ПОВЫШЕНИЕ КИБЕРУСТОЙЧИВОСТИ SCADA И WAMS ПРИ КИБЕРАТАКАХ НА ИНФОРМАЦИОННО-КОММУНИКАЦИОННУЮ ПОДСИСТЕМУ ЭЭС

Гурина Л.А.[1]

Цель исследования: *разработка мер обеспечения киберустойчивости SCADA и WAMS при реализованных угрозах, последствием которых является снижение качества информации, требуемой при управлении электроэнергетической системой (ЭЭС).*

Методы исследования: *вероятностные методы, марковские методы.*

Результат исследования: *проведен сравнительный анализ возможных состояний системы сбора, обработки и передачи информации при кибератаках на информационно-коммуникационную систему. Разработаны модели киберустойчивости SCADA и WAMS. На основе предложенных моделей предложены меры обеспечения киберустойчивости системы сбора, передачи и обработки информации.*

Ключевые слова: *киберфизическая ЭЭС, киберустойчивость, система сбора, обработки и передачи информации, атака внедрения ложных данных, DoS-атака, оценивание состояния.*

DOI:10.21681/2311-3456-2022-2-18-26

Введение

Внедрение новых вычислительных и коммуникационных технологий в ЭЭС, а также разрабатываемые на их основе модели и приложения для управления, привели к трансформации ЭЭС в киберфизические системы. Использование технологий интеллектуальных сетей в киберфизической ЭЭС обеспечивает двусторонние потоки информации между интегрированными информационно-коммуникационной (управляющей и коммуникационной) и физической (технологической) подсистемами при управлении и мониторинге ЭЭС. Таким образом, киберфизическая ЭЭС имеет сложную архитектуру с различными подсистемами, взаимозависимыми и взаимодействующими между собой компонентами [1], что привело к увеличению количества точек доступа для кибератак [2]. Киберфизические ЭЭС становятся более уязвимыми к кибератакам, успешная реализация которых на информационно-коммуникационном уровне может привести к отказам в технологической подсистеме ЭЭС [3]. Таким образом, сбои в информационно-коммуникационной подсистеме прямо или косвенно влияют на надежность ЭЭС [4]. Становится важным сохранение критически важных функций управления ЭЭС [5] и обеспечение киберустойчивости [6] на информационном-коммуникационном уровне при кибератаках.

Целью статьи является анализ киберустойчивости SCADA, WAMS и разработка мер ее обеспечения при кибератаках, влияющих на качество информации, используемой при управлении ЭЭС.

В качестве такой меры предложено использовать методы оценивания состояния ЭЭС [7, 8].

Для анализа киберустойчивости информационно-коммуникационной подсистемы в статье предложены модели переходов состояний при кибератаках на основе полумарковских процессов (SMP – Semi-Markov Processes), отражающие не только процессы переходов состояний при успешно реализованных кибератаках, но и процессы восстановления системы в случае подавления последствий кибератак при принятии мер по обеспечению киберустойчивости ЭЭС. Целесообразность применения предложенных моделей подтверждается на рассмотренных примерах.

Кибеустойчивость систем сбора и обработки информации, используемой при управлении ЭЭС

А. Кибербезопасность ЭЭС

Кибербезопасность - критическая проблема в киберфизических ЭЭС из-за роста уязвимостей, которые

1 Гурина Людмила Александровна, кандидат технических наук, доцент, старший научный сотрудник Лаборатории управления функционированием электроэнергетических систем Института систем энергетики им. Л.А. Мелентьева СО РАН, Иркутск, Россия. E-mail: gurina@isem.irk.ru

могут быть усилены злонамеренным взломом и непреднамеренным неправомерным поведением.

Обеспечение кибербезопасности ЭЭС необходимо для всей ее структуры, составляющими которой являются:

— физическая (технологическая) инфраструктура, включающая производство, передачу, распределение и потребление электроэнергии и
— информационно-коммуникационная управляющая инфраструктура, основными компонентами которой являются системы сбора и обработки информации (SCADA и WAMS); системы управления WACS и защиты WAPS.

Нарушение кибербезопасности ведет к снижению киберустойчивости компонентов информационно-коммуникационной инфраструктуры киберфизической ЭЭС.

Измерительные устройства со встроенной связью и обработкой данных используются для различных уровней управления и защиты в ЭЭС. Аппаратные и программные компоненты систем сбора и обработки данных - SCADA и WAMS, предназначенные для поддержки операций и действий по управлению ЭЭС, являются наиболее уязвимыми компонентами киберфизической ЭЭС. Программные сбои, ошибки в аппаратном обеспечении, а также взаимодействие программного и аппаратного обеспечения необходимо учитывать при обеспечении киберустойчивости SCADA и WAMS [9, 10].

Одной из важных особенностей киберфизических ЭЭС является интеграция высокоскоростных и надежных сетей передачи данных для управления ЭЭС. Коммуникационная часть отвечает за обмен информацией между информационно-коммуникационной и физической подсистемами. Надежность управления ЭЭС зависит от надежности сетей связи. Успешно реализованная кибератака на коммуникационные сети, нарушив передачу данных, может привести к сбою в работе ЭЭС [11].

Кибератаки на системы SCADA и WAMS могут привести к ложному вводу данных, к потере и задержке данных, ошибкам управления и отказу компонентов физических подсистем [12]. В информационно-коммуникационной подсистеме могут быть неучтенные уязвимости, которые могут быть обнаружены и использованы злоумышленниками для успешного осуществления кибератак.

Ошибки, в том числе и в измерениях, используемых при управлении ЭЭС, могут привести к отказу функционирования ЭЭС из-за выработки неправильных управляющих воздействий. Система, устойчивая к вторжению, допускает вероятность того, что кибербезопасность ЭЭС может быть нарушена, но такая система должна иметь способность обнаружить кибератаку на ЭЭС, либо надвигающийся отказ и впоследствии отреагировать на такую атаку, что снижает неблагоприятные последствия атаки [13].

Б. Анализ киберустойчивости SCADA и WAMS при кибератаках на основе полумарковских моделей

Под киберустойчивостью к внешним возмущениям понимается способность системы противостоять непредвиденным нарушениям и событиям, уменьшать начальные негативные воздействия, адаптироваться к ним и восстанавливаться после них [3,14].

Таким образом, устойчивая система должна:

1) уменьшать/поглощать неблагоприятные воздействия (поглощающая способность);

2) адаптироваться к ним (адаптивная способность);

3) восстанавливаться после них (восстанавливающая способность).

Эти способности можно рассматривать как три существенных свойства устойчивости системы к внешним возмущениям: усиление любого из них увеличит устойчивость системы.

Устойчивая система должна устранять сбои, независимо от того, является ли их причиной неисправность компонентов, ошибка оператора или кибератака, и продолжать работать (возможно, с ограниченной функциональностью) [15-17].

В условиях кибератак SCADA и WAMS могут работать в любом из возможных состояний. Как правило, наиболее вероятное состояние начинается с полной работоспособности системы, когда каждый из компонентов и вся подсистема доступны и работают должным образом. Однако, неопределенность измерительной информации и непредсказуемость, обусловленные кибератаками на информационно-коммуникационную систему, при выработке управляющих воздействий могут привести к переходу из полностью функционального состояния в другое состояние ЭЭС.

Для анализа киберустойчивости SCADA и WAMS к кибератакам предлагается использовать полумарковские модели для отображения как процессов распространения последствий кибератак на SCADA и WAMS, так и процессов восстановления [18].

Модели SMP дают возможность графически отображать события отказа/восстановления при кибератаках на информационно-коммуникационную подси-

стему, что является ценной характеристикой их применения. Процесс чередования отказа/восстановления представлен переходами от одного состояния к другому, вместе составляющими диаграмму состояний системы. В теории надежности рассматриваются два состояния системы – безотказная работа и отказ. При кибератаках в дополнение к этим состояниям введены дополнительные состояния полумарковской модели системы, которые представлены в табл. 1.

Таблица 1

Описание состояний SMP-модели

Состояние	Описание
N	Нормальное состояние
V	Состояние уязвимости
C	Состояние взлома
AS	Состояние активной защиты
PS	Состояние пассивной защиты
UD	Состояния необнаружения атаки
SD	Состояние медленной деградации
F	Состояние отказа

На рис. 2 представлена диаграмма переходов состояний модели SMP при кибератаках на систему сбора и обработки информации. Переходы справа налево показывают процессы восстановления при срабатывании пассивной и активной защиты (сплошные линии) и при переходе системы в неустойчивое состояние в случае необнаружения кибератак (пунктирные линии).

На рис. 2 представлена диаграмма переходов состояний модели SMP при кибератаках на систему сбора и обработки информации. Переходы справа налево показывают процессы восстановления при срабатывании пассивной и активной защиты (сплошные линии) и при переходе системы в неустойчивое состояние в случае необнаружения кибератак (пунктирные линии).

Система, устойчивая к вторжению, должна постоянно оценивать наличие любого нарушения безопасности. После обнаружения атаки на систему, должны быть предприняты соответствующие корректирующие действия. Основная суть этого ответа будет заключаться в попытке вернуть систему в безопасное состояние из состояния с нарушением кибербезопасности. Реакцию системы можно охарактеризовать набором функций распределения.

Ключевым вопросом в обеспечении киберустойчивости [19] является обнаружение кибератак и подавление их влияния на качество потоков данных SCADA и WAMS [20], используемых при формировании управляющих воздействий на технологическую часть ЭЭС. Такими мерами являются: улучшение схем обна-

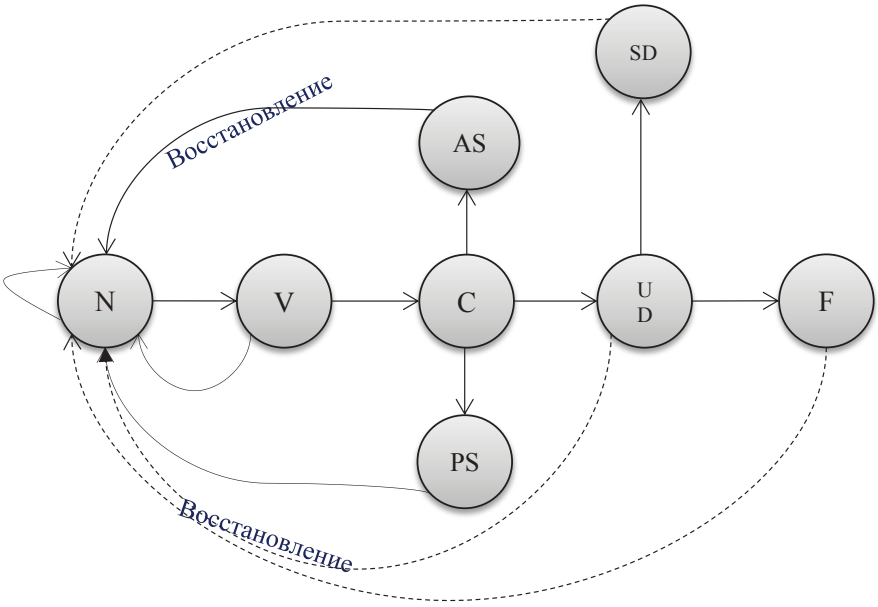

Рис. 2. Диаграмма переходов состояний системы сбора и обработки информации

ружения неверных данных, повышение безопасности системы связи, например, с помощью изолированной физической среды передачи, барьеров доступа и шифрования данных и др.

Методы пассивной защиты (например, брандмауэры, антивирусное программное обеспечение, контроль доступа, установка обновлений и средства реагирования) не обеспечивают предотвращение всех атак, особенно когда они используются для защиты от отказа в обслуживании (DoS) и распределенных DoS-атак, последствием которых является потеря данных измерений.

Активная защита, которая может упреждающе отслеживать злоумышленников и вредоносное программное обеспечение, идентифицированное системами обнаружения вторжений, становится все более привлекательной [21, 22]. Большую роль в обеспечении задач управления информацией требуемого качества при кибератаках играют методы оценивания состояния, предназначенные для расчета текущего режима ЭЭС по данным измерений, на базе которого затем решаются задачи оперативного и противоаварийного управления ЭЭС.

Процедуры обнаружения и компенсации ошибочных измерений при оценивании состояния позволяют существенно снизить вероятность искажения параметров текущего режима и служат эффективным средством идентификации кибератак на системы SCADA и WAMS и ликвидации их последствий на результаты ОС.

Таким образом, с точки зрения взаимодействия физической и информационно-коммуникационной подсистем задача ОС является связующим звеном между ними и выполняет функции «барьера» на пути проникновения искажений в информации о текущем режиме ЭЭС в задачи управления, в том числе вызванных кибератаками на системы сбора и обработки данных в ЭЭС.

Реакция системы на вторжение в систему может быть описана состояниями $\{V, AS, PS, SD, F\}$ и переходами между этими состояниями. Модель SMP основана на случайном процессе $\{X(t): t \geq 0\}$ с дискретным пространством состояний $X_S\{N, V, C, AS, PS, UD, SD, F\}$.

Анализ возможных кибератак на SCADA и WAMS показал, что наиболее опасными по последствиям для качества информации являются атаки внедрения ложных данных (FDI-атака) [23] и отказа в обслуживании (DoS-атака) [24].

Киберустойчивая система при реализованных кибератаках может находиться в состояниях $\{AS, PS\}$ и при принятии мер по устранению последствий кибератак система возвращается в состояние N. Если устойчивость системы нарушается, то система переходит в состояния $\{SD, F\}$. Обнаружение и смягчение влияния FDI-атак и DOS-атак на качество информации методами ОС снижает вероятность перехода системы в пространство состояний $\{SD, F\}$ и создает возможность перехода системы в пространство состояний $\{AS, PS, N\}$ [25].

Следовательно, чтобы системы сбора и обработки находилась или возвращалась в устойчивое к кибератакам состояние, необходима разработка мер активной защиты. В следующем примере проведен анализ целесообразности применения методов ОС ЭЭС в качестве меры по поддержанию киберустойчивости этих систем.

Пример

Рассмотрены реализованные FDI- атака и DoS-атака на систему сбора и обработки информации. В этих случаях предложены SMP-модели системы сбора и обработки информации, диаграммы переходов состояний которых показаны на рис. 6, 7.

В этом случае система сбора и обработки информации описывается состояниями $\{N, V, PS, SD, F\}$.

Система описывается состояниями $\{N, V, SD, F\}$.

При применении методов ОС ЭЭС в условиях кибератак добавляется состояние активной защиты AS и система описывается следующим образом:

— $\{N, V, AS, PS, SD, F\}$ (FDI-атака);

— $\{N, V, AS, SD, F\}$ (DoS-атака).

В табл. 2 представлены условно заданные интервалы времени нахождения системы сбора и обработки информации в возможных состояниях для следующих исследуемых ситуаций:

I. Анализ состояний системы сбора и обработки информации при FDI-атаке без применения методов ОС ЭЭС в качестве меры по поддержанию устойчивого состояния системы.

II. Анализ состояний системы сбора и обработки информации при FDI-атаке при использовании методов ОС ЭЭС в качестве меры по поддержанию устойчивого состояния системы.

III. Анализ состояний системы сбора и обработки информации при DoS-атаке без применения методов ОС ЭЭС в качестве меры по поддержанию устойчивого состояния системы, когда меры пассивной защиты не срабатывают.

IV. Анализ состояний системы сбора и обработки информации при DoS-атаке при использовании методов ОС ЭЭС в качестве меры по поддержанию

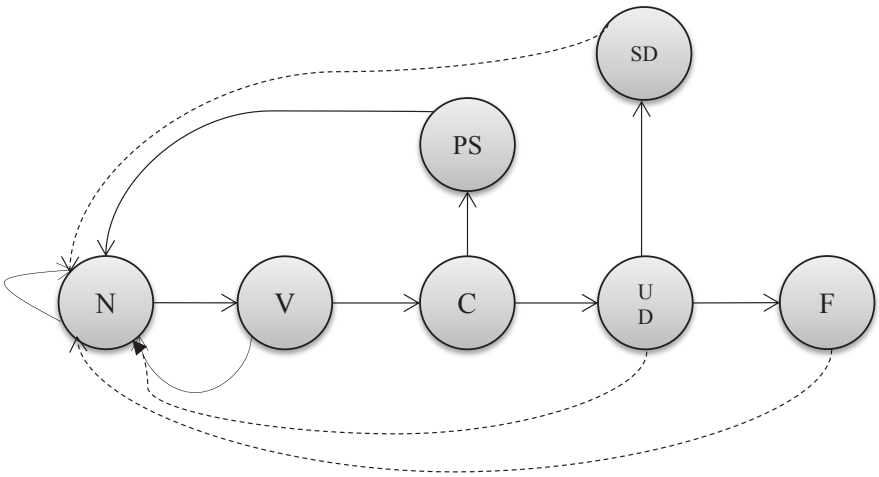

Рис. 6. Диаграмма переходов состояний при FDI-атаке

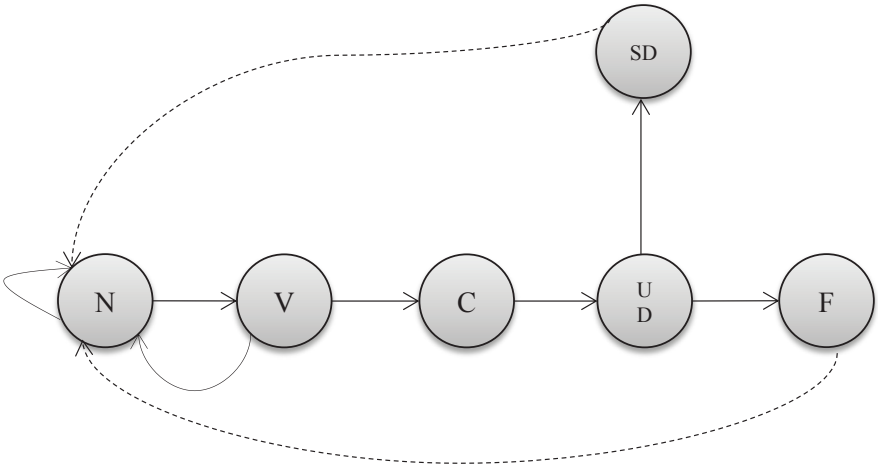

Fig. 7. Диаграмма переходов состояний при DOS-атаке

Таблица 2

Время нахождения системы сбора и обработки информации в различных состояниях (час.)

	I	II	III	IV
N	[100, 400]	[100, 400]	[100, 400]	[100, 400]
V	[1, 24]	[1, 24]	[1, 24]	[1, 24]
AS	-	[20, 350]	-	[20, 350]
PS	[10, 200]	[10, 200]	-	-
SD	[5, 24]	[1, 15]	[5, 48]	[1, 20]
F	[1, 10]	[0, 3]	[1, 15]	[0, 5]
Время наблюдения	$t = 300$			

устойчивого состояния системы.

При заданных интервалах времени $[a,b]$ определены вероятности перехода согласно следующим выражениям [25]:

$$P(Y < X) = \int_a^b \frac{t}{b}\frac{1}{b-a}dt\,,\ P_N = \lim_{t\to\infty} F_N(t) = 1\ ,$$

$$P_F = \lim_{t\to\infty} F_F(t) = 1\,,$$

и составлены матрицы вероятностей перехода [18]:

$$P_I = \begin{pmatrix} N & V & PS & SD & F \\ 0 & 1 & 0 & 0 & 0 \\ 0.52 & 0 & 0.48 & 0 & 0 \\ 0.53 & 0 & 0 & 0.47 & 0 \\ 0.6 & 0 & 0 & 0 & 0.4 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix};$$

$$P_{II} = \begin{pmatrix} N & V & AS & PS & SD & F \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0.52 & 0 & 0.48 & 0 & 0 & 0 \\ 0.53 & 0 & 0 & 0.47 & 0 & 0 \\ 0.53 & 0 & 0 & 0 & 0.47 & 0 \\ 0.53 & 0 & 0 & 0 & 0 & 0.47 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix};$$

$$P_{III} = \begin{pmatrix} N & V & SD & F \\ 0 & 1 & 0 & 0 \\ 0.52 & 0 & 0.48 & 0 \\ 0.55 & 0 & 0 & 0.45 \\ 0 & 0 & 0 & 1 \end{pmatrix};$$

$$P_{IV} = \begin{pmatrix} N & V & AS & SD & F \\ 0 & 1 & 0 & 0 & 0 \\ 0.52 & 0 & 0.48 & 0 & 0 \\ 0.53 & 0 & 0 & 0.47 & 0 \\ 0.53 & 0 & 0 & 0 & 0.47 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Матрицу вероятностей перехода состояний P можно представить в виде

$$P = \begin{pmatrix} Q & C \\ 0 & E \end{pmatrix},$$

где Q - фундаментальная матрица, элементами которой являются вероятности перехода между переходными состояниями, C - матрица вероятностей перехода между переходными и поглощающими состояниями, E - единичная матрица.

Количество посещений переходного состояния i до того, как модель перейдет в поглощающее состояние определяется как

$M = [m_{ij}] = (E-Q)^{-1}$,

где m_{ij} - среднее количество посещения состояния *j*, учитывая, что модель запущена в состоянии *i*.

Среднее время пребывания S_i в состоянии i определяется согласно выражению

$$S_i = \int_0^{a_i}(1-\frac{t}{b_i})dt + \int_{a_i}^{b_i}(1-\frac{t}{b_i})(1-\frac{t-a_i}{b_i-a_i})dt\ ,$$

3) Средняя наработка на отказ определяется по следующей формуле

$$MTBF = \sum_{i\in Trans} M_i S_i\,.$$

4) Интенсивность отказов определяется как

$$\lambda = \frac{1}{MTBF}$$

5) Вероятность безотказной работы при экспоненциальном законе распределения находится из выражения:

$P = e^{-\lambda t}$.

В табл.3 представлены полученные результаты расчета таких показателей, как средняя наработка на отказ, интенсивность отказов и вероятность безотказной работы системы при успешно реализованных кибератаках.

Результаты расчета вероятности безотказной работы системы в условиях кибератак для каждого из рассмотренных случаев показали, что методы ОС могут быть использованы в качестве эффективной меры по поддержанию устойчивости к кибератакам системы сбора и обработки информации.

Таким образом, применение методов оценивания ЭЭС для обнаружения и подавления влияния кибератак на качество информации увеличивает вероятность безотказной работы, система становится более устойчивой к кибератакам.

Выводы

Проведен анализ киберустойчивости систем сбора, передачи и обработки информации. Разработаны модели киберустойчивости этих систем на основе полумарковских процессов при кибератаках на информационно-коммуникационную инфраструктуру ЭЭС. Проанализированы возможные меры по обеспечению киберустойчивости SCADA, WAMS при кибератаках. В качестве одной из этих мер можно рассматривать оценивание состояния ЭЭС.

Таблица 3

Показатели киберустойчивости системы при кибератаках

	I	II	III	IV
$MTBF$	3258,39	6682,68	1235,1	2995,85
λ	0,0003	0,0001	0,0008	0,0003
P	0,91	0,97	0,79	0,91

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

Литература

1. A. Kwasinski. Modeling of Cyber-Physical Intra-Dependencies in Electric Power Grids and Their Effect on Resilience. 2020 8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems. 2020, pp. 1-6. DOI: 10.1109/MSCPES49613.2020.9133702.
2. Zang T., Gao S., Liu B., Huang T., Wang T., Wei X. (2019). Integrated Fault Propagation Model Based Vulnerability Assessment of the Electrical Cyber-Physical System under Cyber Attacks. Reliability Engineering & System Safety. 2019. DOI:10.1016/j.ress.2019.04.024.
3. Voropai N. Electric Power System Transformations: A Review of Main Prospects and Challenges. Energies. 2020, vol.13. DOI: 10.3390/en132156392.
4. P. A. Oyewole, D. Jayaweera. Power System Security With Cyber-Physical Power System Operation. In IEEE Access. 2020, vol. 8, pp. 179970-179982. DOI: 10.1109/ACCESS.2020.3028222.
5. M. Ni, M. Li. Reliability Assessment of Cyber Physical Power System Considering Communication Failure in Monitoring Function. International Conference on Power System Technology (POWERCON). 2018, pp. 3010-3015. DOI: 10.1109/POWERCON.2018.8601964.
6. Воропай Н.И., Колосок И.Н., Коркина Е.С. Проблемы повышения киберустойчивости цифровой подстанции // Релейная защита и автоматизация. 2019. № 1(34). С. 78-83.
7. Хохлов М.В., Готман Н.Э. Робастное обобщенное оценивание состояние ЭЭС: метод на основе линейного целочисленного программирования // Методические вопросы исследования надежности больших систем энергетики. 2017. С. 495-504.
8. Колосок И.Н., Гурина Л.А. Нечетко-вероятностный подход к обнаружению ошибок измерений при оценивании состояния ЭЭС // Методические вопросы исследования надежности больших систем энергетики. 2020. С. 70-79.
9. Sourav Sinha, Neeraj Kumar Goyal, Rajib Mall. Survey of combined hardware–software reliability prediction approaches from architectural and system failure viewpoint. International Journal of System Assurance Engineering and Management. 2019, vol. 10, pp. 453-474. DOI: 10.1007/s13198-019-00811-y
10. Diptendu Sinha Roy, Cherukuri Murthy, Dusmanta Kumar Mohanta. Reliability analysis of phasor measurement unit incorporating hardware and software interaction failures. Generation Transmission & Distribution IET. 2015, vol. 9, no. 2, pp. 164-171. DOI: 10.1049/iet-gtd.2014.0115.
11. Успенский М.И. Составляющие надежности информационной сети системы мониторинга переходных режимов // Методические вопросы исследования надежности больших систем энергетики. 2020. С. 370-379.
12. Колосок И.Н., Гурина Л.А. Оценка рисков управления киберфизической ЭЭС на основе теории нечетких множеств // Методические вопросы исследования надежности больших систем энергетики. В 2-х книгах. 2019. С. 238-247.
13. A. Ashok, M. Govindarasu and J. Wang. Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid. In Proceedings of the IEEE. July 2017, vol. 105, no. 7, pp. 1389-1407. DOI: 10.1109/JPROC.2017.2686394.
14. Reza Arghandeh, Alexandra von Meier, Laura Mehrmanesh, Lamine Mili. On the definition of cyber-physical resilience in power systems. Renewable and Sustainable Energy Reviews, 2016, Vol. 58, pp. 1060-1069. DOI: 10.1016/j.rser.2015.12.193.
15. Craig Poulin, Michael B. Kane, Infrastructure resilience curves: Performance measures and summary metrics. Reliability Engineering & System Safety, Volume 216, 2021, 107926, ISSN 0951-8320, DOI: 10.1016/j.ress.2021.107926.
16. Yasser Almoghathawi, Kash Barker. Component importance measures for interdependent infrastructure network resilience. Computers & Industrial Engineering. 2019, Vol. 133, pp. 153-164. DOI: 10.1016/j.cie.2019.05.001.

17. Daniel A. Sepúlveda Estay, Rishikesh Sahay, Michael B. Barfod, Christian D. Jensen, A systematic review of cyber-resilience assessment frameworks. Computers & Security. 2020, vol. 97, 101996. DOI: 10.1016/j.cose.2020.101996.
18. S. Tang, Z. Liu, L. Wang. Power System Reliability Analysis Considering External and Insider Attacks on the SCADA System. 2020 IEEE/PES Transmission and Distribution Conference and Exposition (T&D). 2020, pp. 1-5. DOI: 10.1109/TD39804.2020.9299922..
19. T. Bettmann. A Framework for Resilient Data Management for Smart Grids. 2019 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW). 2019, pp. 85-88. DOI: 10.1109/ISSREW.2019.00048.
20. Kolosok I., Gurina L. Monitoring and analysis of SCADA and WAMS data for EPS digitalization. In: E3S Web of Conferences 209. ID: 02015 (2020).
21. Bo Chen, Jianhui Wang, Mohammad Shahidehpour. Cyber–physical perspective on smart grid design and operation. IET Cyber-Physical Systems: Theory & Applications. 2018, vol. 3, pp. 129-141. DOI: 10.1049/iet-cps.2017.0143.
22. T. Yang, H. Wang, G. Wang, H. Jiang. Interval state estimation with Limited PMU against False Data Injection Attack. 2019 IEEE Innovative Smart Grid Technologies - Asia (ISGT Asia). 2019, pp. 3669-3673. DOI: 10.1109/ISGT-Asia.2019.8881161.
23. M. Iqbal, M.A. Iqbal. Attacks due to False Data Injection in Smart Grids: Detection & Protection. 2019 1st Global Power, Energy and Communication Conference (GPECOM). 2019, pp. 451-455. DOI: 10.1109/GPECOM.2019.8778503.
24. F. Li, X. Yan, Y. Xie, Z. Sang, X. Yuan. A Review of Cyber-Attack Methods in Cyber-Physical Power System. 2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP). 2019, pp. 1335-1339. DOI: 10.1109/APAP47170.2019.9225126.
25. Колосок И.Н., Гурина Л.А. Оценка показателей киберустойчивости систем сбора и обработки информации в ЭЭС на основе полумарковских моделей // Вопросы кибербезопасности. 2021, №6. С. 2-11. DOI: 10.21681/2311-3456-2021-6-2-11.

INCREASING CYBER RESILIENCE OF SCADA AND WAMS IN THE EVENT OF CYBER ATTACKS ON THE INFORMATION AND COMMUNICATION SUBSYSTEM OF THE ELECTRIC POWER SYSTEM

Gurina L.A.[2]

Research objective: *development of measures to ensure cyber resilience of SCADA and WAMS under realized threats, the consequence of which is a decrease in the quality of information required in the control of the electric power system (EPS).*

Research methods: *probabilistic methods, methods of power system reliability analysis, Markov methods.*

Research result. *A comparative analysis of possible states of information collection, transmission, and processing systems (SCADA, WAMS) during cyberattacks on the information and communication system was carried out. SCADA and WAMS cyber resilience models were developed. On the basis of the models proposed, measures to ensure cyber resilience of information collection, transmission, and processing system were put forward.*

Keywords: *cyber-physical power system; resilience; information collection, processing, and transmission system; false data injection attack; DoS-attack; state estimation.*

The research was conducted within the framework of the scientific project "Theoretical foundations, models and methods to control the expansion and operation of intelligent electric power systems (Smart Grids)", No. FWEU- 2021-0001.

2 Liudmila A. Gurina, Ph.D. in engineering, Associate Professor, Senior Researcher in the Laboratory for Control of Electric Power Systems at Melentiev Energy Systems Institute, SB RAS, Irkutsk, Russia. E-mail: gurina@isem.irk.ru

References

1. Kwasinski A. Modeling of Cyber-Physical Intra-Dependencies in Electric Power Grids and Their Effect on Resilience. 2020 8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems. 2020, pp. 1-6. DOI: 10.1109/MSCPES49613.2020.9133702.
2. Zang T., Gao S., Liu B., Huang T., Wang T., Wei X. Integrated Fault Propagation Model Based Vulnerability Assessment of the Electrical Cyber-Physical System under Cyber Attacks. Reliability Engineering & System Safety. 2019. DOI:10.1016/j.ress.2019.04.024.
3. Voropai N. Electric Power System Transformations: A Review of Main Prospects and Challenges. Energies. 2020, vol.13. DOI: 10.3390/en132156392.
4. Oyewole P.A., Jayaweera D. Power System Security with Cyber-Physical Power System Operation. In IEEE Access. 2020, vol. 8, pp. 179970-179982. DOI: 10.1109/ACCESS.2020.3028222.
5. Ni M., Li. M. Reliability Assessment of Cyber Physical Power System Considering Communication Failure in Monitoring Function. International Conference on Power System Technology (POWERCON). 2018, pp. 3010-3015. DOI: 10.1109/POWERCON.2018.8601964.
6. Voropai N.I., Kolosok I.N., Korkina E.S. Problemy povysheniya kiberustoichivosti tsifrovoi podstantsii // Releinaya zashchita i avtomatizatsiya. 2019. № 1(34). S. 78-83.
7. Khokhlov M.V., Gotman N.E. Robastnoe obobshchennoe otsenivanie sostoyanie EES: metod na osnove lineinogo tselochislennogo programmirovaniya // Metodicheskie voprosy issledovaniya nadezhnosti bol'shikh sistem energetiki. 2017. C. 495-504.
8. Kolosok I.N., Gurina L.A. Nechetko-veroyatnostnyi podkhod k obnaruzheniyu oshibok izmerenii pri otsenivanii sostoyaniya EES // Metodicheskie voprosy issledovaniya nadezhnosti bol'shikh sistem energetiki. 2020. C. 70-79.
9. Sourav Sinha, Neeraj Kumar Goyal, Rajib Mall. Survey of combined hardware–software reliability prediction approaches from architectural and system failure viewpoint. International Journal of System Assurance Engineering and Management. 2019, vol. 10, pp. 453-474. DOI: 10.1007/s13198-019-00811-y
10. Diptendu Sinha Roy, Cherukuri Murthy, Dusmanta Kumar Mohanta. Reliability analysis of phasor measurement unit incorporating hardware and software interaction failures. Generation Transmission & Distribution IET. 2015, vol. 9, no. 2, pp. 164-171. DOI: 10.1049/iet-gtd.2014.0115.
11. Uspenskii M.I. Sostavlyayushchie nadezhnosti informatsionnoi seti sistemy monitoringa perekhodnykh rezhimov // Metodicheskie voprosy issledovaniya nadezhnosti bol'shikh sistem energetiki. 2020. C. 370-379.
12. Kolosok I.N., Gurina L.A. Otsenka riskov upravleniya kiberfizicheskoi EES na osnove teorii nechetkikh mnozhestv // Metodicheskie voprosy issledovaniya nadezhnosti bol'shikh sistem energetiki. V 2-kh knigakh. 2019. C. 238-247.
13. A. Ashok, M. Govindarasu and J. Wang. Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid. In Proceedings of the IEEE. July 2017, vol. 105, no. 7, pp. 1389-1407. DOI: 10.1109/JPROC.2017.2686394.
14. Reza Arghandeh, Alexandra von Meier, Laura Mehrmanesh, Lamine Mili On the definition of cyber-physical resilience in power systems. Renewable and Sustainable Energy Reviews, 2016, Vol. 58, pp. 1060-1069. DOI: 10.1016/j.rser.2015.12.193.
15. Craig Poulin, Michael B. Kane, Infrastructure resilience curves: Performance measures and summary metrics. Reliability Engineering & System Safety, Volume 216, 2021, 107926, ISSN 0951-8320, DOI: 10.1016/j.ress.2021.107926.
16. Yasser Almoghathawi, Kash Barker. Component importance measures for interdependent infrastructure network resilience. Computers & Industrial Engineering. 2019, Vol. 133, pp. 153-164. DOI: 10.1016/j.cie.2019.05.001.
17. Daniel A. Sepúlveda Estay, Rishikesh Sahay, Michael B. Barfod, Christian D. Jensen, A systematic review of cyber-resilience assessment frameworks. Computers & Security. 2020, vol. 97, 101996. DOI: 10.1016/j.cose.2020.101996.
18. S. Tang, Z. Liu, L. Wang. Power System Reliability Analysis Considering External and Insider Attacks on the SCADA System. 2020 IEEE/PES Transmission and Distribution Conference and Exposition (T&D). 2020, pp. 1-5. DOI: 10.1109/TD39804.2020.9299922..
19. T. Bettmann. A Framework for Resilient Data Management for Smart Grids. 2019 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW). 2019, pp. 85-88. DOI: 10.1109/ISSREW.2019.00048.
20. Kolosok I., Gurina L. Monitoring and analysis of SCADA and WAMS data for EPS digitalization. In: E3S Web of Conferences 209. ID: 02015 (2020).
21. Bo Chen, Jianhui Wang, Mohammad Shahidehpour. Cyber–physical perspective on smart grid design and operation. IET Cyber-Physical Systems: Theory & Applications. 2018, vol. 3, pp. 129-141. DOI: 10.1049/iet-cps.2017.0143.
22. T. Yang, H. Wang, G. Wang, H. Jiang. Interval state estimation with Limited PMU against False Data Injection Attack. 2019 IEEE Innovative Smart Grid Technologies - Asia (ISGT Asia). 2019, pp. 3669-3673. DOI: 10.1109/ISGT-Asia.2019.8881161.
23. M. Iqbal, M.A. Iqbal. Attacks due to False Data Injection in Smart Grids: Detection & Protection. 2019 1st Global Power, Energy and Communication Conference (GPECOM). 2019, pp. 451-455. DOI: 10.1109/GPECOM.2019.8778503.
24. F. Li, X. Yan, Y. Xie, Z. Sang, X. Yuan. A Review of Cyber-Attack Methods in Cyber-Physical Power System. 2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP). 2019, pp. 1335-1339. DOI: 10.1109/APAP47170.2019.9225126.
25. Kolosok I.N., Gurina L.A. Otsenka pokazatelei kiberustoichivosti sistem sbora i obrabotki informatsii v EES na osnove polumarkovskikh modelei // Voprosy kiberbezopasnosti. 2021, №6. S. 2-11. DOI: 10.21681/2311-3456-2021-6-2-11.