УДК 658 DOI: 10.36535/0869-4176-2020-01-14

УПРАВЛЯЕМАЯ КЛАСТЕРИЗАЦИЯ И САМОВОССТАНОВЛЕНИЕ РАБОТЫ ИНФОРМАЦИОННЫХ СИСТЕМ В ЭЛЕКТРО- И ТЕПЛОЭНЕРГЕТИКЕ В УСЛОВИЯХ КАСКАДНЫХ АВАРИЙНЫХ СИТУАЦИЙ[1]

Кандидат эконом. наук *Е.П. Грабчак*
Департамент оперативного контроля и управления в электроэнергетике Минэнерго России

Доктор эконом. наук *Е.Л. Логинов*
Международного научно-исследовательского института проблем управления (МНИИПУ)

В.Е. Логинова
Институт национальной энергетической безопасности

Работа посвящена обеспечению надежности и безопасности энергоснабжения в условиях компьютерных атак на информационные элементы в электро- и теплоэнергетике. Сформулирован подход к управляемой временной кластеризации (дезинтеграции) информационных подсистем объектов в электро- и теплоэнергетике в условия чрезвычайной ситуации с последующим самовосстановлением в автоматическом режиме. Предлагается рассчитать желаемые передаточные матрицы вынужденного движения выхода для всех локальных информационных подсистем для регулирования динамики работы объектов в электро- и теплоэнергетике в отношении формирования их синхронных групп для класса многосвязных объектов с запаздыванием, когда измерению доступны скалярные входные и выходные сигналы локальных подсистем.

Ключевые слова: восстанавливаемость, информационная система, мультиагентная технология, информационная атака, децентрализованная стабилизация, управление, интеллектуальные сети, электроэнергетика.

MANAGED CLUSTERING AND SELF-HEALING INFORMATION SYSTEMS IN ELECTRICITY AND HEAT IN THE CONDITIONS CASCADING EMERGENCIES

Ph.D. (Econ.) *E.P. Grabchak*
Department for Operational Control and Management in the Electric Power Industry of the Ministry of Energy of Russia

Dr. (Econ.) *E.L. Loginov*
Institute for Advanced Systems (IRIAS)

V.E. Loginova
Institute of National Energy Security

[1] Статья подготовлена при финансовой поддержке Российского фонда фундаментальных исследований (проект № 19-010-00958 А «Разработка комплекса агент-ориентированных моделей для совершенствования механизмов управления бизнес-процессами в промышленности России в условиях перехода к цифровой экономике»).

The article is devoted to ensuring the reliability and security of power supply in the conditions of computer attacks on information elements of power systems. The approach of controlled time clustering (disintegration) of information subsystems of electric power systems with the subsequent self-healing in automatic mode is formulated. It is proposed to calculate the desired transfer matrixes of the forced output motion for all local information subsystems to regulate the dynamics of the operation of electric power systems with regard to the formation of their synchronous groups for a class of multiply connected objects with delay when scalar input and output signals of local subsystems are available for measurement.

Keywords: recoverability, information system, multi-agent technology, information attack, decentralized stabilization, control, intelligent networks, electric power industry.

Введение

Развитие систем электроэнергетической инфраструктуры с большим количеством интеллектуальных регулирующих устройств с существенной компонентой собственного активного поведения поставило на повестку дня вопрос как обеспечить надежность и безопасность энергоснабжения в условиях компьютерных атак на информационные элементы энергосистем [1; 2].

Президент РФ В.В. Путин 20 июня 2019 года в ходе «Прямой линии» с гражданами России сообщил, что Россия прикладывает необходимые усилия для защиты энергетики от киберугроз. «Что касается работы нашей критически важной инфраструктуры, энергетики, в том числе и других областей, конечно, мы должны думать о том, как себя обезопасить от любых кибератак и любого негативного воздействия», – сказал В.В. Путин [3].

Нарастание угроз и рисков интеллектуальным элементам в электро- и теплоэнергетике

В 2018 году в России специальными системами (ГосСОПКА) в отношении критической информационной инфраструктуры было выявлено более 4,3 млрд. компьютерных атак или попыток внешних воздействий [4].

Особенно опасны эти процессы в электро- и теплоэнергетике. Угрозы информационной компоненте с развитием телекоммуникационных сетей общего пользования, глобальных информационных сетей (Интернет и пр.), интеграции ранее выделенных отраслевых информационных систем управления с глобальными сетями, центрами предоставления облачных услуг и т.п., актуализировали необходимость защиты информационных систем управления в электроэнергетике. Подавляющее число каскадных отключений в электроэнергетике происходит из-за отказов, сбоев или некорректной работы систем управления вследствие информационных атак, наложения инициированных (включая ошибки персонала) и естественных причин (природные явления, недостатки технических элементов и пр.).

Каскадные отключения энергосистем регулярно происходят за рубежом [5]. Выявить, что именно явилось первопричиной блэкаута, информационная атака или неблагоприятное сочетание различных естественных причин, часто затруднительно [10].

Авария 16 июня 2019 г. привела к тому, что в Аргентине, Парагвае и Уругвае 48 млн. человек остались без электроэнергии. Территория Аргентины осталась без электроснабжения практически полностью (98%), за исключением самой южной провинции [6].

Бывают аварии и в нашей стране. Например, в августе 2017 г. блэкаут произошел в МЭС Востока. В зону отключения попало более 1 млн. человек [7].

Защита информационных систем критической инфраструктуры в России

В России работает ряд госструктур ответственных за противодействие компьютерным инцидентам в системах критической инфраструктуры.

В рамках ФСБ России работает система ГосСОПКА - государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак. Помимо накопления и обработки данных об инцидентах, произошедших в компьютерных системах подключенных субъектов, ГосСОПКА позволяет контролировать уровень защищённости критически важных информационных систем, прогнозировать возможные вредоносные посягательства на информационные системы, а также обеспечивает взаимодействие между участниками [8].

Помимо центров в системе ГосСОПКА на высшем уровне работает еще одна структура – Национальный координационный центр по компьютерным инцидентам (НКЦКИ). Его задача - скоординировать действия заинтересованных структурных единиц (госведомства, предприятия и пр.) в предотвращении, обнаружении и устранении последствий кибератак. Здесь суммируется и изучается информация об инцидентах, выявляются характерные признаки, разрабатываются рекомендации по защите информации [9].

Существует также ряд других аналогичных ведомственных структур, например, Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) Банка России и др.

Новые подходы к работе информационных систем управления в электро- и теплоэнергетике в чрезвычайных условиях

С учетом значительной вероятности временного блокирования активности информационных подсистем объектов в электро- и теплоэнергетике, в условиях информационных атак и иных чрезвычайных ситуаций при развитии сбоев, приводящих к каскадным отключениям или блокированию работы, авторы - для поддержания стабильности работы в чрезвычайных ситуациях - предлагают опираться на управляемую кластеризацию информационных подсистем объектов в электро- и теплоэнергетике (временную дезинтеграцию системы на кластеры с последующим самовостановлением в автоматическом режиме).

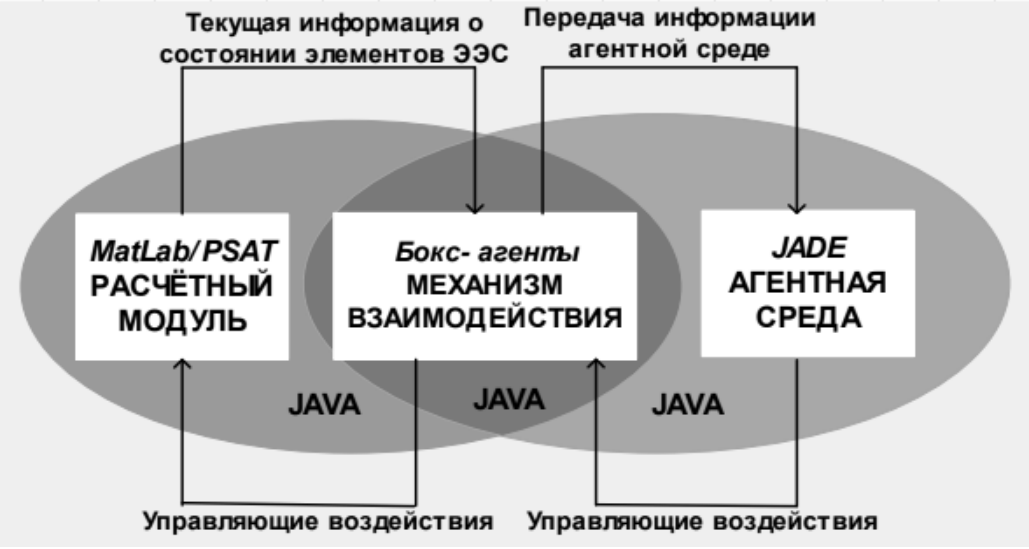

Рис. 1. Общая блок-схема программной реализации мультагентной автоматики [16]

Временная дезинтеграция системы на кластеры ставит задачу поиска новых методов управления [11, 12]. Российскими учеными (Воропай Н.И. и др.) разработан ряд эффективных подходов к повышению эффективности существующих интеллектуальных средств автоматики в объектов в электро- и теплоэнергетикеах со сложной структурой [13, 14].

Наиболее перспективным здесь является использование мультиагентных технологий: системы адаптивного управления (децентрализованной адаптивной координации) режимами объектов в электро- и теплоэнергетике [15].

На рис. 1 приведена общая блок-схема программной реализации мультагентной автоматики для адаптивного управления режимами объектов в электро- и теплоэнергетике.

Агентная интерпретация управленческих моделей самоорганизации

При этом, первоочередное внимание необходимо уделить интеллектуальным сегментам информационных подсистем (smart grid) [17; 18; 19]. Особенно это важно в отношении сложных объектов в электро- и теплоэнергетике с большим количеством автономных подсистем управления, не входящих в глобальные централизованные информационно-управляющие сети [20].

Управляемая временная дезинтеграция системы на кластеры с последующим самовосстановлением в автоматическом режиме путем децентрализованной стабилизации и управления качеством сложносоставной системы в линейной, нелинейной, оптимальной и адаптивной постановках позволяет рассчитать желаемые передаточные матрицы вынужденного движения выхода для всех локальных информационных подсистем. В результате обеспечивается выполнение поставленных целей управления для определенного перечня вариаций возмущений из прогнозируемой области группы энергетических объектов в рамках кластера.

На этой основе создается возможность определения мер по стабилизации работы информационных подсистем в условиях действия на управляемый объект динамичных во времени или величине возмущений для регулирования динамики работы объектов в электро- и теплоэнергетике в отношении формирования их синхронных групп для класса многосвязных объектов с запаздыванием, когда измерению доступны скалярные входные и выходные сигналы локальных подсистем.

Заключение

Предлагаемый подход обеспечивает упреждающую идентификацию уязвимостей к ущербу при информационных атаках и иных чрезвычайных ситуациях в отношении узлов цифровой инфраструктуры объектов в электро- и теплоэнергетике, и, как следствие, поддержание устойчивости работы энергетики нашей страны. Идентификация уязвимостей с применением новых аналитических методов позволяет осуществлять упреждающее каскадные отключения планирование мер регулирования локальных блоков управления в рамках кластеров, гарантирующих устойчивость всей связной системы в динамичных условиях и принятие соответствующих мер к восстановлению функционирования информационных подсистем объектов в электро- и теплоэнергетике. Создается возможность рассчитать желаемые передаточные матрицы вынужденного движения выхода для всех локальных информационных подсистем для регулирования динамики работы объектов в электро- и теплоэнергетике в отношении формирования их синхронных групп для класса многосвязных объектов с запаздыванием, когда измерению доступны скалярные входные и выходные сигналы локальных подсистем.

В результате обеспечивается поддержка процессов принятия решений, детерминированных функциональными задачами отдельных объектов в электро- и теплоэнергетике, обеспечение того, чтобы замкнутая децентрализованными управлениями возмущенная система осталась устойчивой для определенного перечня вариаций возмущений из прогнозируемой области.

Литература

1. Грабчак Е.П. Цифровая трансформация электроэнергетики. Основные подходы // Энергия единой сети. - 2018. № 4 (40). С. 12-26.
2. Логинов Е.Л., Борталевич С.И., Шкута А.А. Развитие интеллектуальных сервисов в автоматизированных информационных системах управления энергетической инфраструктуры. – М.: ИПР РАН. - 2017. – 95 с.
3. Прямая линия Путина. Главные заявления [Электронный ресурс] // https://www.vedomosti.ru/politics/articles/2019/06/19/804549-liniya-putina (Дата обращения 12.09.2019г.)
4. Более 4 млрд. кибератак на Россию зафиксировано в текущем году [Электронный ресурс] // http://www.interfax-russia.ru/Moscow/main.asp?id=989930 (Дата обращения 12.09.2019г.)
5. Крупнейшие аварии на энергетических системах в мире [Электронный ресурс] // https://energosmi.ru/archives/30915 (Дата обращения 12.09.2019г.)
6. Блэкаут в Южной Америке коснулся десятков миллионов человек [Электронный ресурс] // https://regnum.ru/news/polit/2648599.html (Дата обращения 12.09.2019г.)
7. Каскадный эффект: глава Ростехнадзора Алексей Алешин о причинах аварий в энергосистемах России [Электронный ресурс] // - https://iz.ru/765363/aleksei-aleshin/kaskadnyi-effekt (Дата обращения 12.09.2019г.)
8. Как работает антихакерская система ГосСОПКА [Электронный ресурс] // http://licenziya-fsb.com/kak-rabotaet-antihakerskaya-sistema-gossopka (Дата обращения 12.09.2019г.)
9. В России создан Национальный координационный центр по компьютерным инцидентам (НКЦКИ) [Электронный ресурс] // https://habr.com/ru/post/422821/ (Дата обращения 12.09.2019г.)
10. Ростехнадзор назвал единственную реальную причину дальневосточного блэкаута [Электронный ресурс] // https://eaomedia.ru/news/630520/ (Дата обращения 12.09.2019г.)
11. Логинов Е.Л., Борталевич С.И. Проблемы прогнозирования критических технических ситуаций в ЕЭС России с учетом smart grid // Проблемы безопасности и чрезвычайных ситуаций. - 2018. № 1. С. 30-37.
12. Логинов Е.Л., Борталевич С.И., Шкута А.А., Логинова В.Е. Подходы к использованию модели самоорганизации и распада нейронно-сетевых структур для повышения живучести информационных систем органов государственного управления вследствие природных, техногенных катастроф или военных атак // Вестник Московского университета МВД России. - 2017. № 4. С. 187-194.
13. Комплекс интеллектуальных средств для предотвращения крупных аварий в энергосистемах / Воропай Н.И. и др. – Новосибирск: Изд-во Наука, - 2016. – 332 с.
14. Грабчак Е.П., Медведева Е.А., Васильевна И.Г. Как сделать цифровизацию успешной // Энергетическая политика. - 2018. № 5. С. 25-29.
15. Снижение рисков каскадных аварий в объектов в электро- и теплоэнергетикеах / отв. ред. Н.И. Воропай; Рос. акад. наук, Сиб. отделение, Ин-т систем энергетики им. Л.А. Мелентьева и др. - Новосибирск: Изд-во СО РАН. - 2011. - 303 с.
16. Воропай Н.И., Томин Н.В., Курбацкий Д.А. и др. Комплекс противоаварийного управления в ЭЭС для предотвращения аварий, связанных с угрозой «лавины напряжения» [Электронный ресурс] // http://www.rza-expo.ru/doc/presentations/3.1-3.2/s_3_2_6.pdf (Дата обращения 12.09.2019г.)
17. Колосок И.Н., Гурина Л.А. Повышение кибербезопасности интеллектуальных энергетических систем методами оценивания состояния // Вопросы кибербезопасности. - 2018. № 3 (27). С. 63-69.
18. Магницкий Н.А. Обнаружение информационных атак в компьютерных сетях методом распределенных нелинейных динамических систем // Труды Института системного анализа Российской академии наук. - 2013. Т. 63. № 3. С. 60-63.

19. Колесников А.В., Листопад С.В. Функциональная структура гибридной интеллектуальной многоагентной системы гетерогенного мышления для решения проблемы восстановления распределительной электросети // Системы и средства информатики. 2019, №1. С. 41–52.

20. Дронова Ю.В. Риски внедрения интеллектуальных сетей в электроэнергетические комплексы субъектов Российской Федерации // Экономика и управление: проблемы, решения. - 2016. Т. 2. № 6. С. 77-82.

Сведения об авторах

***Грабчак Евгений Петрович*,** директор Департамента оперативного контроля и управления в электроэнергетике Минэнерго России, 107996, ГСП-6, г. Москва, ул. Щепкина, дом 42, 8(495) 631-90-43, E-mail: Grabchak.eugene@gmail.com

Логинов Евгений Леонидович, профессор РАН, дважды лауреат премии Правительства РФ в области науки и техники, начальник службы Ситуационно-аналитического центра Минэнерго России, 107996, ГСП-6, г. Москва, ул. Щепкина, дом 42, 8(903) 100-78-24, E-mail: evgenloginov@gmail.com

Логинова Валерия Евгеньевна, младший научный сотрудник Института национальной энергетической безопасности, 119021, г. Москва, ул. Л.Толстого д.5. стр.1, 8(903) 100-78-24, E-mail: urmastermind@yandex.ru