УДК 620.91
DOI 10.51691/2541-8327_2021_5_3

МОНИТОРИНГ И АНАЛИЗ ДАННЫХ SCADA И WAMS ДЛЯ ЦИФРОВИЗАЦИИ EPS

Наумов И.И.
к.т.н., доцент,
Институт Сферы Обслуживания и Предпринимательства (филиал) Донской государственный технический университет в г. Шахты
Россия, Шахты
Тарасюк М. А.
Студент
Институт Сферы Обслуживания и Предпринимательства (филиал) Донской государственный технический университет в г. Шахты
Россия, Шахты
Моторин Д. Е.
Студент
Институт Сферы Обслуживания и Предпринимательства (филиал) Донской государственный технический университет в г. Шахты
Россия, Шахты

Аннотация:
Свойства электроэнергетических систем (ЭЭС) в настоящее время находятся в процессе цифровой трансформации, что необходимо учитывать при управлении ими. Несмотря на многочисленные преимущества цифрового перехода, все еще существуют проблемы с качеством данных, используемых для управления EPS, и они в большей степени связаны с угрозами кибербезопасности для информационно-коммуникационной инфраструктуры EPS. В статье показано влияние изменений свойств кибербезопасности информационно-коммуникационной инфраструктуры на качество потоков данных, поступающих от SCADA и WAMS, и выявлено их сложное взаимодействие. Возникла потребность в оценке качества данных вовремя кибератак на системы

сбора, передачи и обработки информации. Предлагается алгоритм оценки качества измерений на основе нечеткой логики.
Ключевые слова: Качество данных, SCADA, WAMS, Киберфизическая система, нечеткая логика.

MONITORING AND ANALYSIS OF SCADA AND WAMS DATA FOR EPS DIGITALIZATION

Naumov I.I.
Ph.D., associate professor,
Institute of Service and Entrepreneurship (branch) Don State Technical University in Shakhty
Russia, Shakhty
Tarasyuk M.A.
Student
Institute of Service and Entrepreneurship (branch) Don State Technical University in Shakhty
Russia, Shakhty
Motorin D.E.
Student
Institute of Service and Entrepreneurship (branch) Don State Technical University in Shakhty
Russia, Shakhty

Abstract:
The properties of electric power systems (EPSs) are currently in the process of digital transformation, which should be taken into account when controlling them. Despite the numerous advantages of the digital transition, there are still problems with quality of the data used to control the EPS, and they are to a greater extent associated with the cybersecurity threats to the EPS information and communication infrastructure. The paper demonstrates the effect of changes in cybersecurity properties of the

information and communication infrastructure on the quality of data streams coming from SCADA and WAMS, and reveals their complex interaction. The need has arisen to assess the quality of data during cyberattacks on systems for collecting, transmitting and processing the information. An algorithm is proposed to assess the quality of measurements based on the fuzzy logic.

Keywords: Quality of data, SCADA, WAMS, Cyber-physical system, fuzzy logic.

Введение

Переход к моделям киберфизических электроэнергетических систем (ЭЭС) обусловлен цифровой трансформацией электроэнергетики, процессами взаимодействия, в которых используются новые информационные и коммуникационные технологии, и цифровыми моделями [1]. Киберфизическая система приобретает новые свойства и отличительные особенности, которые необходимо учитывать для управления ею. В этом контексте такие системы не только продолжают сталкиваться с проблемами стабильности с точки зрения кибербезопасности, но эти проблемы становятся еще более выраженными с точки зрения требований к надежности из-за повышенной уязвимости к кибератакам на информационные и коммуникационные подсистемы [2,3]. Актуальность обеспечения управления EPS своевременной и надежной информацией подчеркивается необходимостью разработки новых методов и моделей представления данных на основе технологий искусственного интеллекта.

В настоящее время управление электроэнергетической системой основано как на измерениях SCADA, так и на синхронизированных векторных измерениях, поступающих с измерительных устройств WAMS. Качество измерений SCADA и WAMS имеет решающее значение не только для разработки автоматизированных систем управления, но и для бесперебойной работы САЭ. Под качеством информационных потоков данных понимается степень полноты и достоверности информации, обеспечивающей требуемую

точность в управлении ЭПС.

В статье предлагается метод обработки измерительной информации, основанный на теории нечетких множеств, с учетом таких требований кибербезопасности системы SCADA и WAMS, как своевременность, целостность, доступность, а также киберустойчивость и конфиденциальность [4]. Разработка подхода включала анализ киберфизических свойств системы и выявление возможных кибератак, снижающих качество информационных потоков данных.

В статье показано, что неполнота и неточность информации возрастают из-за кибератак на систему SCADA и WAMS, что может привести к разработке и внедрению некорректных управляющих воздействий и неблагоприятным последствиям для работы ЭЭС [4].

В предлагаемом методе разработан алгоритм анализа рабочих параметров на основе нечетких правил. Этот алгоритм также может быть использован в качестве предварительного этапа обработки данных в качестве барьера для "плохих" данных при оценке состояния EPS.

В предлагаемом методе разработан алгоритм анализа рабочих параметров на основе нечетких правил. Этот алгоритм также может быть использован в качестве предварительного этапа обработки данных в качестве барьера для "плохих" данных при оценке состояния EPS.

Использование технологий искусственного интеллекта при анализе и обработке информационных потоков повысит эффективность управления и надежность ЭПС.

Цифровая трансформация свойств киберфизических электроэнергетических систем

В России, как и в других странах, развитие ЭПС направлено на создание киберфизической системы на основе единой цифровой среды (модель CIM), а также внедрение технологий кибербезопасности и интеллектуальных методов управления с целью повышения надежности и прозрачности ЭПС. операция. CIM (общая информационная модель), основанная на формате данных ODM

(открытая модель для обмена данными моделирования энергосистемы), позволяет строить модели любой сложности, которые затем могут быть преобразованы в любой известный формат данных или любой новый формат данных с помощью дополнительных плагинов. ODM - это открытая модель обмена данными при моделировании энергосистем. ODM - это международный открытый стандарт обмена данными при моделировании и расчете EPS, который поддерживает динамические расчеты [5]. Основанная на моделях CIM, ИТ-инфраструктура, объединяющая интеллектуальные информационные, вычислительные и телекоммуникационные среды, должна обеспечивать двустороннюю связь между информационно-коммуникационной и технологической подсистемами киберфизической EPS.

Прозрачность работы ЭПС требует внедрения новых систем сбора, передачи и обработки информационных потоков; разработка технологий и методов моделирования исследуемых процессов и получения достоверных данных в режиме реального времени об условиях эксплуатации для управления ЭЭС.

Переход к интеллектуальному управлению ЭЭП и растущие потребности в мониторинге и анализе данных требуют технологий цифровой обработки данных, основанных на методах искусственного интеллекта:

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

Несмотря на все очевидные преимущества цифровизации электроэнергетических систем, она делает их более уязвимыми для кибератак, что связано с крупномасштабностью (включая пространственную фрагментацию) технологической части и многокомпонентностью (устройства для сбора, передачи и обработки информации). на всех уровнях управления) информационно-коммуникационной инфраструктуры киберфизических ЭЭО и их информационного взаимодействия. На уровне аппаратной и программной

поддержки контроля растет риск возникновения скрытых угроз. Интеграция технологий ИТ-инфраструктуры способствует увеличению количества кибератак [4].

Управление EPS основано на данных из SCADA и WAMS. Кибератаки, направленные на компоненты этих систем или двусторонние потоки данных информационно-коммуникационных и технологических систем, могут нарушить не только функции управления, но и вызвать сбои в работе САЭ.

Исследование [4] демонстрирует влияние низкого качества информации, которое приводит к ложной визуализации условий работы ЭПС и генерации некорректных управляющих действий из-за кибератак на систему SCADA и WAMS. Анализ качества данных может определить тип кибератаки и выявить пропущенные уязвимости.

Качество потоков данных системы SCADA и WAMS

Крупномасштабный мониторинг EPS включает в себя как систему SCADA, так и WAMS, в которой измерения поступают с устройств PMU. В этих условиях можно управлять EPS на основе

- измерения SCADA;
- измерения WAMS;
- Смешанные измерения.

Технологии синхронизированных векторных измерений могут повысить наблюдаемость системы и предоставить более точную и своевременную информацию для контроля.

Под качеством информационных потоков данных понимается степень полноты и достоверности информации, обеспечивающей требуемую точность решений для управления режимами работы ЭЭС.

В [6] информация для управления EPS классифицируется следующим образом:

- детерминированный;
- вероятностный;
- неуверенный.

Детерминированная информация основана на законах причинно-следственных связей и обусловлена численно однозначной спецификацией типов оборудования, его состава и номинальных параметров.

Вероятностная информация описывает стохастический характер изменения рабочего режима, совокупности компонентов электрической сети, что соответствует заданному поведению ЭЭС.

Неопределенная информация делится на четыре группы:

– двусмысленный;
– неизвестный;
– недостаточный;
– ненадежный.

Под неоднозначностью информации понимается ее многовариантность из-за различных методов, используемых для ее получения и описания. Отсутствие информации о компонентах и рабочих параметрах из-за технических и физических факторов приводит к неопределенности. Различные степени, в которых информация неизвестна или недостаточна, отражают неполноту информации. Информационная недостоверность возникает при несоответствии модели моделируемому процессу, при наличии ошибок измерения, неточности данных и т.д.

Однако совместное использование измерений SCADA и WAMS требует решения следующих задач:

– высокая вычислительная нагрузка;
– большое количество данных;
– слабая обусловленность ковариационных матриц.

Возникают серьезные проблемы качества данных и кибербезопасности, которые имеют сложное взаимодействие. Например, снижение качества данных может быть следствием успешной кибератаки. В то же время анализ качества данных может определить тип кибератаки и выявить упущенные из виду уязвимости [7]. Для проверки свойств кибербезопасности необходимо разработать методы анализа качества данных SCADA и WAMS.

В связи с этим влияние кибератак на качество данных было проанализировано с учетом нарушений свойств кибербезопасности [8] (рис. 1).

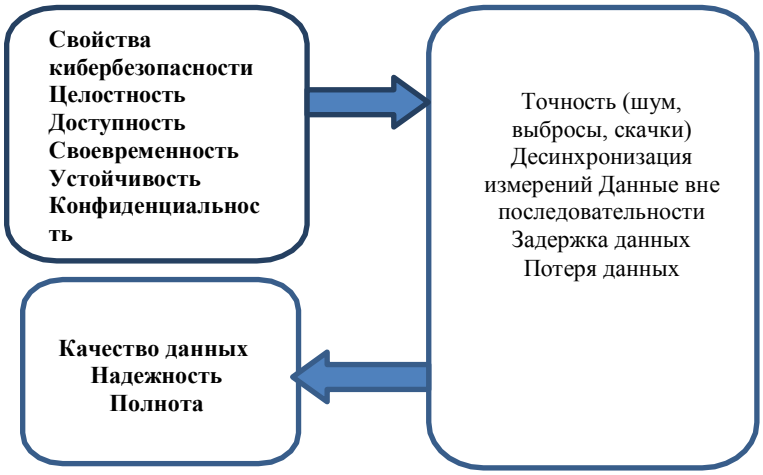

Рис. 1. Влияние кибератак на качество данных.[1]

В [5] введены критерий качества информации и метод его определения на основе теории нечетких множеств. Авторы [9] в зависимости от уровня полноты и достоверности измерений SCADA и WAMS предлагают измерительные модели для оценки состояния ЭЭС. Рассмотрение влияния кибератак на полноту и надежность информации потребовало расширения списка факторов для оценки качества данных. В исследовании [10–14] исследуются возможные кибератаки на системы сбора, передачи и обработки информации, выявляются их уязвимости и показано, как нарушения свойств кибербезопасности систем SCADA и WAMS влияют на функции управления EPS [4].

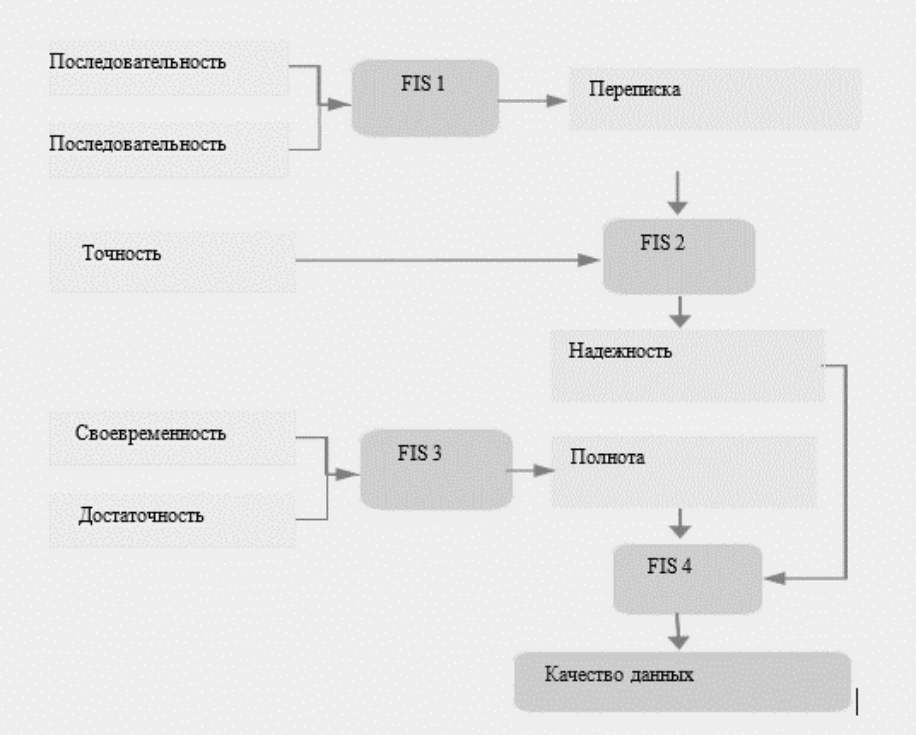

Рис. 2. Нечеткая система оценки качества данных.[1]

Тематическое исследование

Построена нечеткая система оценки качества информации с учетом проблем оценки состояния ЭПС.

Эти исследования указывают на необходимость учета следующих факторов воздействия кибератаки на систему SCADA и WAMS на качество данных:

- последовательность;
- своевременность данных;
- согласованность данных.

Своевременность данных в реальном времени отражает неопределенность информации. При совместном использовании измерений SCADA и PMU необходимо учитывать согласованность данных.

Нечеткая система обработки потоков данных с учетом свойств кибербезопасности SCADA-системы и WAMS.

Предлагаемый алгоритм оценки качества данных основан на следующем

алгоритме:

1. Определить уровень достоверности информации;
2. Определить уровень полноты информации;
3. Оцените качество информации.

Чтобы определить уровни надежности и полноты информации, мы указываем лингвистические переменные (точность, последовательность, согласованность, своевременность, адекватность), определяем наборы терминов и даем их семантическое определение. Разработана нечеткая система защиты от кибератак на системы SCADA и WAMS [15, 16].

Семантическое описание входных и выходных лингвистических переменных представлено в таблицах 1-4.

Таблица 1. Уровни факторов, влияющих на достоверность информации.

Уровень	**Точность**	**Следствие**	**Последовательность**
Низкий 0-0,25	В измерениях есть ошибки из-за кибератак, в том числе не обнаруживаемых.	Последовательность нарушена	Данные не согласованы
Средний 0,25-0,75	Измерения содержат ошибки из-за кибератак, которые могут быть обнаружены с помощью обнаружения неверных данных. методы	Последовательность нарушена, но есть возможность исключения (дублирование, сравнение)	Данные не согласованы, но есть возможность дублирования и восстановления.
Высокая 0,75-1	Измерения содержат погрешности, связанные с погрешностями измерительных приборов и т.д, Не влияющие на точность оценки состояния ЭЭС.	Последовательность не нарушена	Данные согласованы

Таблица 2. Уровни факторов, влияющих на полноту информации.

Уровень	**Своевременность**	**Достаточность**
Низкий 0-0,25	Большая задержка	Нет данных
Средний 0,25-0,75	Отсрочка с возможностью рассмотрения в модели измерения	Потеря данных несущественна для решения проблемы
Высокая 0,75-1	Измерения приходят без задержек	Достаточное количество измерения получены

Таблица 3. Полнота и достоверность данных.

Уровень	Полнота	Надежность
Низкий 0-0,25	Система не наблюдается	Сомнительный
Средний 0,25-0,75	Возможность расчета недостающих значений измерений	Ошибочный
Высокая 0,75-1	Чрезмерные измерения	Надежный

Таблица 4. Качество данных.

Уровень	Качество
Низкий 0-0,25	Сеть ненаблюдаема и / или измерения ненадежны
Средний 0,25-0,75	Использование методов обнаружения недостоверных данных, валидации измерений, ошибок фильтрации, восстановления потоков измерений, учета старения информации позволит оценить состояние EPS с требуемой точностью.
Высокая 0,75-1	Полный надежный поток информации

На рисунках 3-5 показаны полученные трехмерные поверхности полноты, достоверности и качества информации.

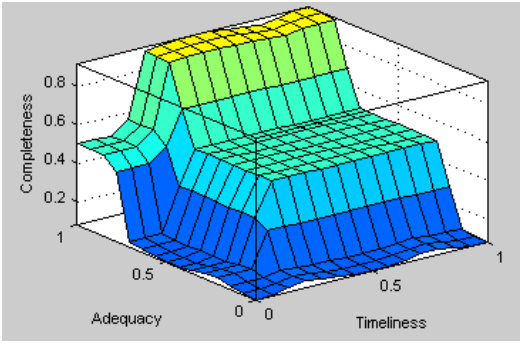

Рис. 3. Нечеткая система оценки качества данных.[3]

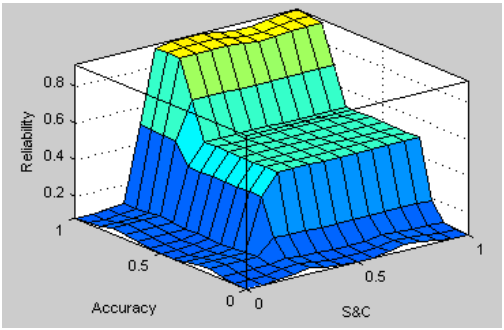

Рис. 4. Зависимость достоверности информации от точности, последовательности и согласованности данных.[3]

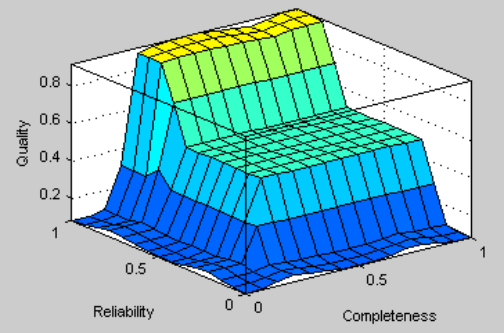

Рис. 5. Качество измерений.[3]

Как видно из графиков, низкий уровень любого из входных факторов, вызванный кибератаками, влияет на качество информации (синий цвет), особенно это влияет на надежность измерений.

Это обосновывает необходимость анализа данных при решении задачи оценки состояния с учетом дополнительных факторов как предварительного этапа обработки данных.

Заключение

Анализируются свойства ЭПС, связанные с созданием киберфизической системы. Исследования показали повышенную уязвимость таких систем к кибератакам на информационно-коммуникационную инфраструктуру.

Показана взаимозависимость между свойствами кибербезопасности системы SCADA и WAMS и качеством измерений. Предлагается алгоритм оценки качества данных при нарушениях свойств кибербезопасности в качестве предварительного этапа оценки состояния ЭПС.

Библиографический список:

1. Массель Л.В. Энергетическая политика 5, 30-42 (2018) [Электронный ресурс]. — Режим доступа — URL: http://www.energystrategy.ru/editions/source/ep52018_5.html (дата обращения 10.04.2021).

2. Шридхар С., Хан А., Говиндарасу М. ISGT (Вашингтон, округ Колумбия, 2012 г.) [Электронный ресурс]. — Режим доступа — URL: https://www.mdpi.com/2079-9292/10/9/1043/pdf (дата обращения 10.04.2021).

3. Шридхар С., Хан А., Говиндарасу М. Материалы IEEE. 100, 210-224. (2012) [Электронный ресурс]. — Режим доступа — URL:

https://ieeexplore.ieee.org/document/6032699 (дата обращения 10.04.2021).

4. Колосок И., Гурина Л. Методологические проблемы исследования надежности крупных энергетических систем (Ташкент, Узбекистан, 2019). [Электронный ресурс]. — Режим доступа — URL: http://www.energetik.energy-journals.ru/index.php/EN/article/view/1320/0 (дата обращения 10.04.2021).

5. Кобец Б. Б., Волкова И. О. Инновационное развитие электроэнергетики на базе концепции Smart Grid. — М.: ИАЦ Энергия, 2010. — 208 с [Электронный ресурс]. — Режим доступа — URL: https://publications.hse.ru/mirror/pubs/share/folder/skziecw02u/direct/71906761 (дата обращения 10.04.2021).

6. Савина Н.В., Гурина Л.А. Энергетика: управление, качество и эффективность использования энергии (Благовещенск, Россия, 2003). [Электронный ресурс]. — Режим доступа — URL: https://textarchive.ru/c-1854814.html (дата обращения 10.04.2021).

7. Колосок И., Гурина Л. Промышленное проектирование, применение и производство (Москва, Россия, 2018). [Электронный ресурс]. — Режим доступа — URL: https://www.semanticscholar.org/author/I.-Kolosok/48091401 (дата обращения 10.04.2021).

8. Колосок И.Н., Гурина Л.А. ОЦЕНКА РИСКОВ КИБЕРБЕЗОПАСНОСТИ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ ИНТЕЛЛЕКТУАЛЬНОЙ ЭНЕРГЕТИЧЕСКОЙ СИСТЕМЫ // Information and mathematical technologies in science and management. -2019. - №2 (14). – С. 40-51 [Электронный ресурс]. — Режим доступа — URL: https://www.imt-journal.ru/archive/public/downloadFromArticle?article_id=82&file_id=89 (дата обращения 10.04.2021).

9. Колосок, И. Н. Прогнозирование параметров режима при мониторинге и управлении электроэнергетической системой / И. Н. Колосок, Л. А. Гурина // Электричество. – 2014. – № 1. – С. 21-27. - [Электронный ресурс]. — Режим доступа — URL: https://lib-db.kuzstu.ru/input/baseview.php?id=21667 (дата обращения 10.04.2021).

10. Лин Х., Дэн И., Сандип Шукла, Джеймс Торп, Ламин Мили, Smart Grid Communications (2012) [Электронный ресурс]. — Режим доступа — URL: https://search.rsl.ru/ru/record/01006606378 (дата обращения 10.04.2021).

11. К. Гай, М. Цю, З. Мин, Х. Чжао, Л. Цю, IEEE Transactions on Smart Grid 8 (5), 2431-2439 (2017) [Электронный ресурс]. — Режим доступа — URL: https://ieeexplore.ieee.org/document/8013904?denied= (дата обращения 10.04.2021).

12. Лунфэй Вэй, Луис Пуше Рондон, Амир Могхадаси, Ариф И.

Сарват, T&D (2018) [Электронный ресурс]. — Режим доступа — URL: https://www.semanticscholar.org/author/Longfei-Wei/2448576 (дата обращения 10.04.2021).

13. Мохд Рихан, Мухтар Ахмад, М. Салим Бег, Умные сети и возобновляемые источники энергии (2013 г.) [Электронный ресурс]. — Режим доступа — URL: https://file.scirp.org/pdf/SGRE_2013090316323131.pdf (дата обращения 10.04.2021).

14. С. Шридхар, А. Хан и М. Говиндарасу, ISGT (Вашингтон, округ Колумбия, 2012 г.) [Электронный ресурс]. — Режим доступа — URL: https://www.semanticscholar.org/author/S.-Sridhar/46804466 (дата обращения 10.04.2021).

15. Яо Лю, Пэн Нин, Майкл К. Рейтер, CCS'09 (Чикаго, Иллинойс, США, 2009 г.) [Электронный ресурс]. — Режим доступа — URL: https://www.semanticscholar.org/author/Yao-Liu/23942578 (дата обращения 10.04.2021).

16. Зануз С., Роджерс К. М., Бертье Р., Бобба Р. Б., Сандерс В. Х., Оверби Т. Дж., IEEE Transactions on Smart Grid 3, 1790-1799 (2012) [Электронный ресурс]. — Режим доступа — URL: https://www.semanticscholar.org/author/R.-Berthier/3006588 (дата обращения 10.04.2021).

Оригинальность 75%