УДК 621.311 : 004.056

ОЦЕНКА КАЧЕСТВА ДАННЫХ SCADA И WAMS ПРИ КИБЕРАТАКАХ НА ИНФОРМАЦИОННО-КОММУНИКАЦИОННУЮ ИНФРАСТРУКТУРУ ЭЭС[1]

Колосок Ирина Николаевна

Д.т.н., ведущий научный сотрудник лаборатории «Управление функционированием электроэнергетических систем», e-mail: kolosok@isem.irk.ru

Гурина Людмила Александровна

К.т.н., доцент, старший научный сотрудник лаборатории «Управление функционированием электроэнергетических систем», e-mail: gurina@isem.irk.ru

Институт систем энергетики им. Л.А. Мелентьева СО РАН,

664130 г. Иркутск, ул. Лермонтова 130

Аннотация. Надежное функционирование электроэнергетических систем (ЭЭС) зависит от качества данных SCADA и WAMS, являющихся частью информационно-коммуникационной инфраструктуры киберфизических ЭЭС. Возрастающие угрозы кибербезопасности ЭЭС указывают на необходимость разработки методов анализа данных, учитывающих последствия кибератак на системы сбора, передачи и обработки информации. Проведенные исследования показали влияние кибератак на качество данных. Выявлена взаимозависимость нарушения свойств кибербезопасности и низкого качества данных. Предложен алгоритм оценки качества данных SCADA и WAMS с учетом свойств кибербезопасности информационно-коммуникационной инфраструктуры ЭЭС.

Ключевые слова: качество данных, SCADA, WAMS, кибербезопасность, нечеткая логика.

Цитирование: Колосок И. Н., Гурина Л. А. Оценка качества данных SCADA и WAMS при кибератаках на информационно-коммуникационную инфраструктуру ЭЭС // Информационные и математические технологии в науке и управлении. 2020. № 1 (17). С. 68 –78 DOI: 10.38028/ESI.2020.17.1.005

Введение. Переход к моделям киберфизических электроэнергетических систем (ЭЭС) обусловлен цифровой трансформацией электроэнергетики на основе новых информационно-коммуникационных технологий и цифровых моделей [7]. При этом проблемы устойчивости таких систем с позиций кибербезопасности не только остаются, но и, из-за повышенной уязвимости к кибератакам информационно-коммуникационных подсистем [13], выходят на первый план с точки зрения требований надежности [1]. Актуальность обеспечения своевременной и достоверной информацией задач управления ЭЭС подчеркивает необходимость разработки новых методов и моделей обработки данных на основе технологий искусственного интеллекта.

[1] Работа выполнена в рамках научного проекта III.17.4.2. программы фундаментальных исследований СО РАН, рег. № АААА-А17-117030310438-1.

В настоящее время, при управлении ЭЭС наряду с измерениями SCADA (Supervisory for Control and Data Acquisition) используются синхронизированные векторные измерения, поступающие от измерительных устройств системы WAMS (Wide Area Measurement Systems). Качество измерений системы SCADA и WAMS имеет решающее значение для бесперебойного функционирования ЭЭС. Под качеством информационных потоков данных понимается степень полноты и достоверности информации, обеспечивающих требуемую точность решения задач управления режимами ЭЭС.

В работе предложен алгоритм оценки качества данных при кибератаках на SCADA и WAMS на основе теории нечетких множеств. При разработке правил систем нечеткого вывода принимались во внимание такие требования кибербезопасности SCADA и WAMS, как своевременность, целостность, доступность, киберустойчивость, конфиденциальность. С учетом [11, 15, 17], проанализированы свойства киберфизических ЭЭС, выявлены возможные кибератаки, снижающие качество информационных потоков данных.

В [3] показано, что кибератаки на систему SCADA и WAMS приводят к выработке и реализации неправильных управляющих воздействий и к неблагоприятным последствиям при функционировании ЭЭС, поэтому крайне важно учитывать влияние кибератак на полноту и достоверность информации, используемой при управлении ЭЭС.

Предлагаемый алгоритм может быть использован как предварительный этап обработки информации в качестве барьера поступления «плохих» данных при решении такой важной задачи, как оценивание состояния ЭЭС.

Использование технологий искусственного интеллекта при анализе и обработке информационных потоков позволит повысить эффективность управления и надежность функционирования ЭЭС.

Цифровая трансформация свойств киберфизических электроэнергетических систем. Управление киберфизической ЭЭС осуществляется на основе единой цифровой среды (модель CIM), внедрения технологий кибербезопасности и применения интеллектуальных методов управления с целью повышения надежности и прозрачности функционирования ЭЭС.

Модель CIM (Common Information Model) на основе формата данных ODM (Open Model for Exchanging Power System Simulation Data) позволяет строить модели различной сложности, которые потом могут быть конвертированы в любой известный либо новый формат данных, используя дополнительно подключаемые модули. ODM - открытая модель для обмена данными при моделировании энергосистем, является международным открытым стандартом обмена данными для моделирования и расчета ЭЭС, поддерживает динамические расчеты [2]. На основе CIM-моделей IT-инфраструктура, интегрирующая интеллектуальную информационную, вычислительную и телекоммуникационную среды [6], должна обеспечить двустороннюю связь информационно-коммуникационной и технологической подсистем киберфизической ЭЭС.

Прозрачность функционирования ЭЭС требует реализации новых систем сбора, передачи и обработки потоков информации, развития технологий и методов моделирования исследуемых процессов, получения достоверных данных в реальном времени о режимах для задач управлении ЭЭС.

Переход к интеллектуальному управлению ЭЭС и возрастающие потребности мониторинга и анализа данных указывают на необходимость применения цифровых технологий обработки данных на основе методов искусственного интеллекта:

- искусственные нейронные сети и генетические алгоритмы;
- логическое программирование;
- онтологический инжиниринг;
- нечеткая логика и т.д.

При всех очевидных преимуществах цифровизации ЭЭС отмечена их повышенная уязвимость к кибератакам, связанная с широкомасштабностью (напр., территориальная разрозненность) технологической части и многокомпонентностью (устройства сбора, передачи и обработки информации на всех уровнях управления) информационно-коммуникационной инфраструктуры киберфизических ЭЭС и их информационного взаимодействия [13]. На уровне аппаратного и программного обеспечения задач управления растет реализация скрытых угроз. Интеграция технологий IT-инфраструктуры увеличивает число кибератак.

Управление ЭЭС осуществляется на основе данных, поступающих от системы SCADA и WAMS. Кибератаки, направленные на компоненты этих систем, или двусторонние потоки данных информационно-коммуникационной и технологической систем, могут нарушить не только функции управления, но и вызвать отказы в работе ЭЭС.

В [3] показано влияние низкого качества информации на ложную визуализацию режимов ЭЭС и выработку неправильных управляющих воздействий вследствие кибератак на системы SCADA и WAMS.

Качество данных измерений системы SCADA, WAMS. Для широкомасштабного мониторинга ЭЭС наряду с системами SCADA внедрена WAMS, измерения в которой поступают от устройств PMU. В этих условиях управление ЭЭС может осуществляться на основе:

- измерений системы SCADA;
- измерений WAMS;
- смешанных измерений.

Технологии синхронизированных векторных измерений позволяют повысить наблюдаемость системы и обеспечить задачи управления более точной и своевременной информацией.

Тем не менее, совместное использование измерений, поступающих от системы SCADA и WAMS, требует решения следующих проблем:

- высокая вычислительная нагрузка;
- большие данные;
- плохая обусловленность ковариационной матрицы погрешностей измерений;
- необходимость синхронизации данных.

Возникают серьезные проблемы качества данных и кибербезопасности, имеющих сложное взаимодействие, при кибератаках на систему SCADA и WAMS. Так, снижение качества данных – последствия успешно проведенной кибератаки. Вместе с тем, анализ качества данных может определить тип реализованной кибератаки и выявить неучтенные

уязвимости [14, 16]. Для проверки свойств кибербезопасности необходима разработка методов анализа качества данных SCADA, WAMS.

В этой связи проведен анализ влияния кибератак на качество данных с учетом нарушений свойств кибербезопасности (рис. 1).

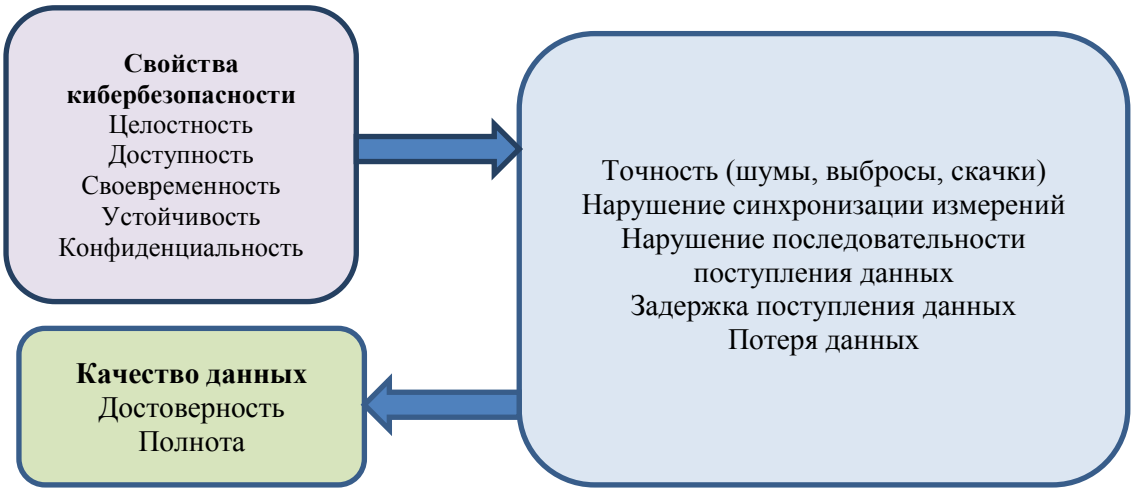

Рис. 1. Влияние кибератак на качество данных.

В [8] введен критерий качества информации и метод его определения на основе теории нечетких множеств. Авторами [5] в зависимости от уровня полноты и достоверности измерений SCADA и WAMS, предложены модели измерений для оценивания состояния ЭЭС. Учет влияния кибератак на полноту и достоверность информации потребовал расширения факторов при оценке качества данных. В работах [10, 12, 18] рассмотрены возможные кибератаки на системы сбора, передачи и обработки информации, выявлены их уязвимости, показано влияние нарушения свойств кибербезопасности системы SCADA и WAMS на функции управления ЭЭС [3]. Данные исследования показали необходимость учета следующих факторов влияния кибератак на качество данных в системах SCADA, WAMS.

- последовательность;
- своевременность поступления данных;
- синхронизация данных.

Своевременность поступления данных учитывает неопределенность информации в реальном времени. Синхронизацию данных необходимо учитывать при совместном использовании измерений SCADA и синхронизированных векторных измерений.

В табл. 1 представлена взаимозависимость качества данных и свойств кибербезопасности при кибератаках на компоненты SCADA и WAMS.

Таблица 1. Взаимозависимость качества данных и свойств кибербезопасности SCADA, WAMS

Компоненты SCADA, WAMS	Качество данных	Свойства кибербезопасности	Кибератаки
PMU, PDC, Super PDC, RTU, MTU	Полнота, достоверность, последовательность, синхронизация	Целостность, конфиденциальность	Атаки внедрения ложных данных, Переполнение буфера, Spoofing, атаки повторного произведения, подделка устройства
Система передачи информации	Полнота, последовательность,	Целостность, доступность,	DOS-атаки, Spoofing,

	своевременность, синхронизация	Своевременность, конфиденциальность	Атака «человек посередине», атаки повторного произведения, компрометация маршрутизаторов связи
Приложение EMS	Полнота, достоверность, последовательность, своевременность, синхронизация	Целостность, доступность, своевременность, киберустойчивость, конфиденциальность	Атаки внедрения ложных данных, DOS-атаки, атаки повторного произведения

Нечеткая система обработки информационных потоков данных с учетом свойств кибербезопасности системы SCADA, WAMS. В основе предлагаемого подхода оценки качества данных заложен алгоритм, реализующий следующие этапы:

1. Определение уровня достоверности информации;
2. Определение уровня полноты информации;
3. Оценка качества информации.

Для определения уровней достоверности и полноты информации заданы лингвистические переменные (точность, последовательность, согласованность, своевременность, достаточность), определены терм-множества и дано их семантическое описание. Разработанная нечеткая система оценки качества данных измерений представлена на рис. 2.

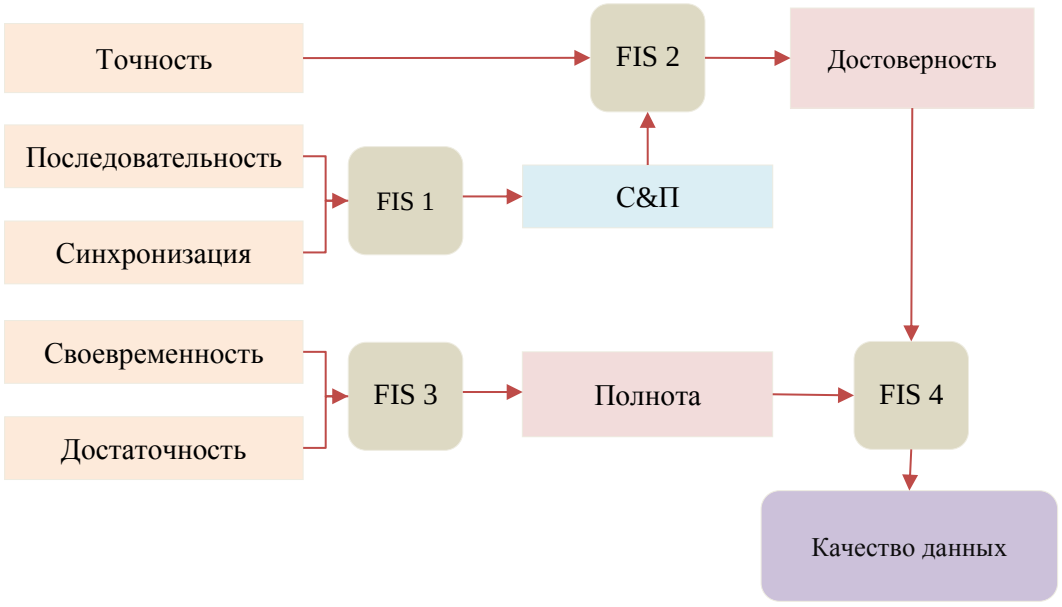

Рис. 2. Нечеткая система оценки качества данных

В зависимости от оценки качества данных выбираются предложенные в [5] модели измерений.

Пример. С учетом проблем оценивания состояния ЭЭС, возникающих при кибератаках на систему SCADA и WAMS [4, 9], построена нечеткая система оценки качества информации.

Семантическое описание входных и выходных лингвистических переменных представлено в таблицах 2-5.

Таблица 2. Уровни факторов, влияющих на достоверность информации

Уровень	Точность	Последовательность	Синхронизация
Низкий 0-0,25	Измерения содержат ошибки, в том числе не обнаруживаемые, полученные в результате кибератак	Нарушена	Данные не синхронизированы
Средний 0,25-0,75	Измерения содержат ошибки в результате кибератак, обнаруживаемые методами достоверизации.	Нарушена, но есть возможность устранения (дублирование, сравнение)	Данные не синхронизированы, но есть возможность дублирования и восстановления
Высокий 0,75-1	Измерения содержат ошибки, полученные из-за погрешности измерительных устройств и т.д, не влияющие на точность ОС ЭЭС	Не нарушена	Данные синхронизированы

Таблица 3. Уровни факторов, влияющих на полноту информации

Уровень	Своевременность	Достаточность
Низкий 0-0,25	Большое запаздывание	Отсутствие данных
Средний 0,25-0,75	Запаздывание с возможностью учета в моделях измерений	Потеря данных не значительна для решения задачи
Высокий 0,75-1	Измерения поступают без задержек	Измерения поступают в достаточном объеме

Таблица 4. Полнота и достоверность информации

Уровень	Полнота	Достоверность
Низкий 0-0,25	Система не наблюдаема	Сомнительные
Средний 0,25-0,75	Возможность дорасчета отсутствующих значений измерений	Ошибочные
Высокий 0,75-1	Избыточный объем измерений	Достоверные

Таблица 5. Качество информации

Уровень	Качество
Низкий 0-0,25	Ненаблюдаемость сети и/или недостоверность измерений
Средний 0,25-0,75	Применение методов достоверизация измерений, фильтрация ошибок, восстановление потоков измерений, учет старения информации позволят оценить состояние ЭЭС с требуемой точностью
Высокий 0,75-1	Полный достоверный поток информации

Полученные трехмерные поверхности полноты, достоверности и качества информации показаны на рис. 3-5.

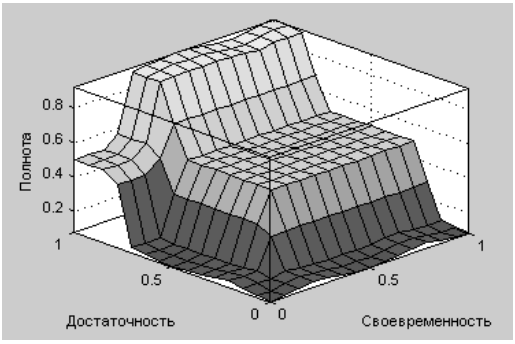

Рис. 3. Зависимость полноты информации от достаточности и своевременности поступления данных

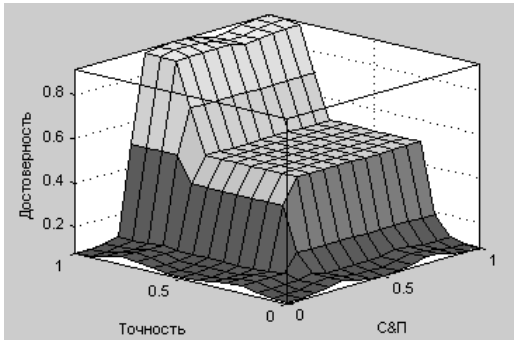

Рис. 4. Зависимость достоверности информации от точности, последовательности и синхронизации данных

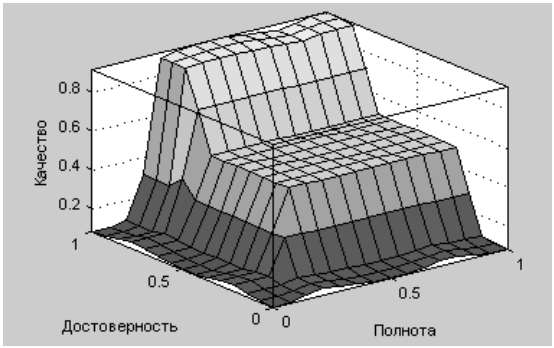

Рис. 5. Качество измерений

Как видно из полученных результатов, низкий уровень любого из входных факторов, вызванный кибератаками, влияет на качество информации (темный цвет на рис. 3-5), особенно это отражается на достоверности измерений.

Тем самым обосновывается необходимость анализа данных при решении задачи оценивания состояния ЭЭС с учетом дополнительных факторов, как предварительный этап обработки данных.

Заключение. Проанализированы свойства ЭЭС, связанные с созданием кибер-физической ЭЭС. Проведенные исследования показали повышенную уязвимость таких систем к кибератакам на информационно-коммуникационную инфраструктуру.

Показана взаимозависимость свойств кибербезопасности системы SCADA, WAMS и качества измерений при кибератаках. Предложен алгоритм оценки качества данных с учетом нарушений свойств кибербезопасности как предварительный этап оценивания состояния ЭЭС, который проиллюстрирован приведенным примером.

СПИСОК ЛИТЕРАТУРЫ

1. Воропай Н.И., Колосок И.Н., Коркина Е.С., Осак А.Б. Киберугрозы и кибербезопасность в электроэнергетических системах // Сборник докладов всероссийской научно-технической конференции «Электроэнергетика глазами молодежи», Иркутск, Россия, 16-20 сентября 2019. Том 1. С.56-67.
2. Кобец Б.Б., Волкова И.О. Инновационное развитие электроэнергетики на базе концепции Smart Grid. М.: ИАЦ Энергия. 2010. 208 с.
3. Колосок И.Н., Гурина Л.А. Оценка рисков управления киберфизической ЭЭС на основе теории нечетких множеств // Методические вопросы исследования надежности больших

систем энергетики: Вып. 70. Методические и практические проблемы надежности систем энергетики. В 2-х книгах. / Книга 1 / отв. ред. Н.И. Воропай. Иркутск: ИСЭМ СО РАН. 2019. С. 238-247.

4. Колосок И.Н., Гурина Л.А. Повышение кибербезопасности интеллектуальных энергетических систем методами оценивания состояния // Вопросы кибербезопасности. 2018. № 3(27). С. 63–69.
5. Колосок И.Н., Гурина Л.А. Прогнозирование параметров режима при мониторинге и управлении электроэнергетической системой // Электричество. 2014. №1. С. 21-27.
6. Массель Л.В., Колосок И.Н., Гурина Л.А. Обработка информационных потоков при мониторинге и управлении режимами интеллектуальных электроэнергетических систем / Вестник ИрГТУ. №2 (73). 2013. С. 30-35.
7. Массель Л.В. Методы и интеллектуальные технологии научного обоснования стратегических решений по цифровой трансформации энергетики // Энергетическая политика. 2018. №5. С. 30-42.
8. Савина Н.В., Гурина Л.А. Выбор критерия качества отображения информации при управлении режимами // Сб. трудов третьей Всеросс. Научн.-техн. конф. С международным участием «Энергетика: управление, качество и эффективность использования энергоресурсов». – Благовещенск, 2003. Том 1. С. 127-132.
9. Хохлов М.В. Уязвимость оценивания состояния ЭЭС к кибератакам // Методические вопросы исследования надежности больших систем энергетики. Вып. 65. Надежность либерализованных систем энергетики / отв. ред. Н.И. Воропай, А.Н. Назарычев. – Иркутск: ИСЭМ СО РАН. 2015. С. 557-566.
10. Hua. Lin, Yi Deng, Sandeep Shukla, James Thorp, Lamine Mili. Cyber Security Impacts on All-PMU State Estimator – A Case Study on Co-Simulation Platform GECO // In Proc. 5-8 Nov. 2012 Smart Grid Communications (SmartGridComm). 2012 IEEE Third International Conf. 2012. Pp. 587-592
11. K. Gai, M. Qiu, Z. Ming, H. Zhao, L. Qiu, Spoofing-Jamming Attack Strategy Using Optimal Power Distributions in Wireless Smart Grid Net-works // IEEE Transactions on Smart Grid. 2017. 8 (5). Pp. 2431-2439. doi: 10.1109/TSG.2017.26640.
12. Longfei Wei, Luis Puche Rondon, Amir Moghadasi, Arif I. Sarwat. Review of Cyber-Physical Attacks and Counter Defense Mechanisms for Advanced Metering Infrastructure in Smart Grid // Transmission and Distribution Conference and Exposition (T&D) 2018 IEEE/PES. 2018. Pp. 1-9.
13. Mohd Rihan, Mukhtar Ahmad, M. Salim Beg Vulnerability Analysis of Wide Area Measurement System in the Smart Grid // Smart Grid and Renewable Energy [Online] (Sep. 2013). P. 1-7. Available: http://www.scirp.org/journal/sigre.
14. S. Sridhar, A. Hahn and M. Govindarasu. Cyber attack-resilient control for smart grid // 2012 IEEE PES Innovative Smart Grid Technologies (ISGT), Washington, DC. 2012. Pp. 1-3.
15. S. Sridhar, A. Hanh, M. Govindarasu. Cyber-Physical System Security for the Electric Power Grid // Proceeding of the IEEE. Jan. 2012. Vol. 100. Pp. 210-224.
16. T.H. Morris, P. Shengyi, U. Adhikari, Cyber Security Recommendations for Wide Area Monitoring, Protection and Control Systems // IEEE Power and Energy Society General Meeting Proceedings. July 2012. Pp. 1-6.

17. Yao Liu, Peng Ning, Michael K. Reiter. False Data Injection Attacks against State Estimation in Electric Power Grids // CCS'09 Proceedings (9-13 November 2009, Chicago, Illinois, USA). Pp. 21-32
18. Zanouz S., Rogers K. M., Berthier R., Bobba R.B., Sanders W.H, Overbye T.J. SCPSE: Security-Oriented Cyber-Physical State Estimation for Power Grid Critical Infrastructure // IEEE Transactions on Smart Grid. December 2012. Vol.3, no.4. Pp.1790-1799.

UDK 621.311 : 004.056

QUALITY ASSESSMENT OF SCADA AND WAMS DATA IN THE CASE OF CYBERATTACKS ON INFORMATION AND COMMUNICATION INFRASTRUCTURE OF EPS [2]

Irina N. Kolosok
Professor, Leading Researcher of Laboratory of Electric Power Systems Operation and Control,
e-mail: kolosok@isem.irk.ru
Liudmila A. Gurina
Doctor, Senior Researcher of Laboratory of Electric Power Systems Operation and Control,
e-mail: gurina@isem.irk.ru
Melentiev Energy Systems Institute
Siberian Branch of the Russian Academy of Sciences
130, Lermontov Str., 664033, Irkutsk, Russia

Abstract. The reliable operation of the electric power systems (EPSs) depends on the quality of data provided by SCADA and WAMS, which are part of the information and communication infrastructure of cyber-physical EPS. Increasing threats to cyber security of EPS indicate the need to develop data analysis methods capable to take into account the effects of cyberattacks on systems for collecting, transmitting and processing the information. The findings of the studies have shown the impact of cyberattacks on the quality of data. The interdependence between the violation of cybersecurity properties and the low quality of data is revealed. The paper proposes an algorithm for quality assessment of SCADA and WAMS data, taking into account the cybersecurity properties of information and communication infrastructure of EPS.

Keywords: quality of data, SCADA, WAMS, cybersecurity, fuzzy logic.

References

1. Voropaj N.I., Kolosok I.N., Korkina E.S., Osak A.B. Kiberugrozy i kiberbezopasnost' v elektroenergeticheskih sistemah [Cyber threats and cybersecurity in electric power systems] // Sbornik dokladov vserossijskoj nauchno-tekhnicheskoj konferencii "Elektroenergetika glazami molodezhi" = in Proceedings of the All-Russian Sicence and Technology al conference "Power

[2] The research was carried out as part of the scientific project III.17.4.2. of the basic research program SB RAS, reg. number AAAA-A17-117030310438-1.

Engineering through the Eyes of Youth", Irkutsk, Rossiya, 16-20 sentyabrya 2019= Irkutsk, Russia, September 16–20, 2019, Tom 1=Vol.1. Pp. 56-67. (in Russian)

2. Kobec B.B., Volkova I.O. Innovacionnoe razvitie elektroenergetiki na baze koncepcii Smart Grid [Innovative development of the electric power industry based on the Smart Grid concept] // M.: IAC Energiya. 2010. 208 p.
3. Kolosok I.N., Gurina L.A. Ocenka riskov upravleniya kiberfizicheskoj EES na osnove teorii nechetkih mnozhestv [Risk control assessment of cyber-physical power system based on the theory of fuzzy sets] // Metodicheskie voprosy issledovaniya nadezhnosti bol'shih sistem energetiki: Vyp. 70. Metodicheskie i prakticheskie problemy nadezhnosti sistem energetiki. V 2-h knigah. / Kniga 1 / otv. red. N.I. Voropaj. Irkutsk: ISEM SO RAN. 2019. Pp. 238-247.
4. Kolosok I.N., Gurina L.A. Povyshenie kiberbezopasnosti intellektual'nyh energeticheskih sistem metodami ocenivaniya sostoyaniya [Improvement of Cybersecurity of Smart Grid by State Estimation Methods] // Voprosy kiberbezopasnosti = Cybersecurity issues**.** 2018. № 3 (27). Pp. 63–69. (in Russian)
5. Kolosok I.N., Gurina L.A. Prognozirovanie parametrov rezhima pri monitoringe i upravlenii elektroenergeticheskoj sistemoj [Prediction of state variables in monitoring and control of the electric power system] // Elektrichestvo = Electricity. 2014. №1. Pp. 21-27. (in Russian)
6. Massel' L.V., Kolosok I.N., Gurina L.A. Obrabotka informacionnyh potokov pri monitoringe i upravlenii rezhimami intellektual'nyh elektroenergeticheskih sistem [Information flow processing when monitor and control Smart Grid regimes] // Vestnik IrGTU = Proccedings of ISTU. 2013. №2(73). Pp. 30-35. (in Russian)
7. Massel' L.V. Metody i intellektual'nye tekhnologii nauchnogo obosnovaniya strategichskih reshenij po cifrovoj transformacii energetiki [Methods and intelligent technologies for scientific substantiation of strategic solutions on digital transformation of energy industry] // Energeticheskaya politika = Energy Policy. 2018. №5. Pp. 30-42. (in Russian)
8. Savina N.V., Gurina L.A. Vybor kriteriya kachestva otobrazheniya informacii pri upravlenii rezhimami [Selection of a quality criterion for displaying the data when managing modes] // Sb. trudov tret'ej Vseross. Nauchn.-tekhn. konf. S mezhdunarodnym uchastiem "Energetika: upravlenie, kachestvo i effektivnost' ispol'zovaniya energoresursov" = in Proceedings of the third All-Russian Science and Technology Conference with international participation "Energy: Management, Quality and Efficiency of Energy Use". – Blagoveshchensk, 2003. t. 1. Pp. 127-132.
9. Hohlov M.V. Uyazvimost' ocenivaniya sostoyaniya EES k kiberatakam [Vulnerability of EPS state estimation to cyberattacks] // Metodicheskie voprosy issledovaniya nadezhnosti bol'shih sistem energetiki. Vyp. 65. Nadezhnost' liberalizovannyh sistem energetiki / otv. red. N.I. Voropaj, A.N. Nazarychev. Irkutsk: ISEM SO RAN. 2015. Pp. 557-566
10. Hua. Lin, Yi Deng, Sandeep Shukla, James Thorp, Lamine Mili. Cyber Security Impacts on All-PMU State Estimator – A Case Study on Co-Simulation Platform GECO // In Proc. 5-8 Nov. 2012 Smart Grid Communications (SmartGridComm). 2012 IEEE Third International Conf. 2012. Pp. 587-592
11. K. Gai, M. Qiu, Z. Ming, H. Zhao, L. Qiu, Spoofing-Jamming Attack Strategy Using Optimal Power Distributions in Wireless Smart Grid Net-works // IEEE Transactions on Smart Grid. 2017. 8 (5). Pp. 2431-2439. doi: 10.1109/TSG.2017.26640.
12. Longfei Wei, Luis Puche Rondon, Amir Moghadasi, Arif I. Sarwat. Review of Cyber-Physical Attacks and Counter Defense Mechanisms for Advanced Metering Infrastructure in Smart Grid // Transmission and Distribution Conference and Exposition (T&D) 2018 IEEE/PES. 2018. Pp. 1-9.

13. Mohd Rihan, Mukhtar Ahmad, M. Salim Beg Vulnerability Analysis of Wide Area Measurement System in the Smart Grid // Smart Grid and Renewable Energy [Online] (Sep. 2013). P. 1-7. Available: http://www.scirp.org/journal/sigre.
14. S. Sridhar, A. Hahn and M. Govindarasu. Cyber attack-resilient control for smart grid // 2012 IEEE PES Innovative Smart Grid Technologies (ISGT), Washington, DC. 2012. Pp. 1-3.
15. S. Sridhar, A. Hanh, M. Govindarasu. Cyber-Physical System Security for the Electric Power Grid // Proceeding of the IEEE. Jan. 2012. Vol. 100. Pp. 210-224.
16. T.H. Morris, P. Shengyi, U. Adhikari, Cyber Security Recommendations for Wide Area Monitoring, Protection and Control Systems // IEEE Power and Energy Society General Meeting Proceedings. July 2012. Pp. 1-6.
17. Yao Liu, Peng Ning, Michael K. Reiter. False Data Injection Attacks against State Estimation in Electric Power Grids // CCS'09 Proceedings (9-13 November 2009, Chicago, Illinois, USA). Pp. 21-32
18. Zanouz S., Rogers K. M., Berthier R., Bobba R.B., Sanders W.H, Overbye T.J. SCPSE: Security-Oriented Cyber-Physical State Estimation for Power Grid Critical Infrastructure // IEEE Transactions on Smart Grid. December 2012. Vol.3, no.4. Pp.1790-1799.