ОЦЕНКА КИБЕРУСТОЙЧИВОСТИ СИСТЕМЫ ОПЕРАТИВНО-ДИСПЕТЧЕРСКОГО УПРАВЛЕНИЯ ЭЭС

Гурина Л.А.[1]

Цель исследования: *разработка алгоритма оценки киберустойчивости системы оперативно-диспетчерского управления (ОДУ) ЭЭС при кибератаках на системы сбора, обработки и передачи информации.*

Методы исследования: *вероятностные методы, методы теории нечетких множеств, методы анализа надежности ЭЭС.*

Результат исследования: *проведен анализ влияния кибератак на функциональность системы ОДУ ЭЭС. Выявлены факторы, обеспечивающие киберустойчивость системы ОДУ ЭЭС при реализованных киберугрозах. Предложена модель киберустойчивости системы ОДУ ЭЭС. Разработан алгоритм оценки киберустойчивости системы ОДУ ЭЭС с учетом рисков кибербезопасности.*

Ключевые слова: *система сбора, обработки и передачи информации, риск кибербезопасности, система управления, функциональность, кибератаки, нечеткая модель.*

DOI: 10.21681/2311-3456-2022-3-23-31

1. Введение

Интеллектуальные электроэнергетические системы (ЭЭС) относятся к киберфизическим системам, которые оснащены цифровыми измерительными устройствами и средствами связи с высокой скоростью и малой задержкой для мониторинга и оперативного управления физической инфраструктурой ЭЭС. По мере того, как связь между информационно-коммуникационной (управляющей) и физической (управляемой) инфраструктурами становится все сильнее, кибератаки могут оказывать все более существенное влияние на нормальное функционирование ЭЭС [1, 2]. Отказы и их распространение в киберфизических электроэнергетических системах существенно отличаются от таковых в традиционых ЭЭС. Кибератаки в управляющей подсистеме стали важным фактором возникновения сбоев не только в информационно-коммуникационной подсистеме, но и в физической подсистеме из-за более тесной связи между этими подсистемами [3]. Поэтому для поддержания надежной и бесперебойной работы ЭЭС важно обеспечение киберустойчивости управляющей подсистемы.

Задачи управления функционированием ЭЭС предъявляют серьезные требования к качеству информации, используемой при формировании управляющих воздействий на ЭЭС. При этом важную роль играет функциональная полнота, надежность работы компонентов системы сбора, передачи и обработки информации и программного обеспечения. Внедрение цифровых компонентов в систему ОДУ физическими процессами ЭЭС на основе различных информационных потоков, делает эту систему критически уязвимой к киберугрозам. Кибератаки, в том числе и специально разработанные вредоносные программы Stuxnet, BlackEnergy, Crash Override и Trisis/Trident, направлены на выведение из строя систем оперативно-диспетчерского управления ЭЭС [4]. Все это усилило опасения не только по поводу рисков кибербезопасности [5,6] системы ОДУ, но и привело к необходимости обеспечения их киберустойчивости при успешно реализованных кибератаках.

Устойчивая система управления — это система, которая поддерживает осведомленность о состоянии и приемлемый уровень нормальной работы в ответ на нарушения, включая угрозы неожиданного и злонамеренного характера [7].

В то время как меры по обеспечению информационной безопасности направлены на предотвращение сбоев для поддержания конфиденциальности, целостности и доступности информации [8,9], обеспечение киберустойчивости направлено на осуществление основных операций, поддержание критических уровней функций управления и быстрое восстановление [10-12]. Киберустойчивость особенно актуальна для системы ОДУ киберфизическими системами, поскольку последствиями киберсбоев могут быть отказы функциональных компонентов систем управления [13].

1 Гурина Людмила Александровна, кандидат техн. 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

Таблица 1

Влияние кибератак на функции оперативного управления ЭЭС

Угрозы	Нарушение функций оперативного управления ЭЭС
Атаки внедрения ложных данных	Выработка неправильных управляющих воздействий (УВ). Потеря контроля частоты, напряжения. Потеря наблюдаемости. Неправильные диспетчерские команды. Ложные характеристики нарушений окажет влияние на операции распределения и передачи.
Атаки синхронизации времени (spoofing-атаки и др.)	Ложная визуализация текущего режима, что приводит к ошибочным действиям по контролю и защите. Потеря контроля частоты, напряжения. Ложная информация относительно наличия и места неисправности. Рассогласование команд на отключение/срабатывание интеллектуальных устройств.
Атаки «отказ в обслуживании» (DoS jamming-атаки и др.)	Задержка управления. Выработка неправильных УВ. Потеря контроля частоты, напряжения. Блокировка управляющего сигнала. Потеря наблюдаемости.
Атаки динамической системы (атаки повторного воспроизведения, DDoS)	Задержка управления. Потеря наблюдаемости. Нарушение контроля частоты, напряжения.
Скоординированные атаки	Все перечисленное выше.
Вредоносное программное обеспечение	Некорректная выработка УВ. Неправильное срабатывание аппаратных и программных устройств. Потеря контроля частоты, напряжения.

Условная мера устойчивости – это адаптивная способность или способность реагировать на угрозу и поддерживать приемлемую функциональность. Устойчивая система должна снижать риски кибербезопасности и предотвращать тяжелые последствия кибератак. Отсюда, при оценке киберустойчивости системы ОДУ предлагается учитывать риск кибербезопасности, позволяющий оценить вероятность возникновения события и последствия, которые могут возникнуть в случае возникновения кибератаки [14].

Существует высокая потребность в оценке показателя киберустойчивости системы ОДУ ЭЭС, отражающего поведение системы при нарушениях кибербезопасности.

Статья организована следующим образом. Во втором разделе дается структура системы ОДУ ЭЭС, определены уязвимые к кибератакам компоненты и приведено определение киберустойчивости ЭЭС. В третьем разделе показана зависимость киберустойчивости системы ОДУ ЭЭС от ряда факторов, определяющих ее уровень, и предложена нечеткая модель киберустойчивости системы ОДУ и мониторинга режимами ЭЭС, учитывающая влияние способностей системы управления поддерживать приемлемую функциональность при возмущающих событиях в системе. Разработан алгоритм оценки киберустойчивости системы управления, описание которого приведено в четвертом разделе. Эффективность применения алгоритма показана на примере в пятом разделе. На основе проведенных исследований сформулированы выводы.

2. Киберустойчивость системы ОДУ ЭЭС

Киберустойчивость определяется как «способность системы защищаться от инцидентов кибератак и поддерживать приемлемый уровень производительности за счет поддержания критической функциональности и своевременного восстановления качества услуг до уровня, существовавшего до инцидента» [15].

При исследовании проблем киберустойчивости системы ОДУ ЭЭС рассмотрена ее иерархическая структура [16], включающая в себя:

- региональное диспетчерское управление;
- объединенное диспетчерское управление;
- центральное диспетчерское управление.

Основными функциями оперативно-диспетчерского управления ЭЭС на разных уровнях иерархии являются:

- оперативный контроль и управление объектами ЭЭС;
- мониторинг надежности ЭЭС;
- оптимизация режимов ЭЭС;
- анализ данных мониторинга в режиме on-line;
- прогнозирование нагрузок и потерь мощности;
- регулирование частоты, перетоков активной мощности;
- оценивание и прогнозирование состояние ЭЭС, пропускной способности сетей и т.д.

Компонентами системы ОДУ ЭЭС являются измерительные подсистемы, подсистемы передачи данных, подсистемы обработки данных, подсистемы синхронизации времени, входящие в системы SCADA/EMS, предназначенные для поддержки действий диспетчерского персонала при оперативном управлении ЭЭС, и WAMS, обеспечивающая возможности мониторинга, управления и контроля ЭЭС [17]. Кибер-инциденты могут возникнуть в любом из описанных компонентов системы ОДУ ЭЭС и привести к нарушению функций управления. В табл. 1 показаны возможные нарушения функций оперативного управления ЭЭС в результате успешно реализованных кибератак.

Ключевыми характеристиками, которыми должна обладать система оперативно-диспетчерского управления ЭЭС для поддержания своей функциональности на приемлемом уровне при кибератаках, являются:

- возможность смягчать и подавлять нежелательные последствия кибератаки;
- возможность реагировать и адаптироваться;
- возможность восстановления.

Состояние уязвимости возникает при снижении кибербезопасности системы управления и характеризуется снижением поглощающих способностей системы, как следствие, повышенным риском опасных по последствиям успешно реализованных кибератак. Таким образом, при исследовании проблемы киберустойчивости системы ОДУ ЭЭС необходим анализ возможных сбоев, нарушающих функциональность системы и снижающих надежность ее компонентов [18].

В результате кибератак на любой компонент системы ОДУ ЭСС возможны следующие ситуации:

- информационные отказы;
- отказы аппаратного обеспечения;
- отказы программного обеспечения;
- отказы взаимодействия аппаратного и программного обеспечения.

Информационные отказы могут возникнуть в результате искажения, потери и задержки информационных потоков, используемых при управлении ЭЭС, при кибератаках на удаленные устройства телемеханики RTU, диспетчерские пункты управления MTU, человеко-машинный интерфейс HMI системы SCADA и/или устройства синхронизированных векторных измерений PMU, концентраторы векторных данных PDC на всех уровнях диспетчерского управления, глобальные навигационные спутниковые системы GPS/ГЛОНАСС (GNSS – Global Navigation Satellite Systems), серверы времени TS (TS – Time Server) системы WAMS, а также сети передачи данных.

Отказы аппаратного и программного обеспечения, а также их взаимодействия [19], влияют на надежность цифровых устройств, напр., PMU или PDC, сети передачи данных [20].

Для поддержания киберустойчивости системы ОДУ важно обеспечение надежности реализаций функций управления, обусловленной надежностью данных, аппаратной, программной надежностью и надежностью сети.

3. Модель киберустойчивости системы ОДУ ЭЭС

Критическая функциональность системы ОДУ ЭЭС — это минимальный ожидаемый уровень, который должен поддерживаться ею в случае кибератаки. Некоторые приложения, используемые при управлении ЭЭС, можно отнести к категории критически важных — их отказ может нанести ущерб технологической части ЭЭС. На киберустойчивость системы ОДУ влияет ее способность смягчать последствия кибератаки и, тем самым, снижать риск кибербезопасности ЭЭС. Возврат системы в нормальное состояние означает способность системы к адаптации и восстановлению. Таким образом, обеспечение киберустойчивости зависит от уровня кибербезопасности, скорости отклика и восстановления (рис. 1).

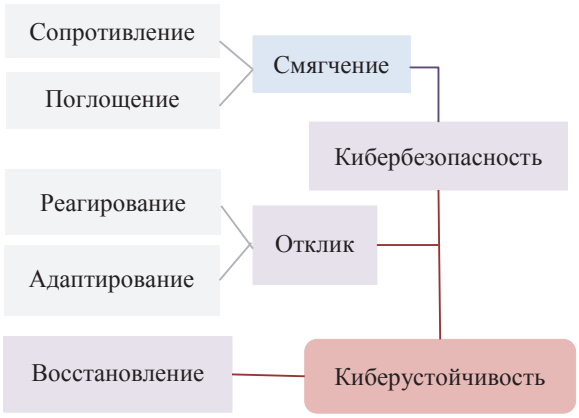

Рис 1. Факторы обеспечения киберустойчивости

Отсюда, показатель киберустойчивости системы оперативно-диспетчерского управления можно описать нечеткой моделью

$$\tilde{R} = \tilde{R}_1 \times \tilde{R}_2 \times \tilde{R}_3, \quad (1)$$

где $\tilde{R}_1$ — лингвистическая переменная «Кибербезопасность системы ОДУ», $\tilde{R}_2$ — лингвистическая переменная «Отклик (ответ) системы ОДУ на кибератаку», $\tilde{R}_3$ — лингвистическая переменная «Восстановление системы ОДУ».

Таблица 2

Уровни риска

Уровень/ диапазон изменения ФП	Описание
Очень низкий $VL,[0,0.04]$	Можно ожидать, что событие угрозы будет иметь незначительное неблагоприятное воздействие на оперативное управление ЭЭС.
Низкий $L,[0.05,0.2]$	Угрожающее событие может иметь ограниченное неблагоприятное воздействие на оперативное управление ЭЭС, последствия для функционирования имеют локальный характер.
Средний $M,[0.21,0.79]$	Опасное событие может оказать серьезное неблагоприятное воздействие на оперативное управление ЭЭС.
Высокий $H,[0.8,0.95]$	Угрожающее событие может иметь серьезное или катастрофическое неблагоприятное последствие для функционирования ЭЭС.
Критически высокий $CH,[0.96,1]$	Событие угрозы может иметь многочисленные серьезные или катастрофические неблагоприятные последствия для функционирования ЭЭС.

Таблица 3

Уровни отклика

Уровень/ диапазон изменения ФП	Описание
Низкий $L,[0,0.24]$	Система ОДУ плохо адаптируется и чувствительно реагирует в условиях кибератак с учетом мер по активной и пассивной защите от кибератак, отмечается низкая функциональность, возможны отказы компонентов, потеря некоторых функций оперативного управления и значительные ошибки в функционировании системы. При этом интенсивность отказов высокая, что обусловливает низкую вероятность безотказной работы.
Средний $M,[0.25,0.79]$	Адаптации системы ОДУ происходит при использовании активной защиты от неблагоприятных последствий кибератак. В качестве реакции системы на кибератаку возможны сбои (самовосстанавливающиеся) в функциональности системы ОДУ. Интенсивность отказов не приводит к значительным ошибкам в функционировании системы ОДУ.
Высокий $H,[0.8,0.95]$	Адаптация и реагирование системы ОДУ при кибератаках происходит без отказов, отмечается приемлемая функциональность системы оперативно-диспетчерского управления, что обусловливает высокую вероятность безотказной работы.

Таблица 4

Уровни восстановления

Уровень/ диапазон изменения ФП	Описание
Низкий $L,[0,0.24]$	Интенсивность восстановления и вероятность восстановления низкая. Среднее время восстановления способности системы ОДУ к выполнению i-й функции после отказа может привести к ошибкам и значительным задержкам управления.
Средний $M,[0.25,0.79]$	Интенсивность восстановления средняя. Среднее время восстановления способности системы ОДУ к выполнению функций после отказа не приводит к значительным ошибкам и задержкам управления.
Высокий $H,[0.8,0.95]$	Интенсивность восстановления позволяет выполнение всех функций оперативного управления в режиме реального времени. Вероятность восстановления высокая.

Таблица 5

Уровни киберустойчивости

Уровень/диапазон изменения ФП	Описание
Низкий $L,[0,0.24]$	Реализация функций оперативного управления в условиях кибератак низкая. Опасность возникновения в системе ОДУ отказов и сбоев высокая. Сочетание отказов компонентов и/или ошибок функциональности системы управления может привести к значительным нарушениям функционирования ЭЭС.
Средний $M,[0.25,0.79]$	В результате кибератак возможны незначительные сбои и ошибки в управлении, которые устранимы и не оказывают критического влияния на функциональность системы ОДУ. Реализация функций оперативного управления осуществляется в требуемом объеме и не приводит к нарушениям функционирования ЭЭС.
Высокий $H,[0.8,0.95]$	Влияние кибератак не приводит к отказам и сбоям системы ОДУ. Срабатывают все меры по обеспечению киберустойчивости. Функциональность системы управления высокая.

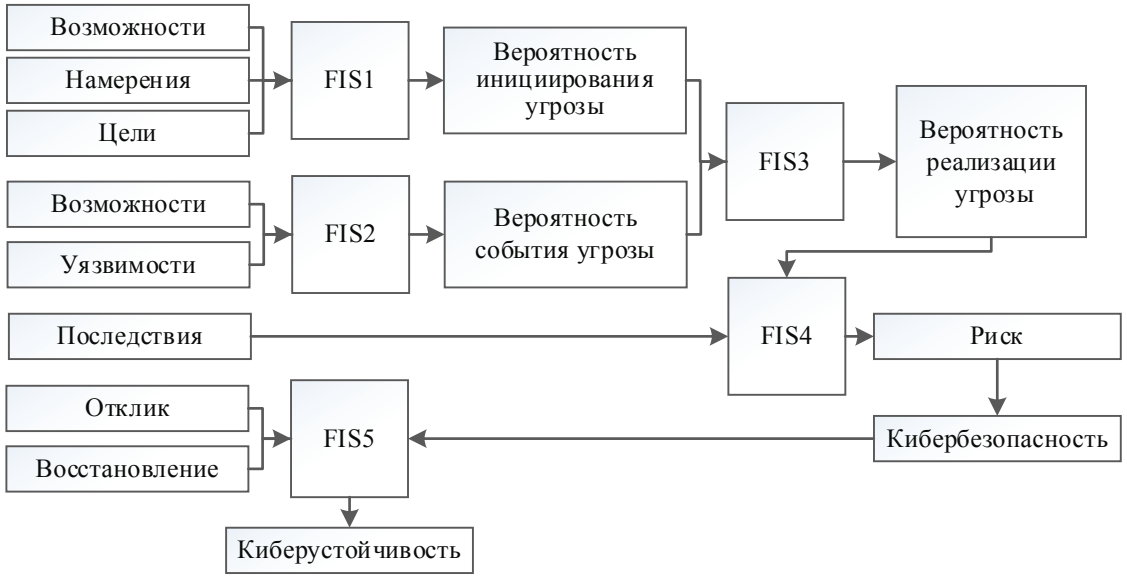

Рис. 2. Оценка киберустойчивости системы оперативно-диспетчерского управления ЭЭС

Уровни входных лингвистических переменных $\tilde{R}_1$, $\tilde{R}_2$, $\tilde{R}_3$ определяют уровень выходной лингвистической переменной $\tilde{R}$ на основе разработанной иерархической нечеткой системы, описание которой приведено в следующем разделе.

Учитывая влияние кибератак на функции оперативного управления (табл. 1), становится важным обеспечить более быстрые отклик и восстановление системы управления, которые могут быть охарактеризованы наименьшей интенсивностью отказов λ_S и максимальной интенсивностью восстановления системы μ_S соответственно:

$$\lambda_S = \frac{1}{MTBF}, \quad (2)$$

$$\mu_S = \frac{1}{MTTR}, \quad (3)$$

где $MTBF$ — средняя наработка системы на отказ, $MTTR$ — среднее время восстановления системы [21].

Уровень киберустойчивости системы ОДУ можно определить ее способностью смягчать последствия кибератаки, т.е. приемлемым уровнем кибербезопасности, а также вероятностью безотказной работы и вероятностью восстановления системы ОДУ при кибератаках, определяемые согласно следующим выражениям при экспоненциальном законе распределения времени безотказной работы

$$P_{R_2} = e^{-\lambda t}, \quad (4)$$

$$P_{R_3} = 1 - e^{-\mu t}, \quad (5)$$

позволяющим дать представление об уровнях отклика и восстановления.

На основе выше изложенного разработан алгоритм оценки киберустойчивости системы ОДУ ЭЭС при кибератаках.

4. Алгоритм оценки киберустойчивости системы ОДУ ЭЭС

С учетом факторов обеспечения киберустойчивости (рис. 1) алгоритм оценки киберустойчивости состоит из следующих этапов:

1. Оценка уровня риска кибербезопасности $\tilde{R}_4$ [14].

2. Оценка уровня кибербезопасности как показателя смягчения и подавления при реализованной киберугрозе:

$$\tilde{R}_1 = 1 - \tilde{R}_4, \quad (6)$$

3. Оценка уровня отклика $\tilde{R}_2$ при нарушении кибербезопасности.

4. Оценка уровня восстановления $\tilde{R}_3$ при нарушении кибербезопасности.

5. Оценка показателя киберустойчивости $\tilde{R}$.

Все факторы, как и киберустойчивость, описываются лингвистическими переменными, для каждого из них определены терм-множества (табл. 2-5) с соответствующим семантическим описанием с учетом данных табл. 1.

Для определения показателя киберустойчивости системы ОДУ ЭЭС согласно модели (1) разработана иерархическая нечеткая система, в которой заложены системы нечеткого логического вывода Мамдани $FIS_i, \left(i = \overline{1,5}\right)$, представленная на рис. 2.

Пример

Для получения оценки киберустойчивости системы ОДУ ЭЭС рассмотрено разрушающее событие в виде DoS-атаки на систему передачи информации. Значения входных лингвистических переменных факторов, определяющих уровень риска кибербезопасности системы ОДУ представлены в таблице 6. При нарушении кибербезопасности условно заданы интенсивность отказа системы $\lambda_S = 0,002$, интенсивность восстановления системы $\mu_S = 0,5$, продолжительность работы системы (Operating time) $t = 100$ час.

На основе алгоритма оценки риска управления ЭЭС получен показатель риска $\tilde{R}_4 = 0.64$ (уровень риска — средний). Согласно (6) определено значение показателя кибербезопасности $\tilde{R}_1 = 0.36$ (уровень кибербезопасности — средний).

Таблица 6

Входные лингвистические переменные, определяющие уровень риска

Факторы	DoS-атака
Возможности	0,8
Намерения	0,81
Цели	0,65
Уязвимости	0,72
Последствия	0,89

Для определения показателей отклика и восстановления вычислим вероятность безотказной работы системы и вероятность восстановления по выражениям (4) и (5): $P_{\tilde{R}_2} = 0.82$ — высокий уровень отклика, $P_{\tilde{R}_3} = 1$ — высокий уровень восстановления.

Отсюда, показатель киберустойчивости $\tilde{R} = 0.84$, что показывает высокий уровень функциональности системы ОДУ, несмотря на нарушения кибербезопасности.

Выводы

В статье рассмотрена проблема обеспечения киберустойчивости системы ОДУ ЭЭС. Проведен анализ причин нарушения киберустойчивости и последствий, к которым могут привести разрушающие события в результате кибератак. Показано, что такие факторы, как кибербезопасность, отклик и восстановление системы обеспечивают киберустойчивость. С учетом этого предложена нечеткая модель киберустойчивости системы ОДУ ЭЭС. Разработан алгоритм оценки показателей киберустойчивости системы ОДУ ЭЭС, использование которого на практике позволит, в дальнейшем, разработать эффективные меры как по обеспечению киберустойчивости, так и по снижению рисков кибербезопасности системы ОДУ ЭЭС.

Литература

1. R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan and L. Mihet-Popa. Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications. IEEE Access. 2020, vol. 8, pp. 151019-151064. DOI: 10.1109/ACCESS.2020.3016826.
2. X. Chu, M. Tang, H. Huang and L. Zhang. A security assessment scheme for interdependent cyber-physical power systems. 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS). 2017, pp. 816-819. DOI: 10.1109/ICSESS.2017.8343036.
3. Voropai N. Electric Power System Transformations: A Review of Main Prospects and Challenges. Energies. 2020, vol.13. No.21. DOI: 10.3390/en13215639
4. N. Jacobs, S. Hossain-McKenzie and E. Vugrin. Measurement and Analysis of Cyber Resilience for Control Systems: An Illustrative Example. 2018 Resilience Week (RWS). 2018, pp. 38-46. DOI: 10.1109/RWEEK.2018.8473549.
5. M. Touhiduzzaman, S. N. G. Gourisetti, C. Eppinger and A. Somani. A Review of Cybersecurity Risk and Consequences for Critical Infrastructure. 2019 Resilience Week (RWS). 2019, pp. 7-13. DOI: 10.1109/RWS47064.2019.8971975.
6. I. Zografopoulos, J. Ospina, X. Liu and C. Konstantinou. Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies. IEEE Access. 2021, vol. 9, pp. 29775-29818. DOI: 10.1109/ACCESS.2021.3058403.
7. J. Zuo, Z. Guo, J. Gan and Y. Lu. Enhancing Continuous Service of Information Systems Based on Cyber Resilience. 2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC). 2021, pp. 535-542. DOI: 10.1109/DSC53577.2021.00085.
8. Shady S. Refaat, Omar Ellabban, Sertac Bayhan, Haitham Abu-Rub, Frede Blaabjerg, Miroslav M. Begovic. Smart Grid Information Security. Smart Grid and Enabling Technologies, IEEE. 2021, pp.229-248. DOI: 10.1002/9781119422464.ch9.
9. E. U. Haq, H. Xu, L. Pan and M. I. Khattak. Smart Grid Security: Threats and Solutions. 2017 13th International Conference on Semantics, Knowledge and Grids (SKG). 2017, pp. 188-193. DOI: 10.1109/SKG.2017.00039.
10. I. Friedberg, K. McLaughlin and P. Smith. A cyber-physical resilience metric for smart grids. 2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). 2017, pp. 1-5. DOI: 10.1109/ISGT.2017.8086065.
11. A. S. Musleh, H. M. Khalid, S. M. Muyeen and A. Al-Durra. A Prediction Algorithm to Enhance Grid Resilience Toward Cyber Attacks in WAMCS Applications. IEEE Systems Journal. March 2019, vol. 13, no. 1, pp. 710-719. DOI: 10.1109/JSYST.2017.2741483.
12. S. Hopkins, E. Kalaimannan and C. S. John. Cyber Resilience using State Estimation Updates Based on Cyber Attack Matrix Classification. 2020 IEEE Kansas Power and Energy Conference (KPEC). 2020, pp. 1-6. DOI: 10.1109/KPEC47870.2020.9167652.
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. 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.
15. M. A. Haque, S. Shetty, B. Krishnappa. ICS-CRAT: A Cyber Resilience Assessment Tool for Industrial Control Systems. 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS). 2019, pp. 273-281. DOI: 10.1109/BigDataSecurity-HPSC-IDS.2019.00058.
16. Колосок И.Н., Гурина Л.А. Повышение кибербезопасности интеллектуальных энергетических систем методами оценивания состояния // Вопросы кибербезопасности. 2018. № 3(27). С. 63–69. DOI: 10.21681/2311-3456-2018-3-63-69.
17. Жуков А.В., Сацук Е.И., Дубинин Д.М., Опалев О.Л., Уткин Д.Н. Вопросы применения технологии синхронизированных векторных измерений для задач мониторинга эксплуатационного состояния электрооборудования // Энергетик. 2017. №9. С. 3-8.
18. Jia Guo, Yifei Wang, Chuangxin Guo, Shufeng Dong and Baijian Wen. Cyber-Physical Power System (CPPS) reliability assessment considering cyber attacks against monitoring functions. 2016 IEEE Power and Energy Society General Meeting (PESGM). 2016, pp. 1-5. DOI: 10.1109/PESGM.2016.7741899.
19. 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.
20. Успенский М.И. Составляющие надежности информационной сети системы мониторинга переходных режимов // Методические вопросы исследования надежности больших систем энергетики. 2020. С. 370-379.
21. Tong, Q., Yang, M., & Zinetullina, A. A Dynamic Bayesian Network-based approach to Resilience Assessment of Engineered Systems. Journal of Loss Prevention. Process Industries. 2020. 104152. DOI:10.1016/j.jlp.2020.104152.

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

ASSESSMENT OF CYBER RESILIENCE OF OPERATIONAL DISPATCH CONTROL SYSTEM OF EPS [2]

Gurina L.A. [3]

The research objective *is to develop an algorithm for assessing the cyber resilience of the operational dispatch control (ODC) system of electric power system (EPS) during cyberattacks on data collecting, processing, and transmitting systems.*

The research methods *include the probabilistic methods, fuzzy set theory methods, and methods of EPS reliability analysis.*

Result of the research: *the impact of cyberattacks on the functionality of the EPS ODC system is analyzed. The factors ensuring the cyber resilience of the EPS ODC system in the case of materialization of cyber threats are identified. A model of cyber resilience of the EPS ODC system is proposed. An algorithm for assessing the cyber resilience of the EPS ODC system is developed factoring in the cybersecurity risks.*

Keywords: *data collection, processing and transmission system; cybersecurity risk; control system; functionality; cyberattacks; fuzzy model.*

References

1. R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan and L. Mihet-Popa. Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications. IEEE Access. 2020, vol. 8, pp. 151019-151064. DOI: 10.1109/ACCESS.2020.3016826.
2. X. Chu, M. Tang, H. Huang and L. Zhang. A security assessment scheme for interdependent cyber-physical power systems. 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS). 2017, pp. 816-819. DOI: 10.1109/ICSESS.2017.8343036.
3. Voropai N. Electric Power System Transformations: A Review of Main Prospects and Challenges. Energies. 2020, vol.13. No.21. DOI: 10.3390/en13215639
4. N. Jacobs, S. Hossain-McKenzie and E. Vugrin. Measurement and Analysis of Cyber Resilience for Control Systems: An Illustrative Example. 2018 Resilience Week (RWS). 2018, pp. 38-46. DOI: 10.1109/RWEEK.2018.8473549.
5. M. Touhiduzzaman, S. N. G. Gourisetti, C. Eppinger and A. Somani. A Review of Cybersecurity Risk and Consequences for Critical Infrastructure. 2019 Resilience Week (RWS). 2019, pp. 7-13. DOI: 10.1109/RWS47064.2019.8971975.
6. I. Zografopoulos, J. Ospina, X. Liu and C. Konstantinou. Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies. IEEE Access. 2021, vol. 9, pp. 29775-29818. DOI: 10.1109/ACCESS.2021.3058403.
7. J. Zuo, Z. Guo, J. Gan and Y. Lu. Enhancing Continuous Service of Information Systems Based on Cyber Resilience. 2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC). 2021, pp. 535-542. DOI: 10.1109/DSC53577.2021.00085.
8. Shady S. Refaat, Omar Ellabban, Sertac Bayhan, Haitham Abu-Rub, Frede Blaabjerg, Miroslav M. Begovic. Smart Grid Information Security. Smart Grid and Enabling Technologies, IEEE. 2021, pp.229-248. DOI: 10.1002/9781119422464.ch9.
9. E. U. Haq, H. Xu, L. Pan and M. I. Khattak. Smart Grid Security: Threats and Solutions. 2017 13th International Conference on Semantics, Knowledge and Grids (SKG). 2017, pp. 188-193. DOI: 10.1109/SKG.2017.00039.
10. I. Friedberg, K. McLaughlin and P. Smith. A cyber-physical resilience metric for smart grids. 2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). 2017, pp. 1-5. DOI: 10.1109/ISGT.2017.8086065.
11. A. S. Musleh, H. M. Khalid, S. M. Muyeen and A. Al-Durra. A Prediction Algorithm to Enhance Grid Resilience Toward Cyber Attacks in WAMCS Applications. IEEE Systems Journal. March 2019, vol. 13, no. 1, pp. 710-719. DOI: 10.1109/JSYST.2017.2741483.
12. S. Hopkins, E. Kalaimannan and C. S. John. Cyber Resilience using State Estimation Updates Based on Cyber Attack Matrix Classification. 2020 IEEE Kansas Power and Energy Conference (KPEC). 2020, pp. 1-6. DOI: 10.1109/KPEC47870.2020.9167652.
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. Kolosok I.N., Gurina L.A. Ocenka riskov upravleniya kiberfizicheskoj EES na osnove teorii nechetkih mnozhestv // Metodicheskie voprosy issledovaniya nadezhnosti bol'shih sistem energetiki [Methodological problems reliability study of large energy systems], v 2-h knigah, 2019, pp. 238-247.

2 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.

3 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

15. M. A. Haque, S. Shetty, B. Krishnappa. ICS-CRAT: A Cyber Resilience Assessment Tool for Industrial Control Systems. 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS). 2019, pp. 273-281. DOI: 10.1109/BigDataSecurity-HPSC-IDS.2019.00058.
16. Kolosok I.N., Gurina L.A. Povyshenie kiberbezopasnosti intellektual'nyh energeticheskih sistem metodami ocenivaniya sostoyaniya // Voprosy kiberbezopasnosti [Cybersecurity issues], 2018, № 3(27), pp. 63-69. DOI: 10.21681/2311-3456-2018-3-63-69.
17. Zhukov A.V., Saczuk E.I., Dubinin D.M., Opalev O.L., Utkin D.N. Voprosy` primeneniya texnologii sinxronizirovanny`x vektorny`x izmerenij dlya zadach monitoringa e`kspluatacionnogo sostoyaniya e`lektrooborudovaniya // E`nergetik [Energetik], 2017. № 9, pp. 3-8.
18. Jia Guo, Yifei Wang, Chuangxin Guo, Shufeng Dong and Baijian Wen. Cyber-Physical Power System (CPPS) reliability assessment considering cyber attacks against monitoring functions. 2016 IEEE Power and Energy Society General Meeting (PESGM). 2016, pp. 1-5. DOI: 10.1109/PESGM.2016.7741899.
19. 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.
20. Uspenskij M.I. Sostavlyayushchie nadezhnosti informacionnoj seti sistemy monitoringa perekhodnyh rezhimov // Metodicheskie voprosy issledovaniya nadezhnosti bol'shih sistem energetiki [Methodological problems reliability study of large energy systems], 2020, pp. 370-379.
21. Tong, Q., Yang, M., & Zinetullina, A. A Dynamic Bayesian Network-based approach to Resilience Assessment of Engineered Systems. Journal of Loss Prevention. Process Industries. 2020. 104152. DOI:10.1016/j.jlp.2020.104152.