УДК 621.311 : 004.056

ОБРАБОТКА СИНХРОНИЗИРОВАННЫХ ВЕКТОРНЫХ ИЗМЕРЕНИЙ МЕТОДАМИ НЕЧЕТКОЙ ЛОГИКИ ПРИ КИБЕРАТАКАХ НА ЭЛЕКТРОЭНЕРГЕТИЧЕСКУЮ СИСТЕМУ

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. Применение интеллектуальных и цифровых технологий в системах измерения, передачи и обработки информации, являющихся частью информационно-коммуникационной инфраструктуры электроэнергетической системы (ЭЭС), направлено на повышение эффективности управления ЭЭС. Вместе с тем, при цифровизации ЭЭС отмечен рост уязвимостей к кибератакам. В связи с этим возрастает актуальность обеспечения задач управления в условиях кибератак своевременной, полной и достоверной информацией. Предложен алгоритм обработки синхронизированных векторных измерений на основе вейвлет-анализа и нечеткой логики, повышающий качество информации, используемой в дальнейшем при оценивании состояния ЭЭС.

Ключевые слова: качество данных, синхронизированные векторные измерения, кибератаки, вейвлет-анализ, нечеткая логика.

Цитирование: Колосок И.Н., Гурина Л.А. Обработка синхронизированных векторных измерений методами нечеткой логики при кибератаках на электро-энергетическую систему //Информационные и математические технологии в науке и управлении. 2020. № 4 (20). С. 56-63. DOI: 10.38028/ESI.2020.20.4.005

Введение. Внедрение систем мониторинга переходных режимов (за рубежом такие системы называют WAMS - Wide Area Measurement Systemsпозволило при управлении ЭЭС наряду с традиционными измерениями SCADA[1] использовать синхронизированные векторные измерения (СВИ), поступающие от устройств PMU[2]. Благодаря более точным измерениям модулей и фаз напряжений в узлах, модулей и фаз токов в ветвях, уровень наблюдаемости и управляемости ЭЭС существенно возрастает. При оценивании состояния ЭЭС использование СВИ повышает точность получаемых оценок. Наряду с этим следует отметить уязвимость не только WAMS, но и всей информационно-коммуникационной инфраструктуры ЭЭС, частью которой является WAMS, к новым угрозам, возникающим в

[1] SCADA (аббр. от англ. Supervisory Control And Data Acquisition — диспетчерское управление и сбор данных) — программный пакет, предназначенный для разработки или обеспечения работы в реальном времени систем сбора, обработки, отображения и архивирования информации об объекте мониторинга или управления.

[2] PMU (аббр. от англ. Phasor Measurement Unit) – прибор, измеряющий комплексные величины тока и напряжения. В отличие от традиционных телеизмерений измерения от PMU синхронизированы по времени через GPS, точность их выше и поступают они в пункты сбора информации тысячами срезов в секунду, тогда как SCADA принимает один срез в несколько секунд

современном киберпространстве [9]. Приобретение ЭЭС киберфизического характера при цифровой трансформации ее свойств расширяет возможности реализации кибератак на информационно-коммуникационную инфраструктуру из-за наличия большого числа уязвимостей на всех уровнях иерархии управления ЭЭС [1]. В этих условиях обеспечение задач управления своевременной, полной и достоверной информацией, для сохранения устойчивого и надежного функционирования ЭЭС, особенно актуально.

Целью данной работы является разработка мер по повышению качества синхронизированных векторных измерений, нарушенного успешно проведенными кибератаками на информационно-коммуникационную инфраструктуру ЭЭС [6-8]. Под качеством информации понимается степень ее полноты и достоверности [3].

Отмечен целый класс кибератак, нарушающих такие свойства кибербезопасности информационно-коммуникационной инфраструктуры ЭЭС, как целостность и доступность [4]. Постоянное усовершенствование кибератак, чтобы быть не обнаруженными, требует пересмотра существующих методов обработки информации, необходимой для формирований управленческих решений.

Оценивание состояния (ОС) является ключевой задачей при управлении ЭЭС. При ее решении выполняется анализ наблюдаемости, обнаружение плохих данных, определяются оптимальные оценки параметров режима [2]. Разработка методов обработки данных, создающих барьер на пути распространения влияния кибератаках, не обнаруживаемые традиционными методами обнаружения плохих данных (ОПД), позволит повысить точность оценок измерений.

Использование только вероятностных методов обработки информации не всегда успешно из-за возникновения неопределенности данных, вызванной кибератаками. В этом случае предлагается совместное использование вейвлет-анализа и нечеткой логики.

Алгоритм обработки измерений. Последствием успешно проведенной кибератаки, например, атаки внедрения ложных данных, при решении оценивания состояния ЭЭС может быть выдача ложных оценок состояния, которые приведут к неправильным управленческим решениям, которые могут вызвать крупномасштабные аварии при функционировании ЭЭС. При этом возникает неопределенность данных измерений, ее характерными признаками являются неполнота и недостоверность. Важно обнаруживать и предотвращать влияние кибератак на качество информации.

Применение вейвлет-анализа и теории нечетких множеств при обработке данных измерений, как предварительный этап ОС ЭЭС, позволит существенно повысить как уровень достоверности, так и уровень полноты информации.

Так как традиционные методы оценивания состояния основаны на вероятностных предположениях об ошибках в измерениях и для надежной оценки состояния зачастую требуется избыточность измерений, применение нечеткой логики позволит использовать интервальный анализ данных и, тем самым, устранить проблему неполных данных.

Общая модель оценивания состояния представляется как

$$y = h(X) + \varepsilon, \qquad (1)$$

где y - вектор измерений с m элементами; X - вектор переменных состояния с n элементами; $h(.)$ – вектор-функция, который связывает переменные состояния и измерения (m функций); ε - вектор шума измерения.

Нечеткая постановка задачи оценивания состояния [11] предполагает, что, по меньшей мере, одно измерение представляется как нечеткое число.

Цель задачи состоит в минимизации взвешенной суммы квадратов ошибок, согласно выражению:

$$min\varepsilon^T R^{-1}\varepsilon. \quad (2)$$

Уравнение (2) представляет задачу взвешенных наименьших квадратов, решение которой получается путем замены ε на выражение, полученное из (1). Эта задачи минимизации затем решается путем формирования системы уравнений

$$H(X)^T R^{-1}[y - h(X)] = 0, \quad (3)$$

где $H(X)^T$ – транспонированная матрица Якоби, R – ковариационная матрица ошибок измерений.

Нечеткое число описывается, как

$$\tilde{Z} =< z_1, z_2, z_3, z_4 >, \quad (4)$$

где $< z_1, z_2, z_3, z_4 >$ - кортеж для трапецеидального нечеткого числа [10].

Параметры z_1, z_2, z_3, z_4 определяются, исходя из следующих выражений

$$\begin{gathered} z_1 = \min\{x_i\}, \\ z_2 = M[x_i] - [M[x_i] - \min\{x_i\}]\sigma, \\ z_3 = M[x_i] + [\max\{x_i\} - M[x_i]]\sigma, \\ z_4 = \max\{x_i\}, \end{gathered} \quad (5)$$

где $M[x_i]$ – математическое ожидание последовательности измерений, σ – среднее квадратическое отклонение последовательности измерений.

Если измерения содержат ошибки, вызванные кибератаками, возможно неточное определение параметров нечеткого числа. Для фильтрации ошибок и достоверизации данных предлагается проведение вейвлет-анализа потоков измерений [5].

Пример. Для демонстрации предложенного подхода обработки данных в качестве примера смоделирована кибератака внедрения ложных данных на устройства СВИ трехузловой схемы участка электрической сети (рис. 1).

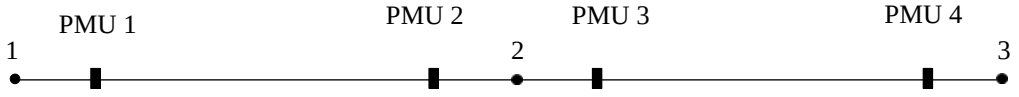

Рис. 1. Фрагмент схемы электрической сети.

На рис. 2, 3 представлены поток измерений напряжения и его гистограмма распределения по нормальному закону. Число измерений $n = 30000$ с интервалом дискретизации $\Delta t = 20$ мс. Результаты вейвлет-анализа показали, что измерения напряжения не содержат грубых ошибок.

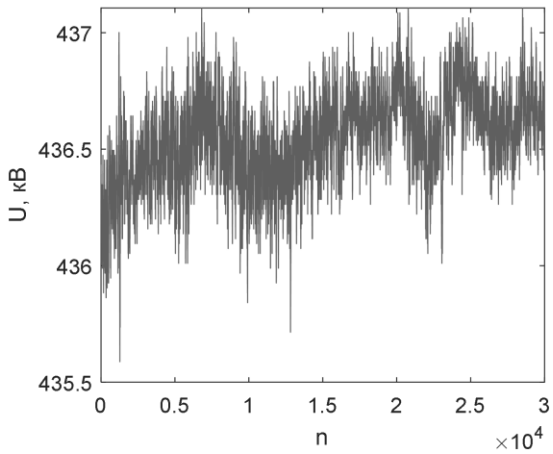

Рис. 2. Измерения напряжения, не содержащие грубых ошибок.

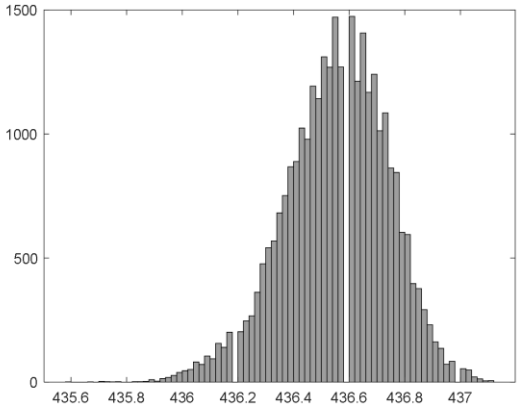

Рис. 3. Гистограмма распределения.

На поток измерения напряжения была сгенерирована атака в виде наложения шума $a(t) = \xi_{KA1}(t) \to N(0, \sigma_a^2)$ (рис. 4, 5).

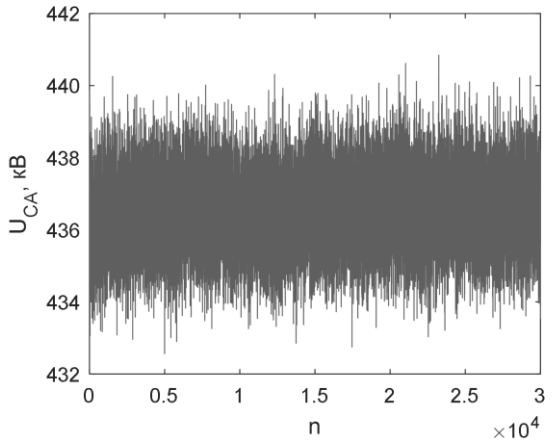

Рис. 4. Поток измерений напряжения при успешно реализованной кибератаке в виде наложения шума.

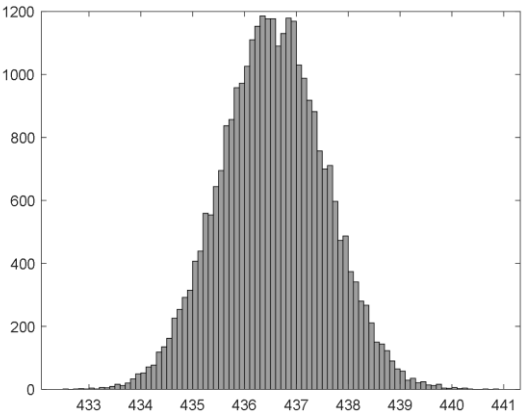

Рис. 5. Гистограмма распределения.

Достоверизация данных проведена путем применения вейвлет-преобразований (фильтрация шумов, восстановление) потока измерений напряжения U_{CA} (рис.6, 7).

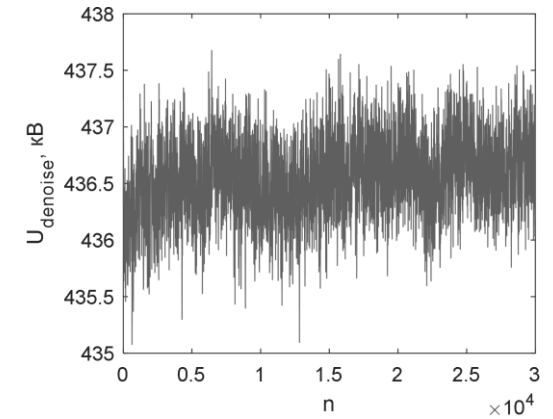

Рис. 6. Восстановленный поток измерений напряжения.

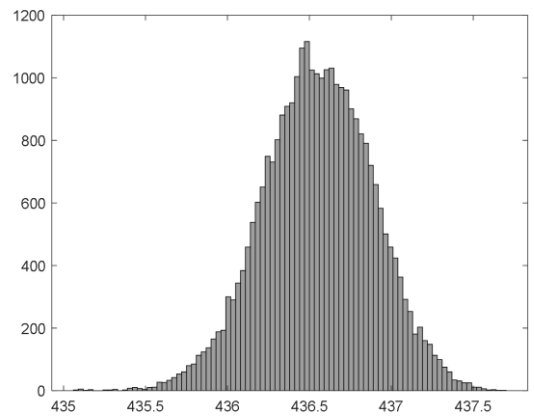

Рис. 7. Гистограмма распределения.

В результате проведенного вейвлет-анализа получены характеристики (математическое ожидание m_U, минимальное min_U и максимальное max_U значения, среднее квадратическое отклонение σ_U) изменения напряжения (табл. 1), требуемые для нахождения параметров нечетких чисел.

Таблица 1. Характеристики изменения напряжения

	U	U_{CA}	$U_{denoise}$
m_U	436.6	436.6	436.6
min_U	435.6	432.6	435.1
max_U	437.1	440.8	437.7
σ_U	0.19	1	0.33

Параметры нечетких чисел для потоков измерений напряжения $\widetilde{U}$, $\widetilde{U}_{CA}$, $\widetilde{U}_{denoise}$ (табл. 2) определялись согласно выражениям (1)-(4).

Таблица 2. Параметры нечетких чисел потоков измерения напряжения

	U	U_{CA}	$U_{denoise}$
z_1	435.6	432.6	435.1
z_2	436.4124	432.6	436.105
z_3	436.6938	440.8	436.96
z_4	437.1	440.8	437.7

Согласно найденным параметрам нечетких чисел сформированы их трапецеидальные функции принадлежностей (рис. 8-10).

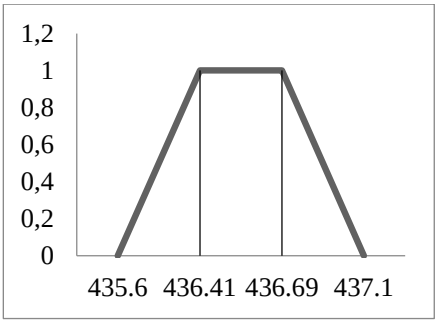

Рис. 8. Функция принадлежности нечеткого числа $\widetilde{U}$.

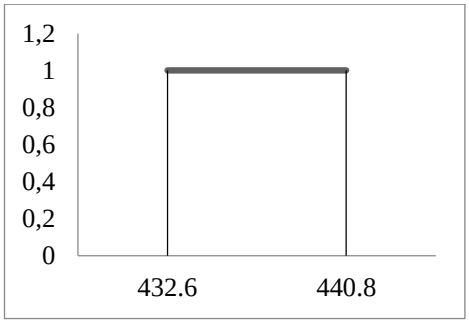

Рис. 9. Функция принадлежности нечеткого числа $\widetilde{U}_{CA}$.

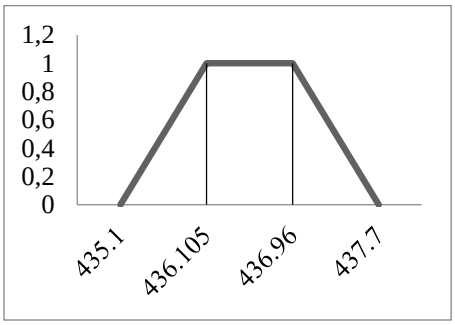

Рис. 10. Функция принадлежности нечеткого числа $\widetilde{U}_{denoise}$.

Сравнительный анализ полученных результатов (табл. 3) показал целесообразность применения вейвлет-анализа процессов изменения переменных режима при кибератаках на информационно-коммуникационную инфраструктуру, снижающих степень достоверности информации. Его применение позволяет устранить влияние искажающих факторов на параметры нечетких чисел, тем самым снижая неопределенность данных.

Таблица 3. Сравнительный анализ полученных результатов

	$\Delta = \widetilde{U} - \widetilde{U}_{CA}$	$\Delta = \widetilde{U} - \widetilde{U}_{denoise}$
v_1	3	0,5
v_2	3,8124	0,3074
v_3	-4,1062	-0,2662
v_4	-3,7	-0,6

Совокупное применение вейвлет-анализа и нечеткой логики при обработке данных увеличивает степень полноты и достоверности информации.

Заключение. Предложенный алгоритм обработки информации на основе вейвлет-анализа и нечеткой логики позволяет повысить точность измерений, необходимых для решения оценивания состояния ЭЭС и, тем самым, обеспечивая надежное управление ЭЭС. Использование нечеткой логики позволяет перейти к интервальным вычислениям при оценивании состояния ЭЭС в условиях неопределенности, вызванной потерей информации при кибератаках на информационно-коммуникационную инфраструктуру ЭЭС, что является предметом дальнейших исследований.

Работа выполнена в рамках научного проекта III.17.4.2. программы фундаментальных исследований СО РАН, рег. № АААА-А17-117030310438-1 и при частичной поддержке гранта РФФИ (№19-07-00351 А)

СПИСОК ЛИТЕРАТУРЫ

1. Воропай Н.И. Направления и проблемы трансформации электроэнергетических систем // Электричество. 2020. № 7. С. 12-21.

2. Гамм А.З., Колосок И.Н. Обнаружение грубых ошибок телеизмерений в электроэнергетических системах. – Новосибирск: Наука. 2000. 152 с.

3. 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.

4. 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.

5. Kolosok I., Gurina L. Wavelet Analysis of PMU Measurements for Identification of Cyber Attacks on TCMS // 2018 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), Moscow, Russia. 2018. Pp. 1-4. doi: 10.1109/ICIEAM.2018.8728768.

6. Kyung Choi, Xinyi Chen, Shi Li, Mihui Kim, Kijoon Chae and JungChan Na. Intrusion Detection of NSM Based DoS Attacks Using Data Mining in Smart Grid // Energies. 2012. No 2. Pp. 4091-4109. doi:10.3390/en5104091.

7. L. Hu, Z. Wang, X. Liu, A. V. Vasilakos and F. E. Alsaadi. Recent advances on state estimation for power grids with unconventional measurements // in *IET Control Theory & Applications*. 2017. Vol. 11. № 18. Pp. 3221-3232. doi: 10.1049/iet-cta.2017.0629
8. M. Yasinzadeh and M. Akhbari. Detection of PMU spoofing in power grid based on phasor measurement analysis // in *IET Generation, Transmission & Distribution*. 2018. Vol. 12.
№ 9. Pp. 1980-1987. doi: 10.1049/iet-gtd.2017.1445.
9. S. Sridhar, A. Hahn and M. Govindarasu. Cyber–Physical System Security for the Electric Power Grid // in *Proceedings of the IEEE*. 2012. Vol. 100. № 1. Pp. 210-224. doi: 10.1109/JPROC.2011.2165269.
10. Uluçay V., Deli I., Şahin M. Trapezoidal fuzzy multi-number and its application to multi-criteria decision-making problems // *Neural Comput & Applic.* 2018. № 30. Pp 1469–1478. https://doi.org/10.1007/s00521-016-2760-3
11. V. Miranda, J. Pereira, and J. T. Saraiva. Load allocation in DMS with a fuzzy state estimator // IEEE Trans. Power Syst. 2000. vol. 15. № 2. Pp. 529–534.

UDK 621.311 : 004.056

PROCESSING OF SYNCHRONOUS PHASOR MEASUREMENTS BY FUZZY LOGIC METHODS IN THE CASE OF CYBERATTACKS ON INFORMATION-COMMUNICATION INFRASTRUCTURE OF A CYBER-PHYSICAL ELECTRIC POWER SYSTEM [3]

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 use of intelligent and digital technologies in systems for measuring, transmitting, and processing information, which are part of the information-communication infrastructure, is aimed at improving the efficiency of EPS management. At the same time, with the EPS digitalization, there has been a rise in vulnerabilities to cyberattacks. In this context, the urgency of providing timely, complete, and reliable data to perform control in the case of cyberattacks is increasing. We propose an algorithm to process synchronized vector measurements based on wavelet analysis and fuzzy logic, which improves the quality of information used in the state estimation of electric power systems.

Keywords: quality of data, PMU measurements, cyberattacks, wavelet analysis, fuzzy logic.

[3] This study is supported by the Siberian Branch of the Russian Academy of Sciences (Project III.17.4.2) of the Federal Program of Scientific Research (No. AAAAA-A17-117030310438-1)

References

1. Voropaj N.I. Napravleniya i problemy transformacii elektroenergeticheskih system [Prospects and problems of electric power system transformations] // Elektrichestvo=. 2020. № 7. Pp. 12-21. (in Russian)

2. Gamm A.Z., Kolosok I.N. Obnaruzhenie grubyh oshibok teleizmerenij v elektroenergeticheskih sistemah [Bad data detection in measurements in electric power systems]. Novosibirsk: Nauka = Science. 2000. 152 p.

3. Kolosok I.N., Gurina L.A. Ocenka kachestva dannyh SCADA i WAMS pri kiberatakah na informacionno-kommunikacionnuyu infrastrukturu EES. Informacionnye i matematicheskie tekhnologii v nauke i upravlenii [Quality assessment of SCADA and WAMS data in the case of cyberattaks on information and communication infrastructure of EPS] // 2020. № 1 (17). Pp. 68-78. (in Russian)

4. 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.

5. Kolosok I., Gurina L. Wavelet Analysis of PMU Measurements for Identification of Cyber Attacks on TCMS // 2018 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM*)*, Moscow, Russia. 2018. Pp. 1-4. doi: 10.1109/ICIEAM.2018.8728768. (in Russian).

6. Kyung Choi, Xinyi Chen, Shi Li, Mihui Kim, Kijoon Chae and JungChan Na. Intrusion Detection of NSM Based DoS Attacks Using Data Mining in Smart Grid // Energies. 2012. № 2. Pp. 4091-4109. doi:10.3390/en5104091.

7. L. Hu, Z. Wang, X. Liu, A. V. Vasilakos and F. E. Alsaadi. Recent advances on state estimation for power grids with unconventional measurements // in *IET Control Theory & Applications*. 2017. Vol. 11. № 18. Pp. 3221-3232. doi: 10.1049/iet-cta.2017.0629

8. M. Yasinzadeh and M. Akhbari. Detection of PMU spoofing in power grid based on phasor measurement analysis // in *IET Generation, Transmission & Distribution*. 2018. Vol. 12.

№ 9. Pp. 1980-1987. doi: 10.1049/iet-gtd.2017.1445

9. S. Sridhar, A. Hahn and M. Govindarasu. Cyber–Physical System Security for the Electric Power Grid // in *Proceedings of the IEEE*. 2012. Vol. 100. № 1. Pp. 210-224. doi: 10.1109/JPROC.2011.2165269.

10. Uluçay V., Deli I., Şahin M. Trapezoidal fuzzy multi-number and its application to multi-criteria decision-making problems // *Neural Comput & Applic.* 2018. № 30. Pp 1469–1478. https://doi.org/10.1007/s00521-016-2760-3

11. V. Miranda, J. Pereira, and J. T. Saraiva. Load allocation in DMS with a fuzzy state estimator // IEEE Trans. Power Syst. 2000. vol. 15. № 2. Pp. 529–534.