ОЦЕНКА РИСКОВ КИБЕРБЕЗОПАСНОСТИ ЭНЕРГЕТИЧЕСКОГО СООБЩЕСТВА МИКРОСЕТЕЙ[1]

Гурина Л. А.[2],

DOI: 10.21681/2311-3456-2024-1-101-107

Цель исследования: *разработка методического подхода оценки риска кибербезопасности микросетей со взаимосвязанными информационными системами.*

Методы исследования: *марковские процессы, вероятностные методы, методы теории нечетких множеств.*

Результат исследования: *рассмотрена иерархическая структура управления энергетическим сообществом, выявлены возможные кибератаки на систему управления сообществом микросетей, приведена классификация кибератак, последствием которых является нарушение качество информации. Предложена модель состояний информационной системы микросети, на основе которой получена структурная модели развития состояний энергетического сообщества при различных способах управления. Разработан подход оценки риска кибербезопасности информационно-коммуникационной инфраструктуры сообщества микросетей.*

Научная новизна *состоит в том, что для оценки риска кибербезопасности информационно-коммуникационной инфраструктуры сообщества микросетей при различных способах управления им в работе предложен подход, позволяющий учитывать возможные состояния информационных систем при кибератаках.*

Ключевые слова: *киберфизическая энергетическая система, микросеть, информационная система, качество информации, риск кибербезопасности, кибератаки.*

ASSESSMENT OF CYBER SECURITY RISK OF MICROGRIDS ENERGY COMMUNITY[3]

Gurina L. A.[4]

The research aims *to develop a methodological approach to assessing the cybersecurity risk of microgrids with interconnected information systems.*

The research relies *on the Markov processes, probabilistic methods, methods of fuzzy set theory.*

Research result: *The hierarchical management structure of energy communities is considered, possible cyber-attacks on the microgrid community management system are identified, and a classification of cyber-attacks is given, the consequence of which is a violation of the quality of information. A model of states of the microgrid information system is proposed, on the basis of which a structural model of the development of states of the energy community under various control methods is obtained. An approach has been developed for assessing the cybersecurity risk of the information and communication infrastructure of a microgrid community.*

The scientific novelty lies in the *fact that in order to assess the cybersecurity risk of the information and communication infrastructure of the microgrid community under various methods of managing it, the work proposes an approach that allows taking into account the possible states of information systems during cyber-attacks.*

Keywords: *cyber-physical energy system, microgrid, information system, information quality, cybersecurity risk, cyber-attacks.*

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 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.

4 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

Введение

Электроэнергетические системы (ЭЭС) претерпевают радикальные изменения своих свойств не только за счет трансформации своей внутренней структуры, но и за счет использования инновационных технологий производства, передачи, хранения, распределения и потребления электроэнергии [1]. Возможности использования возобновляемых источников энергии привели все большему распространению микросетей. Микросети включают в себя такие источники распределенной генерации, как ветряные турбины, дизель-генераторы, топливные элементы, фотоэлектрические системы, системы хранения энергии и т.д. Масштабное применение силовой электроники, инверторов и других цифровых устройств при эксплуатации микросетей привели к росту их уязвимостей к киберугрозам. Несмотря на многочисленные преимущества с технической, экономической и экологической точек зрения, объединение микросетей в энергетические сообщества (ЭСО) [2] способствует появлению дополнительных кибеуязвимостей из-за расширения информационно-коммуникационной инфраструктуры и путей передачи данных в зависимости от способа управления ими. Становится важным оценка риска кибербезопасности ЭСО микросетей.

Применение информационных и коммуникационных технологий играет важную роль при эксплуатации и управлении ЭСО микросетями. Интеграция информационных систем и технологической части микросетей трансформирует их в киберфизические энергетические системы [3] с развитыми программными сетями управления и связи, что ведет к взаимозависимостям между информационной и физической инфраструктурами микросетей [4]. Неисправности и сбои в одной из подсистем могут передаваться между ними, усугубляя последствия как для микросетей, так и для всего сообщества в целом. Так, киберинцидент в информационной системе одной микросети может повлиять на работу не только подвергшейся кибератаке микросети, но и на надежное функционирование остальных микросетей в составе сообщества. Таким образом, работа ЭСО зависит от киберустойчивости взаимозависимых информационных систем микросетей. Нарушение качества информационных потоков в результате кибератак [5], например, задержка или искажение данных, может повлиять на надежную и бесперебойную работу технологической части ЭСО и, тем самым, поставить под угрозу устойчивое и безопасное функционирование интеллектуальных сетей в целом.

Современные системы SCADA, эксплуатируемые при управлении микросетями, перешли к использованию стандартных коммуникационных технологий, чтобы обеспечить доступ к удаленным устройствам и упростить интерфейс между устройствами от разных поставщиков. Следовательно, количество возможных точек атаки, которые могут использовать злоумышленники, резко возросло. Другой распространенной практикой является использование стандартных аппаратных и программных платформ для снижения затрат и повышения гибкости [6]. Новые уязвимости увеличивают риск киберугроз для большого количества SCADA-систем.

Целью работы является разработка методическая подхода оценки риска кибербезопасности сообщества микросетей с учетом взаимосвязей информационных систем.

Для повышения кибербезопасности и киберустойчивости ЭСО необходимо учитывать взаимозависимости не только между информационно-коммуникационной и технологической инфраструктурой микросети, но и сложную взаимосвязь внутри информационно-коммуникационной инфраструктуры сообщества микросетей.

Анализ кибербезопасности сообществ микросетей

А. Структура и задачи управления ЭСО микросетей.

При управлении ЭСО обычно используется иерархическая структура (рис. 1). Основная концепция различных методов управления подразделяется на три уровня: нижний, средний и верхний. Эти методы используются для обеспечения координации между микросетями, которая зависит от многих факторов, включая скоординированный контроль с сетями связи и без них. Уровни управления применимы для работы ЭСО как в сетевом, так и в изолированном режиме.

На нижнем уровне осуществляется управление локальной мощностью, напряжением и током, следуя значениям параметров, заданным контроллерами верхнего уровня. Основными переменными являются выходное напряжение, частота и отслеживаемые значения, получаемые от внутреннего контура управления. Основными целями управления являются первичное регулирование частоты, первичное регулирование напряжения, автоматической частотной разгрузки [7].

На среднем уровне управлении решаются задачи системного уровня, такие как регулирование качества электроэнергии, синхронизация микросетей в составе сообщества, координация распределенной генерации и т.д. [8]. Основными задачами среднего уровня является управление спросом, выбор состава включенного генерирующего оборудования, вторичное регулирование частоты, вторичное регулирование напряжения, прогнозирование

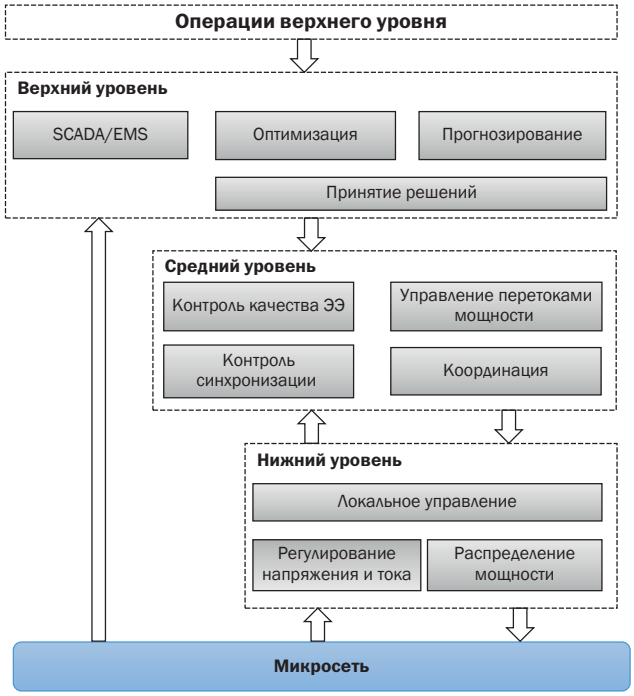

Рис. 1. Иерархическая схема управления сообществом микросетей

графиков нагрузки потребителей, прогнозирование выработки объектами распределенной генерации [9].

Решение задач оптимизации, управления и общего регулирования системы решается на верхнем уровне [10]. С технической и экономической точек зрения оптимальная работа всех генераторов достигается за счет использования методов верхнего уровня управления. Все микросети в составе ЭСО учитывают как технические, так и экономические аспекты системы управления распределением (DMS).

Нижний уровень управления в качестве базового уровня, объединяет контуры управления, направленные на регулирование напряжения, тока и мощности, а также определяет динамические характеристики локальных устройств. Средний и верхний уровни управления обеспечивают такие расширенные функциональные возможности, как поддержание качества напряжения, улучшение распределения тока и оптимизация работы.

Кибератаки могут повлиять на контроль напряжения микросетей, системы управления энергопотреблением и управление потребляемой мощностью [11].

Напряжение интеллектуальной микросети обычно контролируется распределенными генераторами с интерфейсом силовой электроники. В таких системах измеряется уровень напряжения и/или реактивная мощность системы, а система управления вырабатывает реактивную эталонную мощность для выработки электроэнергии. Атаки FDI, которые изменяют измеренное датчиком напряжение и/или данные реактивной мощности, параметры управления, могут повлиять на регулирование напряжения микросети [12]. Более того, злоумышленники могут получить доступ к многоуровневой системе управления микросетью (рис. 1) и изменить управляющие сигналы между уровнями (например, внести ошибки в опорные измерения мощности распределенной генерации).

Кибератаки, нацеленные на частоту микросетей, называются атаками на переходные процессы в микросетях. Злоумышленники могут вносить ошибки в управляющие сигналы между уровнями управления, изменять параметры управления и измерения датчиков или изменять выходные параметры источников питания, чтобы повлиять на изменение частоты микросети [13]. Следует отметить, что регулирование частоты микросети чувствительно к измерениям активной мощности и частоты, а также опорным сигналам. В микросетях частота обычно регулируется вращающимися машинами. Любые атаки, направленные на измерения скорости или угла ротора, могут повлиять на частоту микросетей. В последнее время для повышения устойчивости микросетей используются системы накопления энергии.

Б. Классификация кибератак на информационно-коммуникационную инфраструктуру энергетического сообщества

Первичный и вторичный уровни управления, несущие важную информацию, подвержены кибератакам. Кибератаки в микросетях вызывают не только проблемы с целостностью, доступностью и конфиденциальностью данных, но и могут привести таким к неблагоприятным последствиям как нарушение управления, отказы функционирования всего энергетического сообщества.

Передача данных от измерительных устройств и обмен данными между информационными системами микросетей необходимы для достижения эффективного управления сообществом микросетей. Непрерывный мониторинг и анализ данных играет важную роль в обеспечении качества информации, используемой при управлении микросетями.

Кибератаки на информационно-коммуникационную инфраструктуру можно разделить на атаки на целостность, доступность и конфиденциальность данных. Атака на целостность – это кибератака, последствием которой является недостоверность информации. Наиболее распространенной из кибератак на целостность является атака внедрения ложных данных (FDI-атака). Атака на доступность – это кибератака, которая препятствует своевременному получению необходимых данных или сигналов. К этому типу кибератак относятся атаки отказа

Таблица 1

Классификация кибератак, нарушающих качество информационных потоков при управлении сообществом микросетей

Целостность	Доступность	Конфиденциальность
FDI-атака	Jamming-атака	Социальная инженерия
Hijacking-атака	Wormhole-атака	Подслушивание
Подделка данных	DoS-атака	Анализ трафика Несанкцио-нированный доступ
Атака повторного воспроизведения	DDos-атака	Кража паролей
Wormhole-атака	Переполнение буфера Puppet-атака	Атака «Человек посередине»,
Spoofing-атака	Time Synchronization	Атака перехвата
Атака модификации	Masquerade -атака	Атака повторного воспроизведения
Атака «Человек посередине»	Атака «Человек посередине»	Masquerade -атака
Masquerade-атака	Spoofing-атака	

в обслуживании (DoS-атака). Атака на конфиденциальность относится к кибератакам, при которых неавторизованные лица незаконно получают информацию. Как правило, атаки на конфиденциальность не затрагивают систему напрямую, но часто сочетаются с другими атаками. В таблице 1 приведены возможные кибератаки на информационно-коммуникационную инфраструктуру энергетического сообщества, направленные на целостность, доступность и конфиденциальность информации [14–28].

Оценка рисков кибербезопасности информационно-коммуникационной инфраструктуры сообщества микросетей

На основе описанной иерархии управления способ реализации уровней управления ЭСО микросетей может быть централизованным, децентрализованным или распределенным (рис. 2) [29].

При кибератаках на информационно-коммуникационную инфраструктуру энергетического сообщества возможные состояния информационной системы i-й микросети можно охарактеризовать на основе двухуровневой модели:

$$S_i = \begin{cases} 1, \textit{информационная система микросети подвержена кибератаке} \\ 0, \textit{в противном случае}. \end{cases} \quad (1)$$

Кибератаки на ЭСО могут быть направлены как информационную систему одной микросети, так и на информационные системы нескольких микросетей. Также, в зависимости от способа управления сообществом управления с учетом взаимовлияния информационных систем микросетей, последствия кибератаки на одну из микросетей может быть распространено на информационные системы других микросетей. В [30] при моделировании кибератак на информационные системы микросетей при распределенном вторичном управлении сообществом микросетей проведен

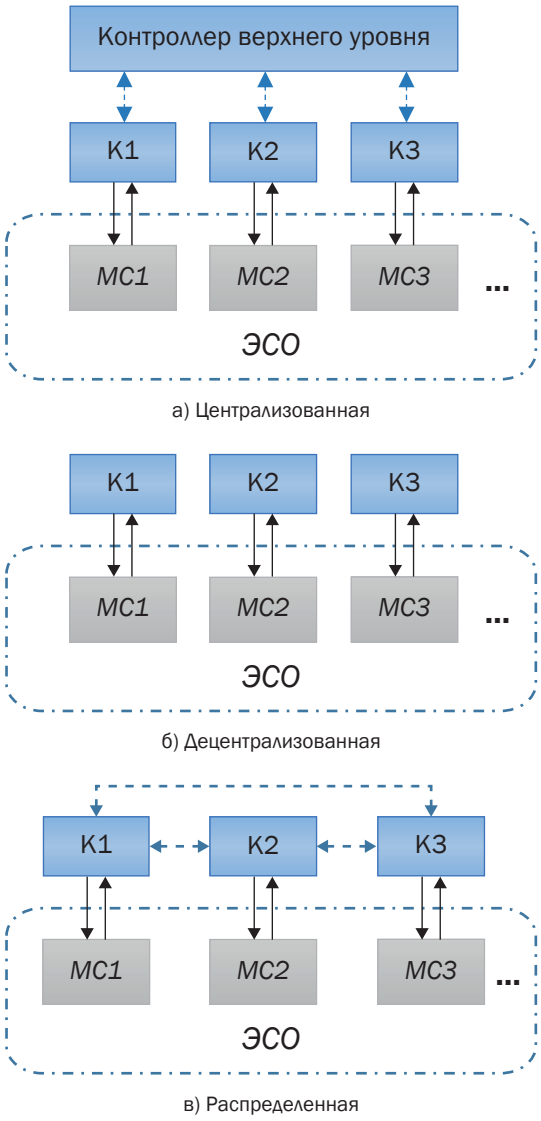

Рис. 2. Способы реализации уровней управления (- - - - - - – потоки данных при взаимодействии микросетей в составе сообщества и управлении им)

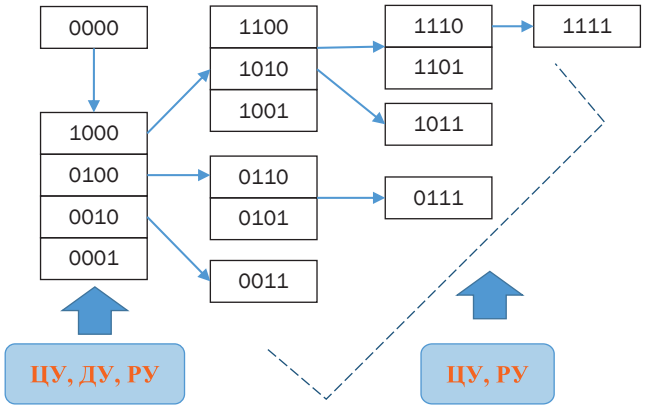

Рис. 3. Возможные состояния информационно-коммуникационной инфраструктуры ЭСО при кибератаках (ЦУ – централизованное управление, ДУ – децентрализованное управление, РУ – распределенное управление)

анализ последствий кибератак на остальные информационные системы микросетей. Наиболее опасными по последствиям для информационно-коммуникационной инфраструктуры энергетического сообщества являются FDI-атака и Hijacking-атака.

На примере четырех микросетей в составе сообщества на основе марковских процессов смоделированы возможные состояния информационно-коммуникационной инфраструктуры при различных способах управления – централизованном, децентрализованном и распределенном (рис. 3.).

Оценка риска кибербезопасности информационно-коммуникационной инфраструктуры ЭСО может быть проведена на основе следующей нечеткой модели

$$\tilde{R}_S = \prod_{i=1}^{N} \tilde{R}i \quad , \qquad (2)$$

где $\tilde{R}_i$ – уровень риска кибербезопасности i-й микросети, N – количество микросетей в составе сообщества.

Оценка уровня риска кибербезопасности i-й микросети определяется при использовании разработанной в [31] иерархической нечеткой системы (рис. 4).

Согласно модели (2) разработана иерархическая нечеткая система определения риска кибербезопасности сообщества микросетей. Для описанного примера ЭСО, включающего четыре микросети, на рис. 5. представлена нечеткая система оценки риска кибербезопасности. Семантическое описание уровней риска кибербезопасности информационно-коммуникационной инфраструктуры сообщества микросетей дано в табл. 2.

Заключение

Выявлены возможные кибератак на информационно-коммуникационную инфраструктуру энергетического сообщества микросетей. Приведена классификация кибератак, последствием которых является нарушение качество информационных потоков. Предложена модель состояний информационных систем микросетей в составе сообщества, на основе которой получена структурная модель развития состояний взаимосвязанных информационных систем микросетей в составе ЭСО. Разработан подход для оценки риска кибербезопасности информационно-коммуникационной инфраструктуры сообщества микросетей.

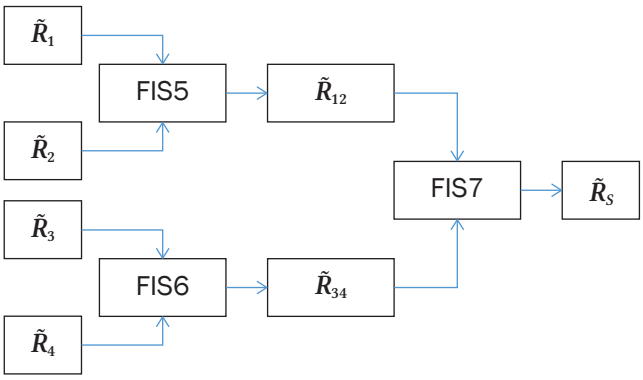

Рис. 5. Иерархическая нечеткая система оценки риска кибербезопасности сообщества микросетей

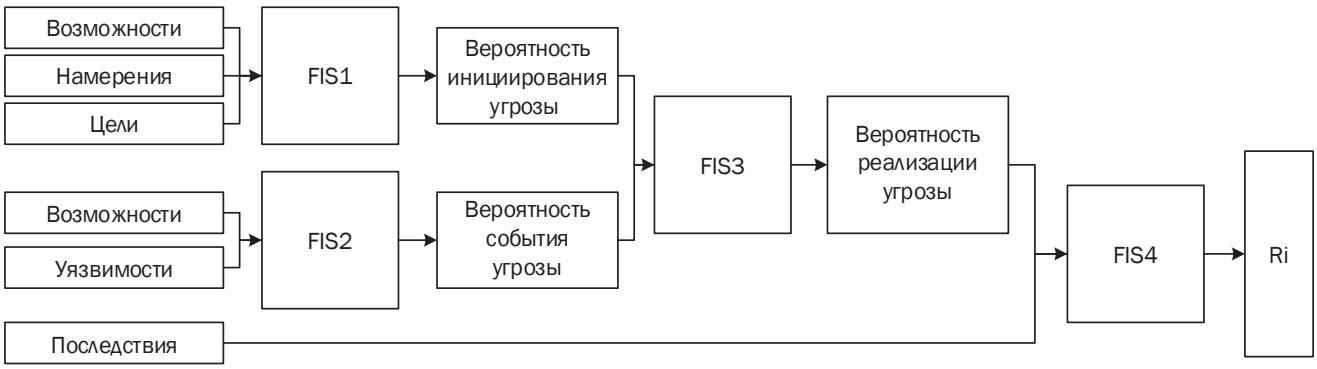

Рис. 4. Иерархическая нечеткая система оценки рисков кибербезопасности микросети

Таблица 2

Уровни риска кибербезопасности ИС микросетей

Уровень/ диапазон изменения	Описание
Низкий L,[0,0.24]	Реализованная кибератака на микросеть не приводит к отказам и сбоям компонентов ИС как самой микросети, так и компонентов ИС остальных микросетей в составе сообщества. Срабатывают все меры по обеспечению киберустойчивости. Функциональность системы управления высокая.
Средний M,[0.25,0.74]	В результате кибератаки на микросеть возможны незначительные сбои и ошибки в управлении сообществом микросетей, которые устранимы и не оказывают критического влияния на функциональность информационно-коммуникационной инфраструктуры. Реализация функций управления осуществляется в требуемом объеме и не приводит к нарушениям функциональности сообщества микросетей.
Высокий H,[0.75,1]	Опасность возникновения отказов и сбоев в энергетическом сообществе высокая в результате кибератак на ИС микросети. Сочетание отказов компонентов и/или ошибок в информационно-коммуникационной инфраструктуре может привести к значительным нарушениям функционирования сообщества микросетей.

Литература

1. *Voropai N. Electric Power System Transformations: A Review of Main Prospects and Challenges. Energies. 2020, 13, 5639. DOI: 10.3390/en13215639*
2. *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.*
3. *Zografopoulos Ioannis, Ospina Juan, Liu XiaoRui, Konstantinou, Charalambos. Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies. 2021*
4. *H. Pan, H. Lian, C. Na and X. Li. Modeling and Vulnerability Analysis of Cyber-Physical Power Systems Based on Community Theory // in IEEE Systems Journal. Sept. 2020, vol. 14, no. 3, pp. 3938–3948. DOI: 10.1109/JSYST.2020.2969023.*
5. *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. 25–35. DOI:10.24160/0013-5380-2021-6-25-32*
6. *D. Pliatsios, P. Sarigiannidis, T. Lagkas and A. G. Sarigiannidis. A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics // in IEEE Communications Surveys & Tutorials. 2020, vol. 22, no. 3, pp. 1942–1976. DOI: 10.1109/COMST.2020.2987688.*
7. *Unamuno E., Barrena JA. Equivalence of primary control strategies for AC and DC microgrids // Energies. 2017, 10(1), pp. 1–13.*
8. *Jin C, Wang J, Wang P. Coordinated secondary control for autonomous hybrid three-port AC/DC/DS microgrid // CSEE J Power Energy Syst. 2018, 4(1), pp. 1–10.*
9. *Илюшин П. В. Перспективы развития и принципы построения систем автоматическоо управления режимами микроэнергосистем // Материалы юбилейной X Международной научно-технической конференции «Электроэнергетика глазами молодежи-2019». Том 1, 2019, с. 59–64.*
10. *Zakariazadeh A, Jadid S, Siano P. Smart microgrid energy and reserve scheduling with demand response using stochastic optimization // Int J Electr Power Energy Syst. 2014, 63, pp. 523–533.*
11. *Sahoo S., Mishra S., Peng, J. C., Dragicevic T. A Stealth Cyber Attack Detection Strategy for DC Microgrids // IEEE Trans. Power Electron. 2019, 34, pp. 8162–8174.*
12. *Hao J., Kang, E., Sun J., Wang Z., Meng, Z., Li X., Ming Z. An Adaptive Markov Strategy for Defending Smart Grid False Data Injection from Malicious Attackers // IEEE Trans. Smart Grid. 2018, 9, pp. 2398–2408.*
13. *Chen C., Zhang, K., Yuan K., Zhu L., Qian M. Novel Detection Scheme Design Considering Cyber Attacks on Load Frequency Control // IEEE Trans. Ind. Inform. 2018, 14, pp. 1932–1941.*
14. *M. Z. Gunduz, R. Das. Analysis of cyber-attacks on smart grid applications // in: 2018 International Conference on Artificial Intelligence and Data Processing (IDAP). 2018, pp. 1–5. DOI:10.1109/IDAP.2018.8620728*
15. *H. Zhang, B. Liu and H. Wu. Smart Grid Cyber-Physical Attack and Defense: A Review // in IEEE Access. 2021, vol. 9, pp. 29641–29659. doi: 10.1109/ACCESS.2021.3058628*
16. *V. S. Rajkumar, A. Ştefanov, A. Presekal, P. Palensky and J. L. R. Torres. Cyber Attacks on Power Grids: Causes and Propagation of Cascading Failures // in IEEE Access. 2023, vol. 11, pp. 103154–103176. DOI:10.1109/ACCESS.2023.3317695*
17. *J. Li and Y. Zhang. Resilient DoS Attack Detector Design for Cyber-Physical Systems // 2023 12th International Conference on Renewable Energy Research and Applications (ICRERA), Oshawa, ON, Canada, 2023, pp. 1-5. DOI:10.1109/ICRERA59003.2023.10269439*
18. *S. Roy, A. Kumar and U. P. Rao. Security Attacks and it's Countermeasures on Smart Grid: A Review // 2023 International Conference on Computer, Electronics & Electrical Engineering & their Applications (IC2E3), Srinagar Garhwal, India, 2023, pp. 1–6. DOI:10.1109/IC2E357697.2023.10262686*
19. *T. Zhang and D. An. Data Integrity Attack Strategy against State Estimation Results of Distributed Power System // 2023 5th Asia Energy and Electrical Engineering Symposium (AEEES), Chengdu, China, 2023, pp. 1146-1151. DOI:10.1109/AEEES56888.2023.10114340*

20. *S. Vahidi, M. Ghafouri, M. Au, M. Kassouf, A. Mohammadi and M. Debbabi. Security of Wide-Area Monitoring, Protection, and Control (WAMPAC) Systems of the Smart Grid: A Survey on Challenges and Opportunities // in IEEE Communications Surveys & Tutorials. 2023, vol. 25, no. 2, pp. 1294–1335. DOI:10.1109/COMST.2023.3251899.*
21. *G. B. Gaggero, D. Piserà, P. Girdinio, F. Silvestro and M. Marchese. Novel Cybersecurity Issues in Smart Energy Communities // 2023 1st International Conference on Advanced Innovations in Smart Cities (ICAISC), Jeddah, Saudi Arabia, 2023, pp. 1–6. DOI:10.1109/ICAISC56366.2023.10085312*
22. *J. Kim, S. Bhela, J. Anderson and G. Zussman. Identification of Intraday False Data Injection Attack on DER Dispatch Signals // 2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Singapore, Singapore, 2022, pp. 40–46. DOI:10.1109/SmartGridComm52983.2022.9960974*
23. *A. Huseinovic, Y. Korkmaz, H. Bisgin, S. Mrdović and S. Uludag. PMU Spoof Detection via Image Classification Methodology against Repeated Value Attacks by using Deep Learning // 2022 XXVIII International Conference on Information, Communication and Automation Technologies (ICAT), Sarajevo, Bosnia and Herzegovina, 2022, pp. 1–6. DOI:10.1109/ICAT54566.2022.9811128*
24. *M. D. Roig Greidanus, S. K. Mazumder and N. Gajanur. Identification of a Delay Attack in the Secondary Control of Grid-Tied Inverter Systems // 2021 IEEE 12th International Symposium on Power Electronics for Distributed Generation Systems (PEDG), Chicago, IL, USA, 2021, pp. 1–6. DOI:10.1109/PEDG51384.2021.9494253*
25. *K. P. Swain, A. Tiwari, A. Sharma, S. Chakrabarti and A. Karkare. Comprehensive Demonstration of Man-in-the-Middle Attack in PDC and PMU Network // 2022 22nd National Power Systems Conference (NPSC), New Delhi, India, 2022, pp. 213-217. DOI:10.1109/NPSC57038.2022.10069874*
26. *M. Z. Gunduz, R. Das. A comparison of cyber-security oriented testbeds for IoTbased smart grids // in: 2018 6th International Symposium on Digital Forensic and Security (ISDFS), 2018, pp. 1–6. DOI:10.1109/ISDFS.2018.8355329*
27. *Z. E. Mrabet, N. Kaabouch, H. E. Ghazi, H. E. Ghazi. Cyber-security in smart grid: survey and challenges // Comput. Electr. Eng. 2018, 67, pp. 469–482. DOI:10.1016/j. compeleceng.2018.01.015*
28. *M. S. Al-kahtani, L. Karim. A survey on attacks and defense mechanisms in smart grids // Int. J. Comput. Eng. Inform. Technol. 2019, 11 (5), 7.*
29. *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.*
30. *Гурина Л. А., Томин Н. В. Разработка комплексного подхода к обеспечению кибербезопасности взаимосвязанных информационных систем при интеллектуальном управлении сообществом микросетей // Вопросы кибербезопасности. 2023, № 4(56), с. 94–104. DOI: 10.21681/2311-3456-2023-4-94-104*
31. *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.*