Показано, что при централизованном и распределенном управлении сообществами микросетей число уязвимостей к кибератакам возрастает за счет взаимозависимости информационных систем. Предложен подход по обеспечению кибербезопасности информационно-коммуникационной инфраструктуры энергетического сообщества, позволяющий при моделировании кибератак на информационные системы микросетей провести анализ их распространения, оценить последствия для интеллектуального управления и, в дальнейшем, разработать меры защищенности взаимозависимых информационных систем от кибератак.

Литература

1. Gjorgievski V.Z., Cundeva S., Georghiou G.E.. Social arrangements, technical designs and impacts of energy communities: A review // Renewable Energy. 2021, vol. 169, pp. 1138-1156. DOI: 10.1016/j.renene.2021.01.078.
2. Warneryd M., Hakansson M., Karltorp K. Unpacking the complexity of community microgrids: A review of institutions' roles for development of microgrids // Renewable and Sustainable Energy Reviews. 2020, 121, 109690, DOI: 10.1016/j.rser.2019.109690.
3. Н. В. Томин, В. А. Шакиров, В. Г. Курбацкий, Д. Н. Сидоров, Д. А. Корев. Энергетические сообщества с возобновляемыми источниками энергии: эффективное планирование и управление в условиях многокритериальности. Часть 1 // Электроэнергия: передача и распределение. 2023, № 3(78), с. 18-27.
4. The Microgrid Case Studies: Community Resilience for Natural Disasters, 2020 https://sepapower.org/resource/the-microgrid-case-studies-community-resilience-for-natural-disasters/
5. Воропай Н.И. Направления и проблемы трансформации электроэнергетических систем // Электричество. 2020, №7, с. 12-21. DOI:10.24160/00135380202071221
6. Xiaojie Xu, Xiuwen Fu. Analysis on Cascading Failures of Directed–Undirected Interdependent Networks with Different Coupling Patterns // Entropy. 2023, vol. 25, no.3, 471. DOI: 10.3390/e25030471.
7. Илюшин П.В., Вольный В.С. Обзор структур микросетей низкого напряжения с распределенными источниками энергии // Релейная защита и автоматизация. 2023, № 1(50), с. 68-80.

8. Diptish Saha, Najmeh Bazmohammadi, Juan C. Vasquez, Josep M. Guerrero. Multiple Microgrids: A Review of Architectures and Operation and Control Strategies // Energies. 2023, 16(2), 600. DOI: 10.3390/en16020600.
9. Rabeb Ben Amor, Salwa Elloumi. Decentralized Control Approaches of Large-Scale Interconnected Systems // Advances in Science, Technology and Engineering Systems Journal. 2018, 3(1), pp. 394-403. DOI: 10.25046/aj030148.
10. A. H. El-Ebiary, M. Mokhtar, M. A. Attia and M. I. Marei. A Distributed Adaptive Control Strategy for Meshed DC Microgrids. 2023 IEEE Conference on Power Electronics and Renewable Energy (CPERE), Luxor, Egypt. 2023, pp. 1-6, doi: 10.1109/CPERE56564.2023.10119627.
11. P. Kant, P. Singhal, M. K. Mahto and D. Jain. Control strategies for DC Microgrids: An overview. 2022 2nd International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC), Mathura, India. 2022, pp. 1-6, doi: 10.1109/PARC52418.2022.9726636.
12. Y. Wang, A. O. Rousis and G. Strbac. On microgrids and resilience: A comprehensive review on modeling and operational strategies // Renewable and Sustainable Energy Reviews. 2020, vol. 134. DOI: 10.1016/j.rser.2020.110313.
13. X. Zhang, M. Dong and J. Ou. A distributed cooperative control strategy based on consensus algorithm in DC microgrid. 2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA), Wuhan, China. 2018, pp. 243-248. DOI: 10.1109/ICIEA.2018.8397722.
14. M. Rekik, Z. Chtourou, C. Gransart and A. Atieh. A Cyber-Physical Threat Analysis for Microgrids. 2018 15th International Multi-Conference on Systems, Signals & Devices (SSD), Yasmine Hammamet, Tunisia. 2018, pp. 731-737. DOI: 10.1109/SSD.2018.8570411.
15. Колосок И.Н., Гурина Л.А. Оценка рисков управления киберфизической ЭЭС на основе теории нечетких множеств. Методические вопросы исследования надежности больших систем энергетики. В 2-х книгах. 2019, с. 238-247.
16. Колосок И.Н., Гурина Л.А. Оценка показателей киберустойчивости систем сбора и обработки информации в ЭЭС на основе полумарковских моделей. Вопросы кибербезопасности. 2021, №6(46), с. 2-11. DOI: 10.21681/2311-3456-2021-6-2-11.
17. Abhinav, H. Modares, F. L. Lewis, F. Ferrese, and A. Davoudi. Synchrony in networked microgrids under attacks // IEEE Trans. Smart Grid, vol. 9, no. 6, pp. 6731–6741, 2018.
18. K. Gupta, S. Sahoo, R. Mohanty, B. K. Panigrahi and F. Blaabjerg. Decentralized Anomaly Identification in Cyber-Physical DC Microgrids. 2022 IEEE Energy Conversion Congress and Exposition (ECCE), Detroit, MI, USA. 2022, pp. 1-6. DOI: 10.1109/ECCE50734.2022.9947581.
19. Гурина Л.А., Айзенберг Н.И. Поиск эффективого решения по обеспечению защиты от киберугроз сообщества микросетей со взаимосвязанными информационными системами // Вопросы кибербезопасности. 2023, № 3.
20. Tomin N., Voropai N., Kurbatsky V., Rehtanz C. Management of Voltage Flexibility from Inverter-Based Distributed Generation Using Multi-Agent Reinforcement Learning // Energies. 2021, 14, 8270. DOI: 10.3390/en14248270.
21. Zhang, K.; Yang, Z.; Liu, H.; Zhang, T.; Basar, T. Fully decentralized multi-agent reinforcement learning with networked agents. arXiv 2018, arXiv:1802.08757.
22. S. Sahoo, J. C. H. Peng, S. Mishra, and T. Dragicevic. Distributed Screening of Hijacking Attacks in DC Microgrids // IEEE Trans. Power Electron. 2020, vol. 35, no. 7, pp. 7574–7582. 2020. DOI: 10.1109/TPEL.2019.2957071.
23. S. Mo, W. -H. Chen and X. Lu. Distributed hybrid secondary control strategy for DC microgrid group based on multi-agent system. 2021 33rd Chinese Control and Decision Conference (CCDC), Kunming, China. 2021, pp. 109-114. DOI: 10.1109/CCDC52312.2021.9602249.

DEVELOPMENT OF AN INTEGRATED APPROACH TO ENSURING THE CYBER SECURITY OF INTERCONNECTED INFORMATION SYSTEMS UNDER INTELLIGENT MANAGEMENT OF A MICROGRID COMMUNITY[4]

Gurina L.A[5], Tomin N.V.[6]

The research aims *to develop approach to ensure the cybersecurity of the information and communication infrastructure of the energy community.*

4 The research was conducted within the framework of the scientific project «Theoretical foundations, models and methods to control the expansion and operation of intelligent electric power systems (Smart Grids)», No. FWEU-2021-0001.

5 Ludmila A. Gurina, Ph.D., Associate Professor, Senior Research Fellow, L.A. Melentyev Institute of Energy Systems SB RAS, Irkutsk, Russia. E-mail: gurina@isem.irk.ru

6 Nikita N. Tomin, Ph.D. in engineering, Head of Laboratory for Control of Electric Power Systems at Melentyev Institute of Energy Power Systems, SB RAS, Irkutsk, Russia. E-mail: tomin.nv@gmail.com

The research relies *on the multi-agent reinforcement learning, Markov processes, probabilistic methods.*

Research result: *Potential threats and vulnerabilities of the information and communication infrastructure of the microgrid community are analyzed. A proposed model of microgrid coalitions take into account such factors as cybersecurity risks, the mutual influence of available microgrid resources to protect against cyber-attacks, and the mutual influence of the consequences of cyber threats. The developed method determines the effectiveness of protection against cyber threats with and without coalitions for the microgrid community.*

Research result: *ways of forming energy communities are considered, various structures for managing such communities are analyzed, threats and vulnerabilities of information systems, possible failures and faults during cyber-attacks that can lead to errors in the formation of control actions are identified. An approach has been developed to ensure the cybersecurity of interconnected information systems of the microgrid community.*

The scientific novelty lies in the *fact that in order to ensure the cybersecurity of information and communication infrastructure with multi-agent management of the energy community of microgrids, an approach is proposed, the methodology of which is to model the energy community, simulate cyber-attacks, assess the consequences of cyber-attacks and develop methods and means of protecting interdependent information systems from cyber-attacks.*

Keywords: *distributed energy, energy community, microgrid, multi-agent management, cybersecurity risks, cyber-attack models.*

References

1. Gjorgievski V.Z., Cundeva S., Georghiou G.E.. Social arrangements, technical designs and impacts of energy communities: A review // Renewable Energy. 2021, vol. 169, pp. 1138-1156. DOI: 10.1016/j.renene.2021.01.078.
2. Warneryd M., Hakansson M., Karltorp K. Unpacking the complexity of community microgrids: A review of institutions' roles for development of microgrids // Renewable and Sustainable Energy Reviews. 2020, 121, 109690, DOI: 10.1016/j.rser.2019.109690.
3. N. V. Tomin, V. A. SHakirov, V. G. Kurbackij, D. N. Sidorov, D. A. Korev. Energeticheskie soobshchestva s vozobnovlyaemymi istochnikami energii: effektivnoe planirovanie i upravlenie v usloviyah mnogokriterial'nosti. CHast' 1 // Elektroenergiya: peredacha i raspredelenie [Electricity: transmission and distribution]. 2023, № 3(78), c. 18-27.
4. The Microgrid Case Studies: Community Resilience for Natural Disasters, 2020 https://sepapower.org/resource/the-microgrid-case-studies-community-resilience-for-natural-disasters/
5. Voropaj N.I. Napravleniya i problemy transformacii elektroenergeticheskih sistem // Elektrichestvo [Elektrichestvo]. 2020, №7, s. 12-21. DOI:10.24160/00135380202071221.
6. Xiaojie Xu, Xiuwen Fu. Analysis on Cascading Failures of Directed–Undirected Interdependent Networks with Different Coupling Patterns // Entropy. 2023, vol. 25, no.3, 471. DOI: 10.3390/e25030471.
7. Ilyushin P.V., Vol'nyj V.S. Obzor struktur mikrosetej nizkogo napryazheniya s raspredelennymi istochnikami energii // Relejnaya zashchita i avtomatizaciya [Relay protection and automation]. 2023, № 1(50), s. 68-80.
8. Diptish Saha, Najmeh Bazmohammadi, Juan C. Vasquez, Josep M. Guerrero. Multiple Microgrids: A Review of Architectures and Operation and Control Strategies // Energies. 2023, 16(2), 600. DOI: 10.3390/en16020600.
9. Rabeb Ben Amor, Salwa Elloumi. Decentralized Control Approaches of Large-Scale Interconnected Systems // Advances in Science, Technology and Engineering Systems Journal. 2018, 3(1), pp. 394-403. DOI: 10.25046/aj030148.
10. A. H. El-Ebiary, M. Mokhtar, M. A. Attia and M. I. Marei. A Distributed Adaptive Control Strategy for Meshed DC Microgrids. 2023 IEEE Conference on Power Electronics and Renewable Energy (CPERE), Luxor, Egypt. 2023, pp. 1-6, doi: 10.1109/CPERE56564.2023.10119627.
11. P. Kant, P. Singhal, M. K. Mahto and D. Jain. Control strategies for DC Microgrids: An overview. 2022 2nd International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC), Mathura, India. 2022, pp. 1-6, doi: 10.1109/PARC52418.2022.9726636.
12. Y. Wang, A. O. Rousis and G. Strbac. On microgrids and resilience: A comprehensive review on modeling and operational strategies // Renewable and Sustainable Energy Reviews. 2020, vol. 134. DOI: 10.1016/j.rser.2020.110313.
13. X. Zhang, M. Dong and J. Ou. A distributed cooperative control strategy based on consensus algorithm in DC microgrid. 2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA), Wuhan, China. 2018, pp. 243-248. DOI: 10.1109/ICIEA.2018.8397722.
14. M. Rekik, Z. Chtourou, C. Gransart and A. Atieh. A Cyber-Physical Threat Analysis for Microgrids. 2018 15th International Multi-Conference on Systems, Signals & Devices (SSD), Yasmine Hammamet, Tunisia. 2018, pp. 731-737. DOI: 10.1109/SSD.2018.8570411.
15. Kolosok I.N., Gurina L.A. Ocenka riskov upravleniya kiberfizicheskoj EES na osnove teorii nechetkih mnozhestv. Metodicheskie voprosy issledovaniya nadezhnosti bol'shih sistem energetiki [Methodological issues in the study of the reliability of large energy systems]. V 2-h knigah. 2019, s. 238-247.

16. Kolosok I.N., Gurina L.A. Otsenka pokazatelei kiberustoichivosti sistem sbora i obrabotki informatsii v EES na osnove polumarkovskikh modelei // Voprosy kiberbezopasnosti [Cybersecurity issues]. 2021, №6. S. 2-11. DOI: 10.21681/2311-3456-2021-6-2-11.
17. Abhinav, H. Modares, F. L. Lewis, F. Ferrese, and A. Davoudi. Synchrony in networked microgrids under attacks // IEEE Trans. Smart Grid, vol. 9, no. 6, pp. 6731–6741, 2018.
18. K. Gupta, S. Sahoo, R. Mohanty, B. K. Panigrahi and F. Blaabjerg. Decentralized Anomaly Identification in Cyber-Physical DC Microgrids. 2022 IEEE Energy Conversion Congress and Exposition (ECCE), Detroit, MI, USA. 2022, pp. 1-6. DOI: 10.1109/ECCE50734.2022.9947581.
19. Gurina L.A., Ajzenberg N.I. Poisk effektivogo resheniya po obespecheniyu zashchity ot kiberugroz soobshchestva mikrosetej so vzaimosvyazannymi informacionnymi sistemami // Voprosy kiberbezopasnosti [Cybersecurity issues]. 2023, № 3.
20. Tomin N., Voropai N., Kurbatsky V., Rehtanz C. Management of Voltage Flexibility from Inverter-Based Distributed Generation Using Multi-Agent Reinforcement Learning // Energies. 2021, 14, 8270. DOI: 10.3390/en14248270.
21. Zhang, K.; Yang, Z.; Liu, H.; Zhang, T.; Basar, T. Fully decentralized multi-agent reinforcement learning with networked agents. arXiv 2018, arXiv:1802.08757.
22. S. Sahoo, J. C. H. Peng, S. Mishra, and T. Dragicevic. Distributed Screening of Hijacking Attacks in DC Microgrids // IEEE Trans. Power Electron. 2020, vol. 35, no. 7, pp. 7574–7582. 2020. DOI: 10.1109/TPEL.2019.2957071.
23. S. Mo, W. -H. Chen and X. Lu. Distributed hybrid secondary control strategy for DC microgrid group based on multi-agent system. 2021 33rd Chinese Control and Decision Conference (CCDC), Kunming, China. 2021, pp. 109-114. DOI: 10.1109/CCDC52312.2021.9602249.