Электричество, 2021, № 6, с. 25–32 *DOI:10.24160/0013-5380-2021-6-25-32*

Идентификация кибератак на системы *SCADA* и *СМПР* в ЭЭС при обработке измерений методами оценивания состояния

КОЛОСОК И.Н., ГУРИНА Л.А.
ИСЭМ СО РАН, Иркутск, Россия

Технические и программные средства систем сбора и обработки информации и задача оценивания состояния, предназначенные для поддержки действий диспетчерского персонала при оперативном и противоаварийном управлении электроэнергетическими системами, являются критически важными и в то же время наиболее уязвимыми к кибератакам компонентами информационно-коммуникационной подсистемы. Для снижения степени влияния кибератак на качество управления предлагается использовать статистические методы обработки измерительной информации. В первую очередь, это методы статического и динамического оценивания состояния, включающие процедуру достоверизации измерений или обнаружения плохих данных. Вместе с тем анализ качества данных может определить тип реализованной кибератаки и выявить неучтенные уязвимости. В статье приведены результаты исследования двух наиболее распространенных методов достоверизации измерений: априорного метода анализа невязок контрольных уравнений и апостериорного метода анализа взвешенных остатков оценивания для идентификации данных, искаженных вследствие сгенерированных специальным образом кибератак. Предложен алгоритм обнаружения ошибочных измерений, возникающих при кибератаках и не идентифицируемых традиционными методами достоверизации измерений при оценивании состояния энергосистемы.

Ключевые слова: *SCADA, СМПР, кибератака, качество данных, достоверность, полнота, обнаружение плохих данных, нечеткие множества, вейвлет-анализ*

Усовершенствование информационно-коммуникационной инфраструктуры при цифровизации электроэнергетической системы (ЭЭС) обеспечивается развитием сенсорных и сетевых технологий на основе внедрения цифрового оборудования, применения интеллектуальных устройств в системах измерения, обработки и передачи информации, требуемой для управления функционированием ЭЭС. Благодаря этому повышается эффективность и гибкость управления и мониторинга ЭЭС [1]. Развитая инфраструктура ЭЭС имеет сложное взаимодействие информационно-коммуникационной и физической подсистем, надежное обеспечение которого при цифровизации ЭЭС все больше зависит от внутренних и внешних воздействий в результате кибератак на системы сбора, обработки и передачи информации. Снижение качества измерений, используемых при управлении, при успешно реализованных киберугрозах на киберфизические ЭЭС отрицательно сказывается на результатах оценивания состояния ЭЭС вследствие не обнаруживаемых традиционными методами поиска ошибочных измерений [2, 3], отсутствия достаточного объема измерений [4].

Целью исследований является разработка алгоритма анализа качества измерений программно-аппаратными комплексами сбора данных и диспетчерского контроля *SCADA* (*Supervisory Control and Data Acquisition*) и *СМПР* (Система мониторинга переходных режимов) при кибератаках на компоненты информационно-коммуникационной подсистемы ЭЭС, как предварительный этап оценивания состояния ЭЭС.

Оценивание состояния (ОС) включает в себя выполнение таких функций, как анализ наблюдаемости ЭЭС, обработка конфигурации сети (топологический анализ сети), идентификация и фильтрация «плохих данных», дорасчет неизмеренных параметров [5]. Для получения корректных оценок всех переменных режима важную роль играет избыточность измерений. При низкой избыточности возникает проблема критических измерений, ошибки в которых нельзя выявить традиционными методами обнаружения плохих данных (ОПД) [6]. В современных комплексах ОС, работающих в темпе обработки данных для задач управления, преимущество отдается методам априорного анализа, которые работают независимо от алгоритма ОС и позволяют обнаружить плохие данные до решения задачи ОС. Для повышения надежности результатов ОС и киберустойчивости программно-вычислительных комплексов (ПВК) ОС априорные методы дублируются апостериорными, которые выявляют плохие данные по результатам оценивания. Эти методы и рассмотрены в статье: априорный метод, построенный на анализе невязок контрольных уравнений, и апостериорный метод анализа взвешенных остатков ОС.

Использование синхронизированных векторных измерений (СВИ) наряду с измерениями *SCADA* позволило существенно улучшить ситуацию, связанную с «плохими данными» и достоверизацией измерений [7]. Тем не менее, известно, что при определенных сочетаниях множественных ошибочных измерений плохие данные могут не обнаруживаться методами ОС [5,8]. Проблема создания фальсифицированных вследствие кибератак наборов измерений, не детектируемых различными методами ОС, впервые была поставлена в работе [2] и затем широко исследована как в зарубежных [9–12], так и отечественных работах [13–15].

В статье проведен анализ качества измерений *SCADA* и *СМПР* при кибератаках на информационно-коммуникационную инфраструктуру ЭЭС. Предложен алгоритм обнаружения ошибочных измерений при недостоверных данных на основе вейвлет-анализа и теории нечетких множеств. Реализация данного алгоритма продемонстрирована при смоделированных кибератаках.

Качество измерений SCADA и СМПР. Внедрение новых информационных и коммуникационных технологий при трансформации ЭЭС в Smart Grid (интеллектуальная электроэнергетическая система) позволило обеспечить системы управления наряду с измерениями *SCADA* высокоточными синхронизированными по времени измерениями.

На практике взаимозависимость информационно-коммуникационной и физической подсистем киберфизической ЭЭС связана с такими ограничениями, как качество и безопасность данных. Надежное функционирование ЭЭС может быть нарушено из-за неполноты и недостоверности измерений *SCADA* и СМПР.

Под качеством данных понимается степень их полноты и достоверности [16].

При цифровизации ЭЭС по-прежнему важно принимать во внимание проблемы качества данных для приложений *EMS* (*Energy Management System*), используемых при управлении ЭЭС, в связи с возрастающими угрозами реализации внешних и внутренних возмущающих воздействий с позиций кибербезопасности и особенностей существующих систем сбора, передачи и обработки измерений, поступающих от измерительных устройств *RTU* (*Remote Terminal Unit*) системы *SCADA* и устройств для СВИ (УСВИ) СМПР.

Успешно реализованные кибератаки на компоненты информационно-коммуникационной инфраструктуры существенно влияют на качество измерений, используемых при управлении ЭЭС (табл. 1). В [16] показана взаимозависимость нарушения свойств кибербезопасности и снижения качества данных.

Для идентификации последствий успешно проведенных кибератак выделены такие факторы, как точность, достаточность, своевременность, синхронизированность, согласованность и последовательность, характеризующие качество измерений.

Достоверность требует точности и синхронизации по времени измерений в пределах допустимых ошибок без нарушения последовательности поступления данных. При оценке точности необходим учет такого фактора, как согласованность измерений. Полнота характеризуется доступностью данных и требует, чтобы данные измерений были без потерь и своевременными, т.е. доставленными с допустимыми задержками.

В [16] на основе разработанного авторами алгоритма оценки качества данных при ОС ЭЭС проанализированы последствия успешно реализованных кибератак для факторов, характеризующих полноту и достоверность информации.

Так, наиболее распространенными кибератаками применительно к киберфизическим электроэнергетическим системам и опасными по последствиям для оценивания состояния ЭЭС являются атаки внедрения

Таблица 1

Кибератаки, снижающие качество измерений
Cyberattacks that reduce the quality of measurements

Угрозы	Информационно-коммуникационная система	Влияние на качество измерений
Атаки внедрения ложных данных	*SCADA* (*RTU*), *СМПР* (УСВИ, концентратор векторных данных (КВД)), ПВК «Оценка», *EMS*, *DMS* (Distribution Management System)	Достоверность
Атаки синхронизации времени (*spoofing*-атаки и др.)	*СМПР* (УСВИ, каналы связи между УСВИ и КВД, *GPS*), ПВК «Оценка»	Достоверность, синхронизация измерений
Атаки «отказ в обслуживании» (*DoS*, *jamming*-атаки и др.)	*SCADA* (*RTU*), СМПР (УСВИ, КВД), ПВК «Оценка», *EMS*, *DMS*	Полнота
Атаки динамической системы (атаки повторного воспроизведения, динамические инъекции ложных данных, *DoS*)	*SCADA* (*RTU*), *СМПР* (УСВИ, КВД), ПВК «Оценка»	Достоверность, полнота
Скоординированные атаки	*SCADA* (*RTU*), *СМПР* (УСВИ), ПВК «Оценка»	Достоверность, полнота
Вредоносное программное обеспечение (*Backdoor*, *Virus*, *worms*, *Trojan hors*)	*SCADA* (*HMI* – человеко-машинный интерфейс), *СМПР*	Достоверность, полнота, согласованность измерений
Атака «человек посередине»	*SCADA*, *СМПР*	Достоверность, полнота

ложных данных (*FDI – False Data Injection*) и *DoS*-атаки (*DoS – Denial of Service*) [17]. Атаки *FDI* направлены на изменение данных измерений и могут обходить пути обнаружения плохих данных в *EMS*. Успешная реализация *DoS*-атак может быть чревата большой потерей данных измерений, сделав систему ненаблюдаемой и невозможным применение традиционных методов ОС.

Для обеспечения решения задачи ОС ЭЭС в условиях кибератак, снижающих качество данных, для обнаружения ошибок в измерениях целесообразно проведение обработки данных как предварительный этап ОС ЭЭС на основе вейвлет-анализа и теории нечетких множеств.

Алгоритм идентификации ошибочных измерений. Разработка данного алгоритма необходима для проведения оценки точности измерений, требуемой для определения уровня достоверности используемой информации при ОС ЭЭС.

По сравнению с атаками FDI на статические модели, атаки *FDI* на случайные процессы изменения параметров режима труднее обнаружить, поскольку атаки могут быть смешаны не только с погрешностями измерительного тракта, но и с шумами каналов связи. В этом случае модель измерений можно описать в виде

$$\overline{y}(t) = y(t) + \xi_y(t) + a(t), \qquad (1)$$

где $y(t)$ – поток истинных значений измеряемых параметров в момент времени t; $\xi_y(t)$ – вектор шума измерений, имеющий нормальное распределение $\xi_y(t) \rightarrow (0, \sigma_y^2)$ с нулевым математическим ожиданием и дисперсией σ_y^2, характеризующей точность измерений; $a(t)$ – кибератака [17].

Атаки $a(t)$ могут быть реализованы путем введения ошибок в поток измерений и/или наложения шума.

Предлагаемый алгоритм идентификации ошибочных измерений *BDId (Bad Data Identification*) состоит из двух этапов:

1. Вейвлет-анализ информационных потоков на основе схемы достоверизации, предложенной в [18];

2. Определение ошибочных измерений в *i*-й момент времени на основе нечеткой системы логического вывода.

Достоинством применения вейвлет-преобразований потоков измерений является снижение влияния кибератак на достоверность информации путем фильтрации шумов и удаления (сглаживания) ошибок в измерениях.

Кроме этого, использование вейвлет-анализа повышает точность определения характеристик потоков измерений, необходимых для построения системы нечеткого логического вывода на втором этапе идентификации ошибочных измерений.

Для построения системы нечеткого логического вывода требуется определение следующих характеристик потоков измерений:

математическое ожидание m_y;

среднее квадратическое отклонение σ_y;

минимальное $\min_y$ и максимальное $\max_y$ значения.

В качестве входных лингвистических переменных (ЛП) рассмотрены «Измерение» вида «$\widetilde{y} = y_{\text{ист}} + \xi_y$» и «Согласованность», которая характеризуется соблюдением законов электрических цепей по рассматриваемым измерениям. Выходной переменной является «Точность измерения», характеризующая наличие или отсутствие ошибок, обусловленных кибератаками. Определены базовые терм-множества лингвистических переменных и дано описание функций принадлежности (ФП) (табл. 2–4). Разработана система нечеткого логического вывода *FIS* (*Fuzzy Inference System*), представленная на рис. 1.

Гауссова функция принадлежности измерений определяется как

$$\mu_y = \begin{cases} 0, y < -3\sigma_y; \\ e^{-k\delta_y^2}; \\ 0, y > 3\sigma_y, \end{cases} \qquad (2)$$

где k характеризует крутизну ФП, $\delta_y = \dfrac{(y - m_y)}{2\sigma_y}$ – разброс значений измерений.

Для крайних термов используются *z*-образные и *s*-образные функции принадлежности [19].

Таким образом, получена схема идентификации ошибочных измерений, представленная на рис. 2.

Пример. Для проверки эффективности использования разработанного алгоритма *BDId* были проанализированы синхронизированные векторные измерения реальной схемы участка электрической сети (рис. 3), в которой размещены УСВИ. Объем выборки для каждого измерения составлял n = 30000 с интервалом дискретизации Δt = 20 мс.

Рис. 4–7 представляют исходные графики изменения перетоков активной мощности P_{2-3} и P_{3-2}, реактивной мощности Q_{2-3} и Q_{3-2}.

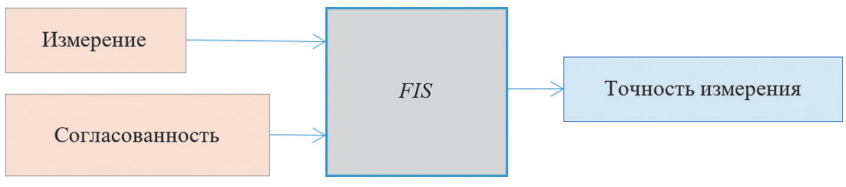

Рис. 1. Система нечеткого логического вывода FIS

Fig. 1. Fuzzy Inference System

Таблица 2

Базовое терм-множество ЛП «Измерение»

Basic term-set of the linguistic variable "Measurement"

Название терма	Представление функций принадлежности (ФП)
Около $\tilde{y}$	Гауссова ФП
Приблизительно $\tilde{y}$	Гауссова ФП
Значительно больше $\tilde{y}$	*z*-образная ФП
Значительно меньше $\tilde{y}$	*s*-образная ФП

Таблица 3

Базовое терм-множество ЛП «Согласованность»

Basic term-set of the linguistic variable "Consistency"

Уровень	Описание
0,75–1	Измерения согласованы
0,25–0,75	Измерения согласованы с допустимой погрешностью, обусловленной технологическими особенностями
0–0,25	Измерения не согласованы

Таблица 4

Базовое терм-множество ЛП «Точность измерения»

Basic term-set of the linguistic variable "Measurement accuracy"

Уровень	Описание
0,75–1	Высокий (достоверные измерения)
0,25–0,75	Средний (сомнительные измерения)
0–0,25	Низкий (ошибочные измерения)

Вейвлет-анализ показал, что измерения не содержат грубых ошибок.

Для этих потоков измерений были вычислены характеристики, необходимые для построения нечеткой системы логического вывода для *BDId* (табл. 5).

По полученным характеристикам для лингвистических переменных «Измерение P_{2-3}», «Измерение P_{3-2}», «Измерение Q_{2-3}», «Измерение Q_{3-2}» построены функции принадлежности в системе нечеткого логического вывода.

При реализации алгоритма *BDId* были проведены расчеты при моделировании кибератак *FDI*, не идентифицируемых традиционными методами обнаружения плохих данных (ОПД): методом контрольных уравнений (КУ), когда проверка достоверности измерений выполняется по невязкам КУ и классическим методом ОС, когда проверка достоверности измерений выполняется по взвешенным остаткам оценивания [5].

Расчеты проводились в имитационном эксперименте, суть которого состояла в моделировании случайных и грубых ошибок измерений на эталонном установившемся режиме, полученном расчетным путем по программе расчета установившегося режима или ОС. В измерения были внесены атаки внедрения ложных данных в виде ошибок $b_{\text{КА}}$. Модель (1) в этом случае принимает вид:

$$\overline{y}_{\text{КА1}} = y(t) + \xi_y(t) + b_{\text{КА}}(t). \qquad (3)$$

Моделирование кибератак, не идентифицируемых по контрольным уравнениям. Для проверки достоверности измерений методом КУ формируются контрольные уравнения и проверяется условие:

$$|w_k| \leqslant d_k, \qquad (4)$$

где w_k – невязка КУ, d_k – некоторое пороговое значение.

Если условие (4) выполняется, то все измерения в данном КУ считаются достоверными.

Были смоделированы две грубые ошибки: в измерении P_{2-3} значением –100 МВт и в измерении P_{3-2} значением +100 МВт. Результаты ОПД и ОС методом КУ и ОПД на основе алгоритма *BDId* представлены в табл. 6.

Расчеты показывают, что искаженные кибератакой измерения P_{2-3}, P_{3-2} методом КУ определялись как достоверные и использовались алгоритмом ОС для расчета оцененного режима. Полученные оценки существенно отклоняются от эталонного режима, хотя значение целевой функции удовлетворяет χ-квадрат критерию [5]. Анализ измерений P_{2-3} и P_{3-2} на основе алгоритма *BDId* позволил идентифицировать измерения как ошибочные с уровнем точности, равным 0,12 (низкий уровень).

Моделирование кибератак, не идентифицируемых по остаткам оценивания состояния. Здесь приведены результаты расчетов при моделировании кибератак «внедрение ложных данных» в соответствии с методикой, описанной в [2]. Эта методика разработана для случая, когда задача ОС решается классическим методом через вектор состояния *x*, а ОПД выполняется после ее решения (апостериорно) по взвешенным остаткам оценивания, которые вычисляются по формуле

$$\hat{r}_W = R_y^{-1/2} \left| \overline{y} - y(\hat{x}) \right|$$

и для достоверных измерений не должны превышать величину порога, равную 3–3,5.

Исходя из классической постановки ОС с учетом

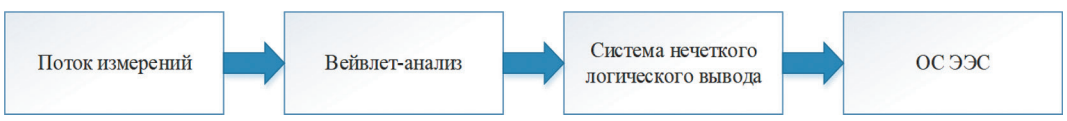

Рис. 2. Идентификация ошибочных измерений при оценивании состояния ЭЭС

Fig. 2. Identification of erroneous measurements at EPS state estimation

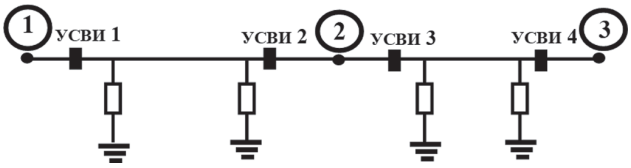

Рис. 3. Схема участка электрической сети

Fig. 3. Electric network site diagram

связи между оценками измерений $\hat{y}$ и оценками вектора состояния $\hat{x}$ ($\hat{y} = H\hat{x}$, где H – матрица Якоби), кибератаки моделировались согласно [2]:

1. Задается ненулевой вектор c, искажающий компоненты вектора состояния.

2. Формируется вектор атак $a = HC$ длиной m, где m – количество измерений.

Вектор ошибочных измерений определяется как $y_a = y + a$.

3. Выполняется ОС. Оценки вектора состояния, полученные после КА, равны $\hat{x}_a = \hat{x} + c$.

4. Вычисляются остатки оценивания:

$$r_w = R_y^{-1/2} \left\| y_a - H\hat{x}_a \right\| = R_y^{-1/2} \left\| y + a - H(\hat{x} + c) \right\| =$$

$$= R_y^{-1/2} \left\| y - H\hat{x} + (a - Hc) \right\| = R_y^{-1/2} \left\| y - H\hat{x} \right\|.$$

Полученные при этом остатки оценивания равны остаткам, вычисленным по результатам ОС без кибератаки.

Для проведения расчетов был задан искажающий вектор c = (0, 0, 20, 0, 0), моделирующий кибератаку. Результаты ОС классическим методом, идентификация ошибочных измерений по взвешенным остаткам и методом *BDId* приведены в табл. 7.

Полученные результаты свидетельствуют о том, что, несмотря на внесенные в вектор состояния искажения, метод анализа взвешенных остатков не обнаружил ошибочных измерений, т.е. не позволил идентифицировать кибератаку. На основе алгоритма *BDId* вычисленные уровни точности для P_{2-3} (0,126), Q_{2-3} (0,117), P_{3-2} (0,125), Q_{3-2} (0,117), позволили идентифицировать эти измерения как ошибочные.

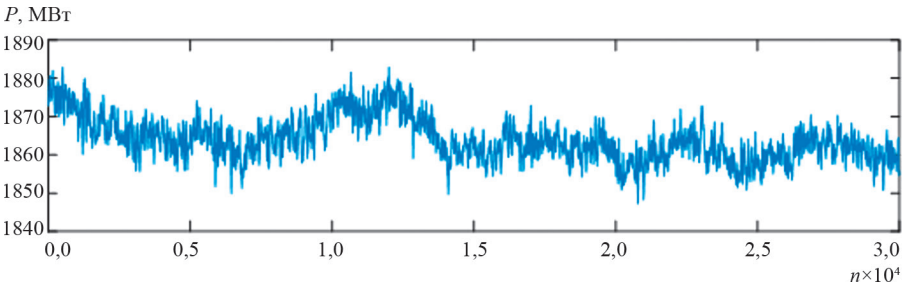

Рис. 4. Изменение перетока активной мощности P_{2-3}

Fig. 4. Change in active power flow P_{2-3}

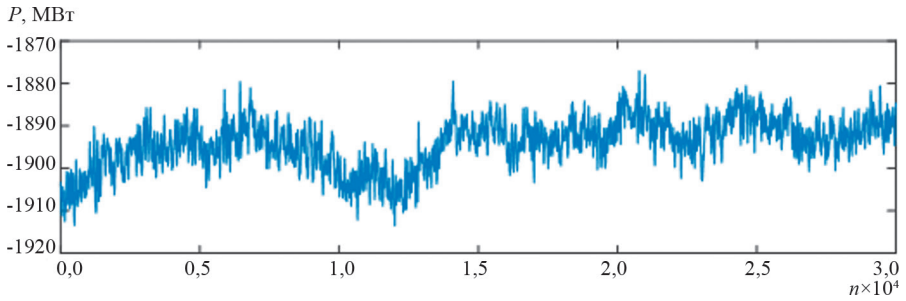

Рис. 5. Изменение перетока активной мощности P_{3-2}

Fig. 5. Change in active power flow P_{3-2}

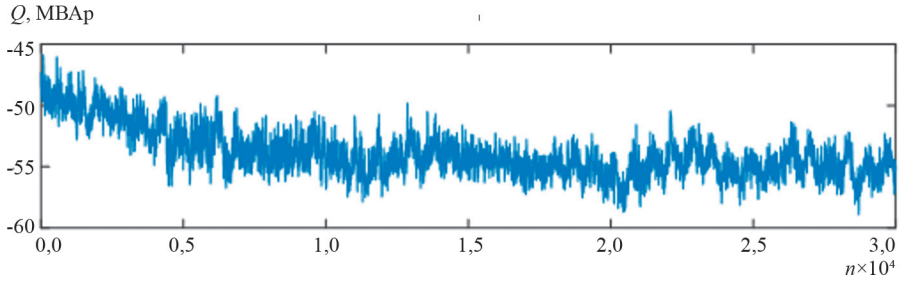

Рис. 6. Изменение перетока реактивной мощности Q_{2-3}

Fig. 6. Change in reactive power flow Q_{2-3}

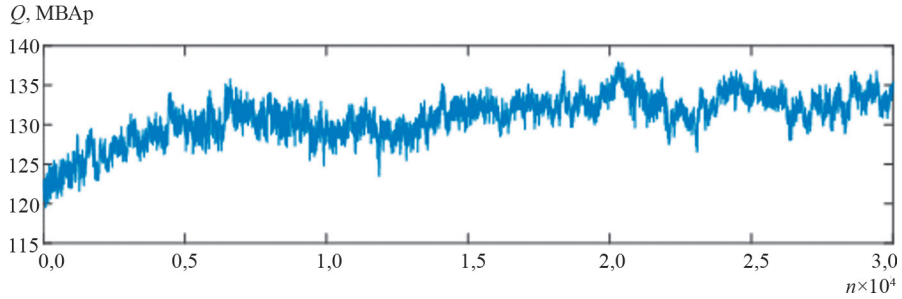

Рис. 7. Изменение перетока реактивной мощности Q_{3-2}

Fig. 7. Change in reactive power flow Q_{3-2}

Таблица 5

Характеристики процессов изменения перетоков активной и реактивной мощности линии 2–3

Characteristics of the processes of changing the active and reactive power flows of the line 2–3

Параметр	P_{2-3}	P_{3-2}	Q_{2-3}	Q_{3-2}
m_y	–1864	1894	–53,94	130,9
σ_y	5,635	5,772	1,896	2,826
$\min_y$	–1883	1877	–58,9	119,5
$\max_y$	–1847	1914	–45,86	137,9

Таблица 6

Результаты ОПД и ОС методом КУ и ОПД на основе алгоритма *BDId*

Bad data detection and state estimation results by test equation and bad data detection methods based on the *BDId* algorithm

Параметр	Эталон	Без грубой ошибки	С грубой ошибкой	Метод КУ		*BDId*
				ОПД	Оценки	
P_{1-2}	–992,7	–993	–	Дост.	–994	Дост.
Q_{1-2}	–187,5	–183	–	Дост.	–189	Дост.
P_{2-1}	1010	1013	–	Дост.	1011	Дост.
Q_{2-1}	–468	–446	–	Дост.	–464	Дост.
P_{2-3}	**–1880**	**–1879**	**–1979**	**Дост.**	**–1982**	**Ошиб.**
Q_{2-3}	29	34	–	Дост.	48	Дост.
P_{3-2}	**1896**	**1903**	**2003**	**Дост.**	**2000**	**Ошиб.**
Q_{3-2}	–92	–90	–	Дост.	–85	Дост.
Значение целевой функции – 9,98						

Таблица 7

Результаты ОС классическим методом, идентификация ошибочных измерений по взвешенным остаткам и методом *BDId*

State estimation results using the classical method, identification of erroneous measurements by weighted residuals and the *BDId* method

Параметр	Эталон	Измерения без грубой ошибки	Атака	Измерения с грубой ошибкой	Расчет классическим методом		*BDId*
					Оценки	Взвешенные остатки	
P_{1-2}	–992,7	–993	0	–	–994	0,256	–
Q_{1-2}	–187,5	–183	0	–	–189	0,709	–
P_{2-1}	1010	1013	0	–	1011	0,257	–
Q_{2-1}	–468	–446	0	–	-464	1,86	–
P_{2-3}	**–1880**	**–1879**	**–32,5**	**–1911**	**–1928**	**3,49**	**Ошиб.**
Q_{2-3}	**29**	**34**	**–432,5**	**–398**	**–395**	**0,327**	**Ошиб.**
P_{3-2}	**1896**	**1903**	**33,3**	**1963**	**1946**	**3,05**	**Ошиб.**
Q_{3-2}	**–92**	**–90**	**434,8**	**345**	**339**	**0,682**	**Ошиб.**
Значение целевой функции – 20,17							

Выводы. В статье приведены результаты исследования двух наиболее распространенных методов обнаружения плохих данных: априорного метода анализа невязок контрольных уравнений и апостериорного метода анализа взвешенных остатков оценивания для идентификации данных, искаженных вследствие сгенерированных специальным образом кибератак. Для идентификации ошибочных измерений, обусловленных кибератаками на *SCADA* и *СМПР*, предложен алгоритм обработки данных на основе вейвлет-анализа и теории нечетких множеств. Этот алгоритм относится к априорным методам ОПД, надежно функционирует даже при низкой избыточности измерений и может использоваться как предварительный этап независимо от реализованной процедуры оценивания состояния. Его использование позволит своевременно исключить влияние успешно реализованных кибератак на результаты оценивания состояния ЭЭС, тем самым обеспечивая функции управления достоверной информацией.

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

СПИСОК ЛИТЕРАТУРЫ

1. **Воропай Н.И.** Направления и проблемы трансформации электроэнергетических систем. – Электричество, 2020, № 7, с. 12–21.

2. **Liu Y., Reiter M. K., Ning P.** False data injection attacks against state estimation in electric power grids. – 16th ACM Conference on Computer and Communications Securty. Proceedings, 2009, pp. 21–32.

3. **Хохлов М.В.** Оптимизационные модели недетектируемых и неидентифицируемых FDI-атак. – Материалы международ. научного семинара им. Ю.Н. Руденко «Методические вопросы исследования надежности больших систем энергетики», 2016, с. 366–376.

4. **Hu L., Wang Z., Liu X., Vasilakos A.V., Alsaadi F.E**. Recent advances on state estimation for power grids with unconventional measurements. – IET Control Theory & Applications, 2017, vol. 11(2), pp. 3221–3232.

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

6. **Глазунова А.М., Колосок И.Н.** Достоверизация критических измерений и критических групп на основе контрольных уравнений при оценивании состояния ЭЭС. – Труды всеросс. конф. «Энергетика России в XXI веке: развитие, функционирование, управление», Иркутск, 2006, с. 696–704.

7. **Tarali A., Abur A.** Bad data detection in two-stage state estimation using phasor measurements. – 3rd IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe). Proceedings, Berlin, 2012, pp. 1–8.

8. **Abur A., Exposito A.G.** Power System State Estimation – Theory and Implementation. New York: Marchel Dekker, 2004, 327 p.

9. **Hug G., Giampapa J.A.** Vulnerability Assessment of AC State Estimation with Respect to False Data Injection Cyber-Attacks. – IEEE Transactions on Smart Grid, 2012, vol. 3(3), pp. 1362–1370.

10. **Chakhchoukh Y., Ishii H.** Cyber-attacks scenarios on the measurement function of power state estimation. – American Control Conference (ACC). Proceedings, Chicago, IL, USA, 2015, pp. 3676–3681.

11. **Chakhchoukh Y., Ishii H.** Enhancing Robustness to Cyber-Attacks in Power Systems Through Multiple Least Trimmed Squares State Estimations. – IEEE Transactions on Power Systems, 2016, vol. 31 (6), pp. 4395–4405.

12. **Zhuang P., Deng R., Liang H.** False Data Injection Attacks Against State Estimation in Multiphase and Unbalanced Smart Distribution Systems. – IEEE Transactions on Smart Grid, 2019, vol. 10 (6), pp. 6000–6013.

13. **Хохлов М.В.** Уязвимость оценивания состояния ЭЭС к кибератакам. – Материалы международ. научного семинара им. Ю.Н. Руденко «Методические вопросы исследования надежности больших систем энергетики», 2015, с. 557–566.

14. **Khokhlov M.V.** A matroid theory approach to constructing the sparse attacks on power system state estimation. – International Conference on Problems of Critical Infrastructures. Proceedings, Irkutsk, Energy System Institute, 2015, pp.57–65.

15. **Голодненко И.С., Колосок И.Н.** Кибербезопасность SCADA систем в электроэнергетике. – Материалы всеросс. научно-практической конф. с международ. участием «Повышение эффективности производства и использования энергии в условиях Сибири». Иркутск: Изд-во ИРНИТУ, 2019, с. 71–76.

16. **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.

17. **Колосок И.Н., Гурина Л.А.** Оценка рисков управления киберфизической ЭЭС на основе теории нечетких множеств. Методические вопросы исследования надежности больших систем энергетики. Кн. 1, 2019, с. 238–247.

18. **Kolosok I., Gurina L.** Wavelet Analysis of PMU Measurements for Identification of Cyber Attacks on TCMS. – International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), Moscow, Russia, 2018, pp. 1–4.

19. **Богатырев Л.Л., Манусов В.З., Содномдорж Д.** Математическое моделирование режимов электроэнергетических систем в условиях неопределенности. Улан-Батор: Изд-во типографии МГТУ, 1999, 348 с.

[27.01.2021]

Авторы: ***Колосок Ирина Николаевна*** *– доктор техн. наук, ведущий научный сотрудник отдела электроэнергетических систем, Институт систем энергетики им. Л.А. Мелентьева Сибирского отделения РАН.*

Гурина Людмила Александровна *– кандидат техн. наук, старший научный сотрудник отдела электроэнергетических систем, Институт систем энергетики им. Л.А. Мелентьева Сибирского отделения РАН.*

Elektrichestvo, 2021, No. 6, pp. 25–32 *DOI:10.24160/0013-5380-2021-6-25-32*

Identification of Cyberattacks on SCADA and WAMS Systems in Electric Power Systems when Processing Measurements by State Estimation Methods

KOLOSOK Irina N. *(Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences, Irkutsk, Russia) – Leading Researcher of the Electric Power Systems Dept., Dr.Sci. (Eng.).*

GURINA Liudmila A. *(Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences, Irkutsk, Russia) – Senior Researcher of the Electric Power Systems Dept., Cand.Sci. (Eng.).*

The hardware and software tools of the data acquisition and processing systems, as well as the state estimation procedure intended to support the actions of dispatching personnel in performing operational and emergency control of electric power systems (EPS), are critically important components of the EPS information and communication subsystem, but at the same time, they are most vulnerable to cyberattacks. To reduce the extent to which cyberattacks can affect the control quality, it is proposed to use statistical methods for processing measurement information. First of all, these are static and dynamic state estimation methods, including a procedure for verifying measurements or detecting bad data. An analysis of data quality can determine the type of cyberattack undertaken and identify overlooked vulnerabilities. The article presents the findings from a study of two most commonly used bad data detection methods: the a priori method for analyzing the residuals of test equations and the a posteriori method for analyzing the weighted estimation residuals to identify data distorted as a consequence of specially generated cyberattacks. An algorithm to detect erroneous measurements that appear during cyberattacks and are not identified by conventional measurement verification methods in performing EPS state estimation is proposed.

K e y w o r d s: *SCADA, WAMS, cyberattack, data quality, reliability, completeness, bad data detection, fuzzy sets, wavelet analysis*

REFERENCES

1. **Voropai N.I.** *Elektrichestvo – in Russ. (Electricity)*, 2020, No 7, pp. 12–21.

2. **Liu Y., Reiter M. K., Ning P.** False data injection attacks against state estimation in electric power grids. – 16th ACM Conference on Computer and Communications Securty. Proceedings, 2009, pp. 21–32.

3. **Khokhlov M.V.** *Materialy мezhdunarod. nauchnogo seminara im. Yu.N. Rudenko «Metodicheskie voprosy issledovaniya nadezhnosti bol'shikh sistem energetiki» – in Russ. (Materials of the international scientific seminar named after Yu.N. Rudenko "Methodological issues of reliability research of large power systems")*, 2016, pp. 366–376.

4. **Hu L., Wang Z., Liu X., Vasilakos A.V., Alsaadi F.E.** Recent advances on state estimation for power grids with unconventional measurements. – IET Control Theory & Applications, 2017, vol. 11(2), pp. 3221–3232.

5. **Gamm A.Z., Kolosok I.N.** *Obnaruzhenie grubyh oshibok teleizmerenij v elektroenergeticheskih sistemah* (Bad data detection in measurements in electric power systems). Novosibirsk: Nauka, 2000, 152 p.

6. **Glazunova A.M., Kolosok I.N.** *Trudy vseross. konf. «Energetika Rossii v XXI veke: razvitie, funkcionirovanie, upravlenie» – in Russ. (Proceedings of the All-Russian Conference "Energy of Russia in the XXI Century: Development, Functioning, Management")*, Irkutsk, 2006, pp. 696–704.

7. **Tarali A., Abur A**. Bad data detection in two-stage state estimation using phasor measurements. – 3rd IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe). Proceedings, Berlin, 2012, pp. 1–8.

8. **Abur A., Exposito A.G.** Power System State Estimation – Theory and Implementation. New York: Marchel Dekker, 2004, 327 p.

9. **Hug G., Giampapa J.A.** Vulnerability Assessment of AC State Estimation with Respect to False Data Injection Cyber-Attacks. – IEEE Transactions on Smart Grid, 2012, vol. 3(3), pp. 1362–1370.

10. **Chakhchoukh Y., Ishii H.** Cyber-attacks scenarios on the measurement function of power state estimation. – American Control Conference (ACC). Proceedings, Chicago, IL, USA, 2015, pp. 3676–3681.

11. **Chakhchoukh Y., Ishii H.** Enhancing Robustness to Cyber-Attacks in Power Systems Through Multiple Least Trimmed Squares State Estimations. – IEEE Transactions on Power Systems, 2016, vol. 31 (6), pp. 4395–4405.

12. **Zhuang P., Deng R., Liang H.** False Data Injection Attacks Against State Estimation in Multiphase and Unbalanced Smart Distribution Systems. – IEEE Transactions on Smart Grid, 2019, vol. 10 (6), pp. 6000–6013.

13. **Khokhlov M.V.** *Materialy мezhdunarod. nauchnogo seminara im. Yu.N. Rudenko «Metodicheskie voprosy issledovaniya nadezhnosti bol'shikh sistem energetiki» – in Russ. (Materials of the international scientific seminar named after Yu.N. Rudenko "Methodological issues of reliability research of large power systems")*, 2015, pp. 557–566.

14. **Khokhlov M.V.** A matroid theory approach to constructing the sparse attacks on power system state estimation. – International Conference on Problems of Critical Infrastructures. Proceedings, Irkutsk, Energy System Institute, 2015, pp.57–65.

15. **Golodnenko I.S., Kolosok I.N.** *Materialy vserosc. nauchno-prakticheskoy konf. s mezhdunarod. uchastiem «Povyshenie effektivnosti proizvodstva i ispol'zovaniya energii v usloviyah Sibiri» – in Russ. (Materials of the All-Russian scientific and practical conference with international participation "Improving the Efficiency of Energy Production and Use in Siberia ").* Irkutsk: Izd-vo IRNITU, 2019, pp. 71–76.

16. **Kolosok I.N., Gurina L.A.** *Informacionnye i matematicheskie tekhnologii v nauke i upravlenii – in Russ. (Information and mathematical technologies in science and management),* 2020, No.1 (17), pp. 68–78.

17. **Kolosok I.N., Gurina L.A.** *Otsenka riskov upravleniya kiberfizicheskoy EES na osnove teorii nechetkikh mnozhestv. Metodicheskie voprosy issledovaniya nadezhnosti bol'shikh sistem energetiki* (Risk Assessment of Cyberphysical ES Management Based on the Theory of Fuzzy Sets. Methodological Issues of the Study of Large Energy Systems Reliability). Kn. 1, 2019, pp. 238–247.

18. **Kolosok I., Gurina L.** Wavelet Analysis of PMU Measurements for Identification of Cyber Attacks on TCMS. – International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), Moscow, Russia, 2018, pp. 1–4.

19. **Bogatyrev L.L., Manusov V.Z., Sodnomdorzh D.** *Matematicheskoe modelirovanie rezhimov elektroenergeticheskih sistem v usloviyah neopredelennosti* (Mathematical modeling of EPS conditions under uncertainty). Ulan-Bator: Izd-vo tipografii MGTU, 1999, 348 p.

[27.01.2021]