УДК 621.311 : 004.056

ОЦЕНКА РИСКОВ КИБЕРБЕЗОПАСНОСТИ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ ИНТЕЛЛЕКТУАЛЬНОЙ ЭНЕРГЕТИЧЕСКОЙ СИСТЕМЫ[1]

Колосок Ирина Николаевна

Д.т.н., ведущий научный сотрудник лаборатории «Управление функционированием электроэнергетических систем», e-mail: kolosok@isem.irk.ru

Гурина Людмила Александровна

К.т.н., доцент, научный сотрудник лаборатории «Управление функционированием электроэнергетических систем» , e-mail: gurina@isem.irk.ru

Институт систем энергетики им. Л.А. Мелентьева СО РАН,

664130 г. Иркутск, ул. Лермонтова 130

Аннотация. Парадигма цифровой энергетики ориентирована на создание кибер-физических систем и широкомасштабное использование технологий Smart Grid. Наряду с большими возможностями такого перехода отмечается чувствительность интеллектуальной энергосистемы (ИЭС) к все возрастающим киберугрозам. Необходимость обеспечения и сохранения надежного функционирования ИЭС в условиях внешних и внутренних кибер-атак требует анализа и учета возможных рисков кибербезопасности ИЭС и разработки дальнейших мер ее поддержания. В данной работе рассмотрена информационно-коммуникационная инфраструктура ИЭС и проанализированы свойства кибербезопасности SCADA, WAMS, являющихся частью инфраструктуры. Особое внимание уделено анализу факторов риска кибербезопасности, учитываемых в дальнейшем при разработке алгоритма оценки рисков кибербезопасности информационно-коммуникационной инфраструктуры ЭЭС на основе теории нечетких множеств, что является (результат исследования авторов). Работоспособность алгоритма в условиях неопределенности показывает его эффективность.

Ключевые слова: риск, кибербезопасность, система SCADA, WAMS, электроэнергетическая система.

Цитирование: Колосок И.Н., Гурина Л.А. Оценка рисков кибербезопасности информационно-коммуникационной инфраструктуры интеллектуальной энергетической системы // Информационные и математические технологии в науке и управлении. 2019. № 2 (14). С. 40–51. DOI: 10.25729/2413-0133-2019-2-04

Введение. Внедрение новых информационных и коммуникационных технологий в электроэнергетические системы (ЭЭС) обеспечивает развитие системы в рамках концепции Smart Grid (интеллектуальной энергосистемы (ИЭС)) и создание кибер-физической системы, что привносит много преимуществ. В то же время появляются новые риски кибербезопасности. Характер взаимодействия кибер-уровня (информационно-коммуникационной системы) с физическим уровнем (генерация-передача-распределение)

[1] Работа выполнена в рамках научного проекта III.17.4.2. программы фундаментальных исследований СО РАН, рег. № АААА-А17-117030310438-1

усиливает зависимость функционирования физической системы от растущих угроз киберфизической системе в целом и успешно использованных злоумышленниками уязвимостей компонентов кибер-системы, в частности [17, 5]. Появилась необходимость оценки кибербезопасности информационно-коммуникационной системы на основе риск-ориентированного подхода.

Управление ЭЭС осуществляется на основе данных, поступающих от системы SCADA и WAMS, входящих в информационно-коммуникационную систему. Проведенный анализ источников угроз, уязвимостей и возможных кибератак на систему управления позволил выделить свойства системы SCADA и WAMS как критически важных объектов в киберпространстве. При этом основное внимание было уделено не способам защиты, а сохранению системой управления выполнения своих основных функций при кибератаках [3, 10, 12–14].

В статье рассмотрен алгоритм оценки рисков кибербезопасности информационно-коммуникационной инфраструктуры ЭЭС на основе теории нечетких множеств. Достоинством данного подхода является возможность адаптивного и гибкого управления в зависимости от уровней риска.

Информационно-коммуникационная инфраструктура ИЭС. Информационно-коммуникационная инфраструктура включает в себя информационные и коммуникационные системы и сервисы, а также информацию, содержащуюся в этих системах и сервисах. Она состоит из аппаратного и программного обеспечения, которое обрабатывает, хранит и передает информацию, требуемую при управлении физической системой [6,9]. Кроме этого, компьютерные системы, системы управления (SCADA, WAMS), сети, такие, как Интернет и кибер-сервисы также являются частью информационно-коммуникационной инфраструктуры, что повышает ее уязвимость к кибератакам.

В традиционных IT-системах требованиями информационной безопасности является сохранение конфиденциальности, целостности, доступности (CIA) систем передачи информации [9, 18].

Поскольку системы SCADA и WAMS являются жесткими системами реального времени [7, 1], а завершение операции после ее крайнего срока считается бесполезным и потенциально может вызвать каскадный эффект в физическом системе, то, в дополнение к перечисленным требованиям при оценке риска, необходимо учитывать своевременность и киберустойчивость [8] для поддержания надежного функционирования ЭЭС.

Отсюда, требования к кибербезопасности информационно-коммуникационной инфраструктуры (SCADA, WAMS) следующие:

1. Своевременность (оперативность отправления, передачи, получения данных) явно выражает критичность по времени систем управления, заданную в результате того, что она является системой реального времени, и параллелизм в системах SCADA, WAMS из-за широко рассредоточенных распределенных систем. В более общем смысле, это свойство означает, что любая запрашиваемая, сообщаемая, выдаваемая и распространяемая информация не должна быть устаревшей, а соответствовать реальному времени.
2. Доступность означает, что любой компонент системы SCADA,WAMS должен быть готовым к использованию, когда необходимо.

3. Целостность требует, чтобы данные генерировались, передавались, отображались, хранились в системе SCADA, WAMS, будучи подлинными и неповрежденными из-за несанкционированного вмешательства.
4. Конфиденциальность относится к тому, что постороннее лицо не должно иметь никакого доступа к информации, относящейся к конкретной системе SCADA, WAMS. Конфиденциальность имеет второстепенное значение для целостности данных. Однако конфиденциальность важной информации, такой как пароли, ключи шифрования, подробная конфигурация системы и т.д., должна быть на первом месте, когда речь идет о проблемах безопасности в промышленности.
5. Киберустойчивость – это способность системы сдерживать локальное воздействие кибератак, идентифицировать и задерживать поток искаженных данных в пределах области, подверженной кибератаке, без дальнейшей передачи и использования этих данных при управлении физической подсистемой, чтобы не привести к возникновению аварийных ситуаций вплоть до развития крупных системных аварий.

Все эти требуемые свойства кибербезопасности не являются взаимоисключающими, но тесно связаны. Например, нарушая целостность, злоумышленник может изменить управляющие сигналы, чтобы вызвать неисправность компонентов SCADA и WAMS, что может в конечном итоге повлиять на доступность. В целом, строгое принудительное управление доступом может также обеспечить конфиденциальность, целостность, доступность, своевременность и киберустойчивость системы. Различие требуемых свойств информационной безопасности и кибербезопасности кибер-инфораструктуры связано с тем, что система SCADA и WAMS должны работать в режиме реального времени и постоянно функционировать.

Поэтому оценка рисков кибербезопасности ИЭС должна включать все перечисленные требования кибербезопасности информационно-коммуникационной инфраструктуры ИЭС.

Оценка рисков кибербезопасности информационно-коммуникационной инфраструктуры. Риск кибербезопасности - это вероятность нежелательного исхода в результате инцидента, события или происшествия, определяемая его вероятностью и нанесенным ущербом [2]. Этот риск является одним из компонентов организационного риска, который может включать в себя многие виды риска (напр., инвестиционный риск, риск управления программой, риск безопасности и т.д.).

Оценку риска предлагается проводить на основе теории нечетких множеств [15]. В качестве входных лингвистических переменных факторов риска рассмотрены:

x_1 - возможности противника;

x_2 - намерения противника;

x_3 - цели противника;

x_4 - уязвимости информационно-коммуникационной системы;

x_5 - воздействия на информационно-коммуникационную систему.

Выходными лингвистическими переменными являются:

y_1 - вероятность инициирования угрозы;

y_2 - вероятность события угрозы;

y_3 - полная вероятность реализации угрозы;

R - риск.

Для каждой лингвистической переменной определены терм-множества $\{VL, L, M, H, CH\}$, где VL - очень низкий уровень с диапазоном значений функции принадлежности [0;0.04]; L - низкий уровень с диапазоном значений функции принадлежности [0.05;0.2]; M - средний уровень с диапазоном значений функции принадлежности [0.21;0.79]; H - высокий уровень с диапазоном значений функции принадлежности [0.8;0.95]; CH - критически высокий уровень с диапазоном значений функции принадлежности [0.96;1]. Семантические описания терм-множеств для каждого фактора риска, как и для самого риска проводилось с учетом [16] и представлены в табл. 1-8.

Такие факторы как возможности, намерения и цели противника использованы для оценки вероятности инициирования угрозы (y_1). Сочетания факторов, таких как возможности противника и уязвимости информационно-коммуникационной инфраструктуры использованы для оценки вероятности события угрозы как результат неблагоприятного воздействия (y_2). Комбинация этих вероятностей была использована для определения полной вероятности реализации угрозы (y_3) согласно с заданными правилами нечеткого вывода. Наконец, сочетания полной вероятности реализации угроз и уровней воздействий на информационно-коммуникационную систему позволяют получить оценку риска кибербезопасности.

Таблица 1. Возможности противника

Уровень	Описание
Очень низкий	У противника очень ограниченные ресурсы, опыт и возможности для проведения успешной атаки.
Низкий	Противник имеет ограниченные ресурсы, опыт и возможности для проведения успешной атаки.
Средний	У противника есть умеренные ресурсы, опыт и возможности для проведения нескольких успешных атак.
Высокий	Противник обладает сложным опытом, обладающим значительными ресурсами и возможностями проведения нескольких успешных скоординированных атак.
Критически высокий	Противник обладает очень сложным уровнем знаний, обладает достаточными ресурсами и может создавать возможности проведения нескольких успешных, непрерывных и скоординированных атак.

Таблица 2. Намерения противника

Уровень	Описание
Очень низкий	Злоумышленник стремится нарушить или уничтожить киберресурсы информационно-коммуникационной системы и делает это, не беспокоясь об обнаружении атаки
Низкий	Злоумышленник активно стремится получить критическую или конфиденциальную информацию или разрушить киберресурсы информационно-коммуникационной системы и делает это, не беспокоясь об обнаружении атаки
Средний	Противник пытается получить или изменить конкретную критическую или конфиденциальную информацию или разрушить киберресурсы организации, установив точку доступа в информационно-коммуникационных системах. Противник стремится минимизировать обнаружение атаки, особенно при проведении атак в течение длительных периодов времени. Противник стремится помешать выполнению функций управления
Высокий	Злоумышленник стремится подорвать/помешать критическим аспектам выполнения основных целей или функций управления, программ или создать условия, способствующие сделать это в будущем, поддерживая доступ в информационно-коммуникационной системе. Противник очень обеспокоен тем, чтобы свести к минимуму обнаружение кибератаки, особенно при подготовке к будущим атакам.
Критически высокий	Противник пытается подорвать, серьезно затруднить или уничтожить выполнение основных функций, программ, используя доступ к информационно-коммуникационной системе. Противник обеспокоен раскрытием методов разведки только в той мере, в какой это будет препятствовать его возможностям завершить запланированные действия.

Таблица 3. Цели противника

Уровень	Описание
Очень низкий	У противника может быть и не быть цели проведения кибератаки на какие-либо конкретные организации или группы организаций.
Низкий	Противник использует общедоступную информацию для определения цели в группе интересующих его организаций или информации и ищет возможности осуществления кибератаки в этой группе.
Средний	Противник анализирует общедоступную информацию для осуществления кибератаки на информационно-коммуникационную систему, программное обеспечение или информацию.
Высокий	Противник анализирует информацию, полученную с помощью разведки, для постоянного доступа к информационно-коммуникационной системе, программному обеспечению или функциям управления, уделяя особое внимание критически важной информации, ресурсам или функциям, конкретным сотрудникам, поддерживающим эти функции.
Критически высокий	Противник анализирует информацию, полученную с помощью разведки для постоянного проведения кибератак в отношении информационно-коммуникационной системы, программного обеспечения, функций управления, ориентируясь на конкретную критически важную информацию, функции, конкретных сотрудников, взаимодействующие организации.

Таблица 4. Уязвимости информационно-коммуникационной системы

Уровень	Описание
Очень низкий	Уязвимость не вызывает беспокойства.
Низкий	Уязвимость вызывает незначительную озабоченность, но эффективность исправления может быть улучшена.
Средний	Уязвимость представляет собой умеренную озабоченность, основанную на подверженности уязвимости и простоте эксплуатации и/или на серьезности воздействий, которые могут возникнуть в результате ее использования.
Высокий	Уязвимость вызывает серьезную озабоченность на основе выявления уязвимости и простоты эксплуатации и/или серьезности воздействий, которые могут возникнуть в результате ее использования.
Критически высокий	Уязвимость не защищена и доступна, и ее эксплуатация может привести к серьезным последствиям.

Таблица 5. Воздействия на информационно-коммуникационную систему

Уровень	Описание
Очень низкий	Ожидается, что событие, связанное с угрозой, окажет незначительное негативное влияние на операции управления кибер-физической системой.
Низкий	Ожидается, что событие угрозы будет иметь ограниченное неблагоприятное воздействие на операции управления кибер-физической-системой.
Средний	Ожидается, что событие угрозы будет иметь серьезные неблагоприятные последствия для операций управления кибер-физической системой.
Высокий	Ожидается, что событие, связанное с угрозой, окажет серьезное или катастрофическое неблагоприятное воздействие на операции управления кибер-физической системой.
Критически высокий	Ожидается, что событие угрозы будет иметь многочисленные серьезные или катастрофические неблагоприятные последствия для кибер-физической системы.

Таблица 6. Вероятность инициирования события угрозы

Уровень	Описание
Очень низкий	Маловероятно, что противник инициирует событие угрозы.
Низкий	Противник вряд ли инициирует событие угрозы.
Средний	Вероятно, противник инициирует событие угрозы.
Высокий	Противник скорее всего инициирует событие угрозы.
Критически высокий	Противник почти наверняка инициирует событие угрозы.

Таблица 7. Вероятность события угрозы

Уровень	Описание
Очень низкий	Если событие угрозы инициируется или происходит, оно, с низкой вероятностью, будет иметь неблагоприятные последствия.
Низкий	Если событие угрозы инициируется или происходит, оно, маловероятно, будет иметь неблагоприятные последствия.

Средний	Если событие угрозы инициируется или происходит, оно, с некоторой степенью вероятности, будет иметь неблагоприятные последствия.
Высокий	Если событие угрозы инициируется или происходит, оно, с высокой вероятностью, будет иметь неблагоприятные последствия.
Критически высокий	Если событие угрозы инициируется или происходит, оно почти наверняка будет иметь неблагоприятные последствия.

Таблица 8. Уровни риска

Уровень	Описание
Очень низкий	Очень низкий риск означает, что можно ожидать, что событие угрозы будет иметь незначительное неблагоприятное воздействие на кибер-физическую систему.
Низкий	Низкий риск означает, что угрожающее событие может иметь ограниченное неблагоприятное воздействие на кибер-физическую систему.
Средний	Умеренный риск означает, что опасное событие может оказать серьезное неблагоприятное воздействие на кибер-физическую систему.
Высокий	Высокий риск означает, что угрожающее событие может иметь серьезное или катастрофическое неблагоприятное воздействие на кибер-физическую систему.
Критически высокий	Очень высокий риск означает, что можно ожидать, что событие угрозы может иметь многочисленные серьезные или катастрофические неблагоприятные последствия для кибер-физической системы.

Для оценки риска кибербезопасности информационно-коммуникационной инфраструктуры построена иерархическая нечеткая система (рис. 1). В основу предлагаемого алгоритма оценки риска заложены системы нечеткого логического вывода Мамдами (F_1, F_2, F_3, F_4) [4], реализуемые в MatLAB.

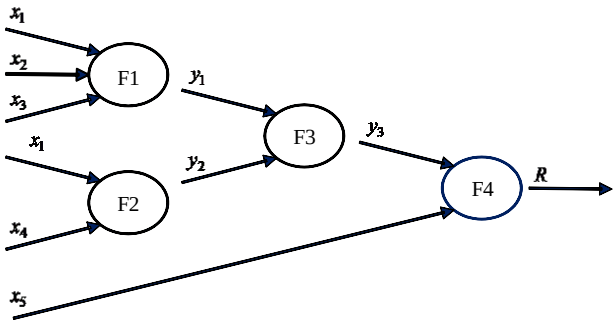

Рис. 1. Иерархическая нечеткая система оценки риска кибербезопасности информационно-коммуникационной инфраструктуры

Трехмерные поверхности зависимости выходных переменных от входных переменных, полученные с помощью GUI-модуля Surface Viewer, представлены на рис. 2-7.

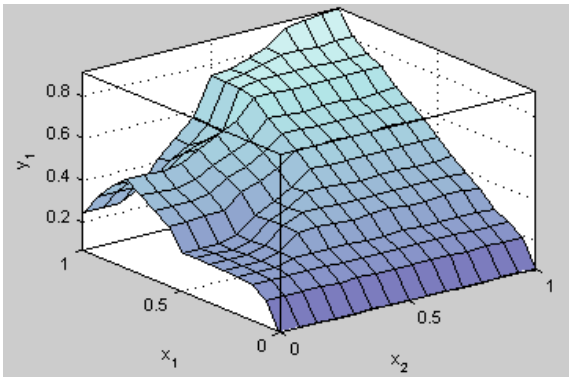

Рис. 2. Вероятность инициирования угрозы $y_1 = f(x_1, x_2)$ в зависимости от уровней возможностей и намерений противника

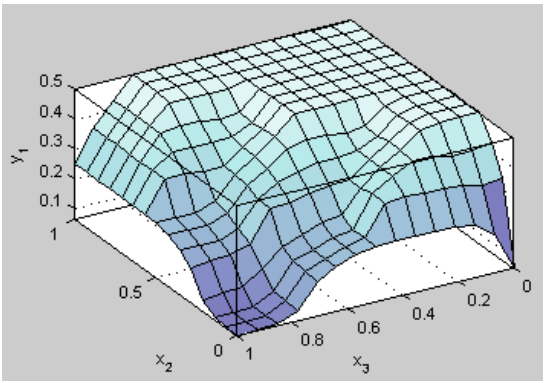

Рис. 3. Вероятность инициирования угрозы $y_1 = f(x_2, x_3)$ в зависимости от уровней намерений и целей противника

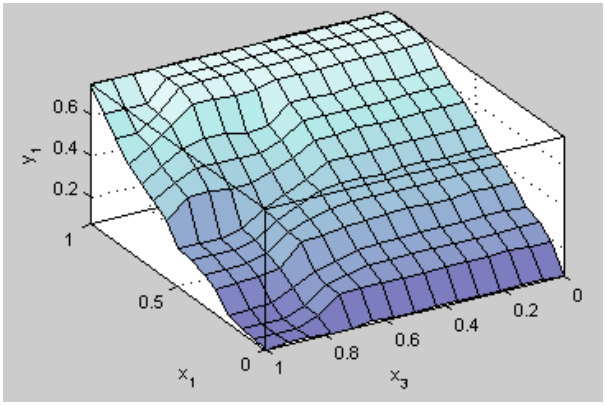

Рис. 4. Вероятность инициирования угрозы $y_1 = f(x_1, x_3)$ в зависимости от уровней возможностей и целей противника

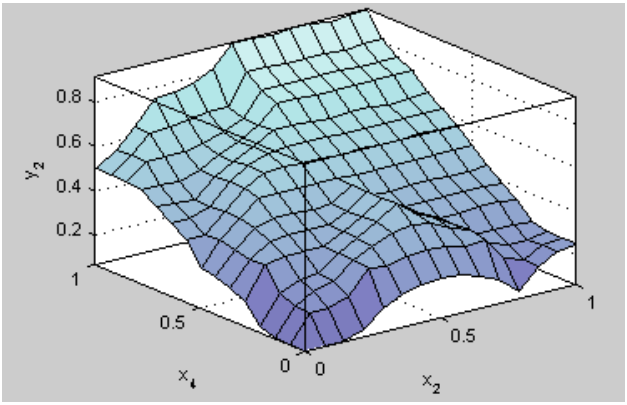

Рис. 5. Вероятность события угрозы $y_2 = f(x_1, x_4)$ в зависимости от уровней уязвимостей информационно-коммуникационной инфраструктуры и возможностей противника

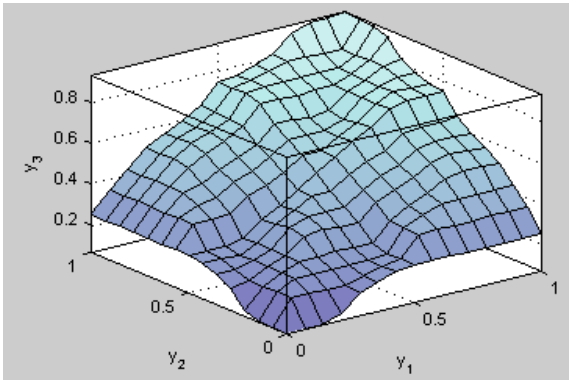

Рис. 6. Полная вероятность реализации угрозы $y_3 = f(y_1, y_2)$ в зависимости от уровней вероятности события угрозы и вероятности инициирования угрозы

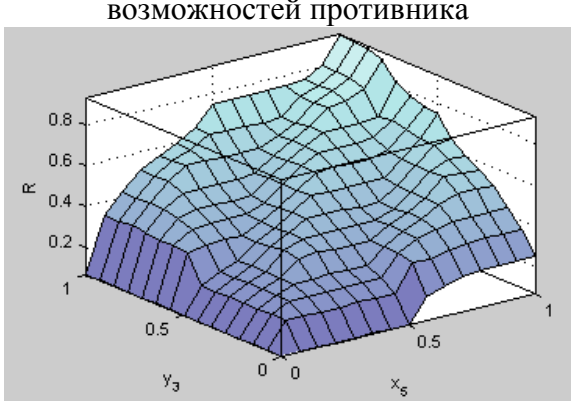

Рис. 7. Оценка риска $R = f(x_5, y_3)$ в зависимости от уровней воздействия и полной вероятности реализации угрозы

Пример. В качестве примера оценен риск кибербезопасности при jamming-атаке на систему WAMS [11]. При реализации такой кибератаки отмечена потеря таких свойств кибербезопасности, как доступность и своевременность передачи данных. Такие атаки могут нарушить работу системы и даже приводить к отказу системы.

Пусть входные переменные (намерения, возможности, цели противника, уязвимости и воздействия) имеют следующие значения: $x_1 = 0.82$ (высокий уровень), $x_2 = 0.75$ (средний уровень), $x_3 = 0.67$ (средний уровень), $x_4 = 0.84$ (высокий уровень), $x_5 = 0.91$ (высокий уровень).

При заданных входных переменных, определим выходные лингвистические переменные согласно правилам нечеткого вывода систем F_1, F_2, F_3, F_4. Вероятность инициирования угрозы $y_1 = 0.682$, вероятность события угрозы $y_2 = 0.756$, полная вероятность реализации угрозы $y_3 = 0.637$, оценка риска кибербезопасности при jamming-атаках $R = 0.667$.

Полученная оценка риска соответствует среднему уровню, и говорит о том, что опасное событие может оказать серьезное неблагоприятное воздействие на систему WAMS.

Заключение. Показана необходимость учета дополнительных требований кибербезопасности (своевременность, киберустойчивость) информационно-коммуникационной инфраструктуры ИЭС при оценке рисков.

Предложен алгоритм оценки риска кибербезопасности на основе теории нечетких множеств, применение которого особенно актуально в условиях неопределенности.

Анализ риска кибербезопасности информационно-коммуникационной инфраструктуры и его оценка важны для дальнейшего определения организационного риска при управлении ИЭС.

СПИСОК ЛИТЕРАТУРЫ

1. Аюев Б.И., Ерохин П.М., Куликов Ю.А. Система мониторинга переходных режимов ЕЭС/ОЭС // Технологии управления режимами энергосистем XXI века: Сб. докл. Всеросс. Научно-практ. конф. / Под ред. А.Г. Фишова. Новосибирск: Изд_во НГТУ. 2006. С. 83–92.
2. Дорофеев А.В., Марков А.С. Менеджмент информационной безопасности: основные концепции // Вопросы кибербезопасности. 2014. № 1 (2). С. 67–73.
3. Колосок И.Н., Гурина Л.А. Повышение кибербезопасности интеллектуальных энергетических систем методами оценивания состояния // Вопросы кибербезопасности. 2018. № 3 (27). С. 63–69. DOI:1021681/2311-3456-2018-3-63-69
4. Леоненков А.В. Нечеткое моделирование в среде MATLAB и fuzzyTECH. СПб.: БХВ-Петербург. 2005. 736 с.
5. Массель Л.В. Использование современных информационных технологий в Smart Grid как угроза кибербезопасности энергетических систем России // Information technology and security. Украина, Киев, Институт социальной связи и защиты информации НТУ Украины «КПИ». №1(3) 2013. С. 56–65.
6. Массель Л.В., Колосок И.Н., Гурина Л.А. Обработка информационных потоков при мониторинге и управлении режимами интеллектуальных электроэнергетических систем // Вестник ИрГТУ. 2013. №2(73). С. 30–35.
7. СТО 59012820.35.240.50.004-2011. Системы диспетчерского управления в электроэнергетике. Система сбора данных и оперативного контроля (SCADA) в диспетчерском управлении. Режим доступа: https://www.so-ups.ru (дата обращения 03.04.2019)
8. B. Zhu, A. Joseph and S. Sastry. A Taxonomy of Cyber Attacks on SCADA Systems // International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing. Dalian. 2011. Pp. 380–388. doi: 10.1109/iThings/CPSCom.2011.34.
9. FIPS 199 Standards for Security Categorization of Federal Information and Information Systems, February 2004.
10. Gurina L., Kolosok I. Calculation of cyber security index in the problem of power systems state estimation based on SCADA and WAMS measurements // Lecture Notes in Computer Science. 2016 Т. 8985. Pp. 172–177.

11. K. Gai, M. Qiu, Z. Ming, H. Zhao, and L. Qiu. Spoofing-Jamming Attack Strategy Using Optimal Power Distributions in Wireless Smart Grid Networks // IEEE Transactions on Smart Grid. 2017. Pp. 1–1.
12. Kolosok I., Gurina L. Cyber Security-Oriented Smart Grid State Estimation // E3S Web Conf. Vol. 69. 2018. Green Energy and Smart Grids (GESG 2018). Pp. 1–5. DOI: https://doi.org/10.1051/e3sconf/20186902004
13. Kolosok I., Gurina L. State Estimation of Electric Power System under DOS-attacks on SCADA system and WAMS // Proceedings of the Vth International workshop "Critical infrastructures: Contingency management, Intelligent, Agent-based, Cloud computing and Cyber security" (IWCI 2018). Advances in Intelligent Systems Research. vol. 158. 2018. Pp. 94–99. https://doi.org/10.2991/iwci-18.2018.17
14. Kolosok I., Korkina E., Gurina L. Vulnerability analysis of the state estimation problem under cyber attacks on WAMS // International Conference on Problems of Critical Infrastructures Joint 6th Conference of International Institute for Critical Infrastructures and 6th International Conference on Liberalization and Modernization of Power Systems. Edited by Z.A. Styczynski and N.I. Voropai. 2015. Pp. 73–84.
15. Ming-Chang Lee. Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method // International Journal of Computer Science & Information Technology (IJCSIT). 2014. Vol.6. No 1. Pp. 29–45. DOI: 10.5121/ijcsit.2014.6103
16. National Institute of Standards and Technology NIST Special Publication 800-30 rev. 1 (Sep. 2012), Guide for Conducting Risk Assessments.
17. Siddharth Sridhar, Adam Hahn, Manimaran Govindarasu. Cyber-Physical System Security for the Electric Power Grid // Proceedings of the IEEE. Vol. 100. No 1. January 2012. Pp. 210–224.
18. The Smart Grid Interoperability Panel Cyber Security Working Group, “Introduction to NISTIR7628 Guidelines for Smart Grid Cyber Security”. September 2010. Режим доступа: http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf (дата обращения 03.04.2019)

UDK 621.311 : 004.056

CYBERSECURITY RISK ASSESSMENT OF INFORMATION AND COMMUNICATION INFRASTRUCTURE OF INTELLIGENT ENERGY SYSTEM[2]

Irina N. Kolosok
Dr., Professor, Leading Researcher of Laboratory of Electric Power Systems Operation and Control, e-mail: kolosok@isem.irk.ru
Liudmila A. Gurina
PhD., Researcher of Laboratory of Electric Power Systems Operation and Control, e-mail: gurina@isem.irk.ru
Melentiev Energy Systems Institute Siberian Branch of the Russian Academy of Sciences
130, Lermontov Str., 664033, Irkutsk, Russia

Abstract. The digital energy paradigm is focused on the establishment of cyber-physical systems and the large-scale use of Smart Grid technologies. Apart from the great potential of such a transition, an intelligent energy system (IES) is noted to be sensitive to ever-increasing cyber threats. The need to ensure and maintain reliable IES operation in the event of external and internal cyber-intrusions requires an analysis and consideration of possible risks of the IES cybersecurity and the development of further measures to maintain it. This paper is focused on the information and communication infrastructure of the IES and cybersecurity properties of SCADA and WAMS, which are part of the infrastructure. Particular attention is paid to the analysis of cybersecurity risk factors that are further taken into account when developing a cybersecurity risk assessment algorithm of the information and communication infrastructure of the electric power system based on the theory of fuzzy sets, which is the result of the presented research. The performance of the algorithm under uncertainty demonstrates its effectiveness.

Key words: risk, cybersecurity, SCADA system, WAMS, electric power system.

References

1. Ayuev B.I., Erohin P.M., Kulikov YU.A. Sistema monitoringa perekhodnyh rezhimov EES/OES [UPS/IPS Wide Area Measurement System] // Tekhnologii upravleniya rezhimami energosistem XXI veka: Sb. dokl. Vseross. Nauchno-prakt. konf. / Pod red. A.G. Fishova = Technologies for managing power systems of the XXI century: Collection of reports of the All-Russian Scientific and Practical Conference / Ed. A.G. Fishov. Novosibirsk. Izd_vo NGTU = NSTU Publishing House. 2006. Pp. 83–92. (in Russian)
2. Dorofeev A.V., Markov A.S. Menedzhment informacionnoj bezopasnosti: osnovnye koncepcii [Cyber security management: basic concept] // Voprosy kiberbezopasnosti = Cybersecurity issues. 2014. № 1 (2). Pp. 67–73. (in Russian)

[2] The research has been carried out within the framework of the scientific project III.17.4.2. of the Program for Fundamental Research of SB RAS. Reg. No. AAAA-A17-117030310438-1

3. Kolosok I.N., Gurina L.A. Povyshenie kiberbezopasnosti intellektual'nyh energeticheskih sistem metodami ocenivaniya sostoyaniya [Improvement of Cybersecurity of Smart Grid by State Estimation Methods] // Voprosy kiberbezopasnosti = Cybersecurity issues**.** 2018. № 3 (27). Pp. 63–69. DOI:1021681/2311-3456-2018-3-63-69 (in Russian)
4. Leonenkov A.V. Nechetkoe modelirovanie v srede MATLAB i fuzzyTECH [Fuzzy simulation in MATLAB and fuzzyTECH]. St. Petersburg. BHV-Petersburg. 2005. 736 p. (in Russian)
5. Massel L.V. Ispol'zovaniye sovremennykh informatsionnykh tekhnologiy v Smart Grid kak ugroza kiberbezopasnosti energeticheskikh sistem Rossii [The use of modern information technology in SMART GRID as a threat to cyber security of the energy system of Russia // Information technology and security. Ukraine. Kiev. Institut sotsial'noy svyazi i zashchity informatsii NTU Ukrainy «KPI» = Institute of Special Communication and Information Security of National Technical University of Ukraine "Kyiv Polytechnic Institute" , №1(3) 2013. Pp. 56–65. (in Russian)
6. Massel' L.V., Kolosok I.N., Gurina L.A. Obrabotka informacionnyh potokov pri monitoringe i upravlenii rezhimami intellektual'nyh elektroenergeticheskih sistem [Information flow processing when monitor and control Smart Grid regimes] // Vestnik IrGTU = Proccedings of ISTU. 2013. №2(73). Pp. 30-35. (in Russian)
7. STO 59012820.35.240.50.004-2011. Sistemy dispetcherskogo upravleniya v elektroenergetike. Sistema sbora dannyh i operativnogo kontrolya (SCADA) v dispetcherskom upravlenii [Company Standard 59012820.35.240.50.004-2011. Dispatch control systems in electric power. The Supervisory Control And Data Acquisition (SCADA) in dispatch control]. Available at: https://www.so-ups.ru (accessed 03.04.2019) (in Russian)
8. B. Zhu, A. Joseph and S. Sastry. A Taxonomy of Cyber Attacks on SCADA Systems // 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing. Dalian. 2011. Pp. 380–388. doi: 10.1109/iThings/CPSCom.2011.34.
9. FIPS 199 Standards for Security Categorization of Federal Information and Information Systems, February 2004
10. Gurina L., Kolosok I. Calculation of cyber security index in the problem of power systems state estimation based on SCADA and WAMS measurements // Lecture Notes in Computer Science. 2016 T. 8985. Pp. 172–177.
11. K. Gai, M. Qiu, Z. Ming, H. Zhao, and L. Qiu. Spoofing-Jamming Attack Strategy Using Optimal Power Distributions in Wireless Smart Grid Networks // IEEE Transactions on Smart Grid. 2017. Pp. 1–1.
12. Kolosok I., Gurina L. Cyber Security-Oriented Smart Grid State Estimation // E3S Web Conf. Vol. 69. 2018. Green Energy and Smart Grids (GESG 2018). Pp. 1–5. DOI: https://doi.org/10.1051/e3sconf/20186902004
13. Kolosok I., Gurina L. State Estimation of Electric Power System under DOS-attacks on SCADA system and WAMS // Proceedings of the Vth International workshop "Critical infrastructures: Contingency management, Intelligent, Agent-based, Cloud computing and Cyber security" (IWCI 2018). Advances in Intelligent Systems Research. vol. 158. 2018. Pp. 94–99. https://doi.org/10.2991/iwci-18.2018.17

14. Kolosok I., Korkina E., Gurina L. Vulnerability analysis of the state estimation problem under cyber attacks on WAMS // International Conference on Problems of Critical Infrastructures Joint 6th Conference of International Institute for Critical Infrastructures and 6th International Conference on Liberalization and Modernization of Power Systems. Edited by Z.A. Styczynski and N.I. Voropai. 2015. Pp. 73–84.
15. Ming-Chang Lee. Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method // International Journal of Computer Science & Information Technology (IJCSIT). 2014. Vol.6. No 1. Pp. 29–45. DOI: 10.5121/ijcsit.2014.6103
16. National Institute of Standards and Technology NIST Special Publication 800-30 rev. 1 (Sep. 2012), Guide for Conducting Risk Assessments.
17. Siddharth Sridhar, Adam Hahn, Manimaran Govindarasu. Cyber-Physical System Security for the Electric Power Grid // Proceedings of the IEEE. Vol. 100. No 1. January 2012. Pp. 210–224.
18. The Smart Grid Interoperability Panel Cyber Security Working Group, "Introduction to NISTIR7628 Guidelines for Smart Grid Cyber Security". September 2010. Available at: http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf (accessed 03.04.2019)