УДК 519.87:621.311

АНАЛИЗ УЯЗВИМОСТИ ЭНЕРГЕТИЧЕСКОЙ ИНФРАСТРУКТУРЫ И ЕГО РЕАЛИЗАЦИЯ

[1]Еделев А.В., [1]Береснева Н.М., [2]Горский С.А.

[1]ФГБУН «Институт систем энергетики им. Л.А. Мелентьева СО РАН», Иркутск, e-mail: flower@isem.irk.ru;

[2]ФГБУН «Институт динамики систем и теории управления им. В.М. Матросова СО РАН», Иркутск, e-mail: gorskysergey@mail.ru

Главной целью анализа уязвимости является выявление недостатков в конструкции и механизмах управления энергетической инфраструктурой, которые могут способствовать распространению крупного возмущения по ней самой и также по взаимосвязанным критическим инфраструктурам. В статье представлен разработанный подход к анализу уязвимости энергетической инфраструктуры, который строится на методической основе оценки уязвимости. Оценка уязвимости характеризует в количественной и качественной форме падение производительности энергетической инфраструктуры после воздействия крупного возмущения. Концептуальная схема анализа уязвимости рассмотрена как цепочка обработки, хранения и анализа природно-климатических данных, временных рядов значений технологических и социально-экономических параметров функционирования инфраструктурных объектов. Реализованный как распределённый пакет прикладных программ, разработанный подход к анализу уязвимости может применяться для оценки эффективности функционирования инфраструктурных объектов в особо экстремальных условиях с целью формирования рекомендаций по мониторингу объекта и окружающей среды, а также предложений по дальнейшему развитию объектов и управлению ими с точки зрения защиты от крупных возмущений, таких как стихийные бедствия, техногенные катастрофы и преднамеренные (умышленные) нарушения. Также приводятся некоторые результаты вычислительных экспериментов по изучению возможностей масштабирования вычислительной схемы, формализующей оценку уязвимости энергетической инфраструктуры в виде набора параметров и операций над ними.

Ключевые слова: энергетические системы, анализ уязвимости, живучесть, пакет прикладных программ, высокопроизводительные вычисления, критические инфраструктуры

VULNERABILITY ANALYSIS OF ENERGY INFRASTRUCTURE AND ITS IMPLEMENTATION

[1]Edelev A.V., [1]Beresneva N.M., [2]Gorskiy S.A.

[1]Melentiev Energy Systems Institute of SB RAS, Irkutsk, e-mail: flower@isem.irk.ru;

[2]Matrosov Institute for System Dynamics and Control Theory of SB RAS, Irkutsk, e-mail: gorskysergey@mail.ru

The main purpose of vulnerability analysis is to identify deficiencies in the design and management mechanisms of the energy infrastructure, which can contribute to the spread of a major disturbance on itself and, also, on interconnected critical infrastructures. The article introduces a developing approach to the analysis of the vulnerability of the energy infrastructure, which vulnerability assessment characterizes in quantitative and qualitative form a drop in the productivity of the energy infrastructure after the impact of a major disturbance. The conceptual scheme of vulnerability analysis is considered as a chain processing, storage and analysis of natural and climatic data, time series values technological and socio-economic parameters functioning infrastructure facilities. Implemented as a distributed package of application programs, the developed approach to vulnerability analysis can be used to assess the effectiveness of the functioning of infrastructure facilities in particularly extreme conditions in order to form recommendations for monitoring the facility and the environment, as well as proposals for further development of facilities and their management from the point of view of protection from cereals. Also, some results of computational experiments to study the possibilities of scaling the computational scheme are given, formalizing the vulnerability assessment of energy infrastructure in the form of a set of parameters and operations on them.

Keywords: energy systems, vulnerability analysis, resilience, application software package, high-performance computing, critical infrastructures

Энергетическая инфраструктура (ЭИ) является одной из ключевых критических инфраструктур. Ниже ЭИ может обозначать как отдельную энергетическую систему, так и метасистему, объединяющую несколько взаимодействующих систем.

Живучестью ЭИ называется способность системы прогнозировать возникновение крупных возмущений, подготавливаться и противостоять им, восстанавливаться после их воздействия [1, 2]. Эти этапы схематично отображены на рис. 1.

Функция $F(t)$ на рис. 1 отражает общую производительность ЭИ в определённый момент времени t. В исходный момент времени t_0 её значение равно F_0. В момент t_1 происходит возмущение, производительность ЭИ падает до значения $F(t_2)$, и до момента t_3 система старается приспособиться к воздействию возмущения и его последствиям.

Начиная с момента t_3, ЭИ различными способами стремится в кратчайшие сроки восстановить свою производительность до некоего приемлемого уровня $F(t_4)$. Начиная с момента t_4, ЭИ повышает свою живучесть и готовится к новым возмущениям.

Концепция уязвимости (рис. 1) имеет в научной литературе две тесно связанные интерпретации [3]. В первом случае уязвимость рассматривается как аспект живучести, который отражает «пассивную» реакцию системы на возмущения [2] в виде размера и масштаба негативных последствий для системы в результате воздействия конкретного возмущения [4]. Во втором случае уязвимость имеет локальный смысл и характеризуется элементом системы, отказ или отключение которого приводит к аварийному режиму работы системы с масштабными негативными последствиями [5].

Анализ уязвимости играет центральную роль в исследовании живучести ЭИ. Главной целью анализа уязвимости ЭИ является выявление недостатков в конструкции и механизмах управления системой, которые могут способствовать распространению крупного возмущения по ней самой и также по взаимосвязанным критическим инфраструктурам [5].

Концептуальная схема анализа уязвимости ЭИ, обобщающая в основном зарубежный опыт в этом направлении, показана на рис. 2.

Первые четыре этапа, показанные на рис. 2, соответствуют первой задаче, решаемой анализом уязвимости ЭИ, – разработке методической основы оценки уязвимости ЭИ. Если говорить более конкретно, то необходимо охарактеризовать в количественной и качественной форме падение системной производительности в промежутке времени между моментами t_1 и t_2 на рис. 1 [1], обеспечивая следующее [6]:

− изучение функционирования ЭИ в особо экстремальных условиях с нескольких перспектив (например, топологической и функциональной, статической и динамической);

− универсальность принципов моделирования функционирования ЭИ при крупных возмущениях по отношению к разным уровням территориальной и технологической иерархии энергетических систем;

− учёт взаимосвязей разных типов между ЭИ и прочими критическими инфраструктурами.

Для анализа уязвимости ЭИ не существует единственного способа его проведения. Можно лишь отметить, что в зависимости от поставленных целей он колеблется между двумя интерпретациями уязвимости, соответствующих на рис. 2 глобальному анализу уязвимости и поиску критических элементов. Поэтому вторая задача анализа уязвимости ЭИ в методическом и практическом плане заключается в поддержке формализации и реализации алгоритмов обработки и анализа результатов оценки уязвимости ЭИ. Здесь сложность заключается в выборе такого способа представления и выполнения таких алгоритмов, который был бы не привязан к конкретному языку программирования или среде выполнения.

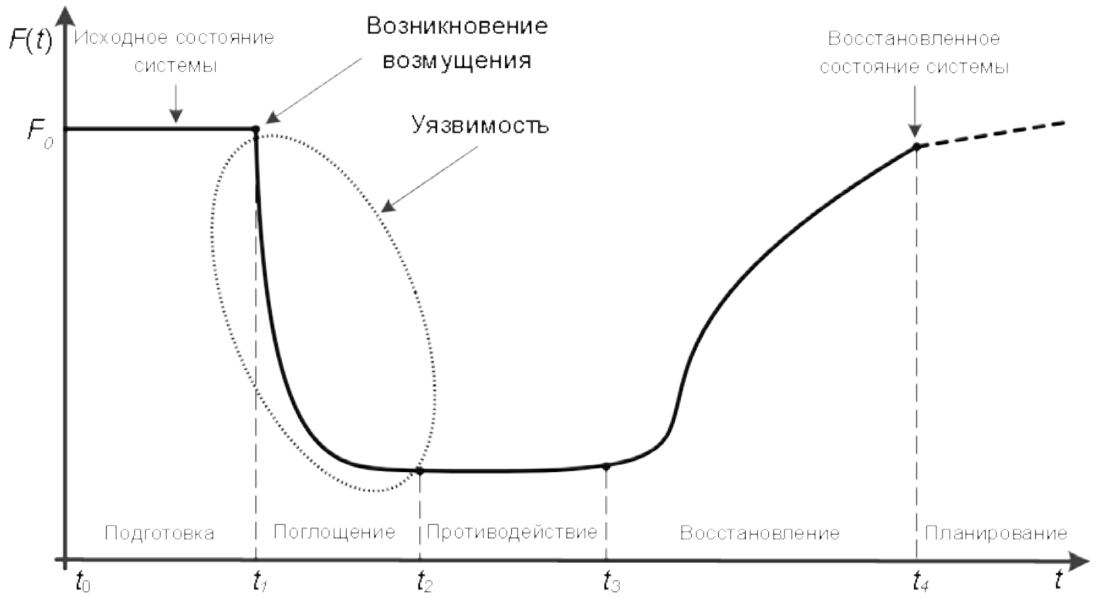

Рис. 1. Функционирование энергетической инфраструктуры в особо экстремальных условиях

Рис. 2. Концептуальная схема анализа уязвимости энергетической инфраструктуры

Первый этап схемы анализа уязвимости ЭИ на рис. 2 рассмотрен в [6], второй и третий этапы подробно описаны в [7]. Целью данной статьи является краткое представление четвёртого и пятого этапов схемы анализа уязвимости ЭИ.

Показатели и критерии уязвимости

Помимо описания объектов [8], представляющих в совокупности территориально-производственную структуру ЭИ, к конфигурации инфраструктуры (рис. 2) относятся природно-климатические факторы [9], технологические и социально-экономические параметры функционирования объектов, мониторинг которых представлен в [10]. Можно сказать, что на рис. 2 представлена цепочка обработки, хранения и анализа вышеперечисленных типов данных.

Выбор и расчёт показателей уязвимости (четвёртый этап на рис. 2) в большинстве случаев происходит следующим образом. Сначала выбирается параметр функционирования из конфигурации ЭИ, по которому можно судить о её производительности с требуемой стороны (функция F на рис. 1). Зачастую параметр функционирования отражает физические особенности определённых типов технологических процессов, протекающих на объектах, формирующих территориально-производственную структуру ЭИ (рис. 3). Параметр функционирования характеризуется максимально возможным и расчётным значением. Первое значение ($F_0=F(t_0)$ на рис. 1) извлекается из системы мониторинга [10]. Второе, равное $F(t)$, определяет интенсивность использования или уровень загрузки технологических процессов в момент $t \in [t_1, t_2]$ и определяется после моделирования возмущения по заданному сценарию [7]. Показатель уязвимости вычисляется как падение производительности в абсолютной или относительной форме: $(F_0\text{-}F(t))$ и $(F_0\text{-}F(t))/F_0$ соответственно.

Вышеописанные характеристики представляют собой последствия крупного возмущения и описываются триплетом «Расчётные данные», показанным на рис. 3.

Абсолютные или относительные значения показателей уязвимости в рамках каждого сценария возмущения могут определяться как для отдельных территорий, так и их групп. Также на основе простых показателей могут создаваться комплексные показатели уязвимости. Всё это в совокупности на рис. 3 образует триплет «Показатель уязвимости».

Главное отличие триплета «Критерий уязвимости» от триплета «Показатель уязвимости» заключается в том, что первый, в отличие от второго, не привязан к конкретному сценарию возмущения (рис. 3). Выбор критериев уязвимости зависит от вида и целей анализа уязвимости, а их значения обычно рассчитываются посредством какой-либо операции суммирования или усреднения значений показателей уязвимости по всему множеству сценариев возмущений для заданных типов объектов ЭИ или территорий, на которых они расположены.

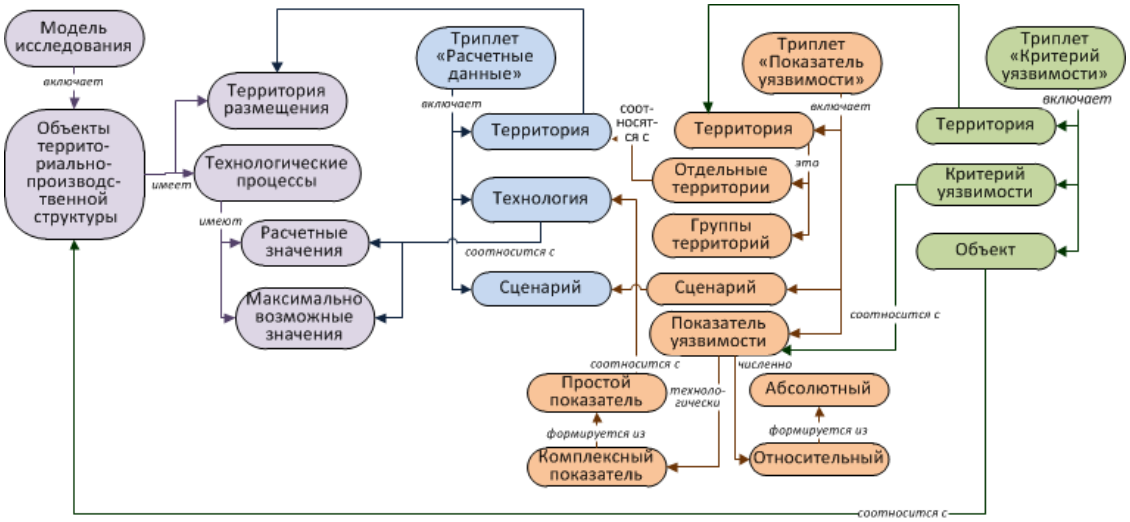

Рис. 3. Триплеты «Расчётные данные», «Показатель уязвимости» и «Критерий уязвимости»

Таким образом, онтология на рис. 3 описывает цепочку преобразования «Расчётные данные – Показатель уязвимости – Критерий уязвимости» и определяет структуры данных, требуемые для хранения информации при проведении анализа уязвимости ЭИ.

Вычислительная модель анализа уязвимости энергетической инфраструктуры

Алгоритмы расчёта критериев уязвимости ЭИ и их анализа (пятый этап на рис. 2) могут быть весьма сложными и запутанными, то есть содержать условные ветвления и циклы. Далее данные алгоритмы, в отличие от показателей уязвимости, большей частью имеющих уникальный характер, могут быть обобщены и иметь универсальный характер по отношению к различным уровням территориальной и технологической иерархии ЭИ.

Формализация и реализация алгоритмов обработки и анализа результатов оценки уязвимости ЭИ выполняется в рамках концепции распределённого пакета прикладных программ (РППП) [11].

Вычислительную модель РППП образуют три концептуально отдельных уровня знаний (вычислительный, схематический и продукционный). Параметры и операции пакета отражают схематические знания. Параметры представляют соответствующие характеристики и свойства предметной области. Операции определяют отношения вычислимости между двумя подмножествами параметров предметной области. Такое соотношение позволяет вычислить искомые значения параметров первого подмножества, когда известны значения для параметров второго подмножества. Вычислительный слой в пакете реализован модулями, являющимися программной реализацией операций. Спецификация каждого модуля включает в себя информацию об исполняемой программе (имя, версия, входные и выходные параметры, инструкции по запуску и др.). Условия выполнения операции в процессе решения вычислительной задачи в зависимости от текущего хода вычислений и состояния ресурсов определяются продукциями, формирующими продукционный слой знаний.

С точки зрения вычислительной модели РППП оценка уязвимости, расчёт критериев уязвимости и их анализ по своей сути являются вычислительными задачами и могут быть формально описаны в терминах параметров и операций. На основе формулировки постановки вычислительной задачи планируется схема её решения, которая отражает информационно-логические связи между операциями пакета. Важным преимуществом такого способа формализации алгоритмов является то, что, во-первых, схема решения задачи может быть включена в вычислительную модель любого РППП как новая операция, во-вторых, спецификация каждого модуля может легко подстраиваться под заданный уровень территориальной и технологической иерархии ЭИ без изменения самой схемы решения задачи. Это предоставляет широкие возможности в методическом и практическом плане по обобщению и универсализации алгоритмов проведения оценки уязвимости и расчёта критериев уязвимости.

Результаты исследования и их обсуждение

Авторами был реализован РППП для анализа уязвимости ЭИ, одно из практических применений которого, например, показано в [12]. Ниже приводятся результаты проверки масштабируемости расчётной схемы оценки уязвимости для примерно ста тысяч сценариев возмущений.

Расчётная схема оценки уязвимости ЭИ, представленная на рис. 4, разбита на две части. Часть s_1, включающая модули m1, m2, m3 и m4, написанные на языке программирования C++ [13], реализует второй и третий этапы концептуальной схемы анализа уязвимости ЭИ (рис. 2). Часть s_2, состоящая из модулей m5 и m6, написанных на диалекте языка запросов SQL для распределённого хранилища данных Apache Ignite [14, 15], реализует четвёртый этап (рис. 2).

На рис. 5 показана зависимость ускорения вычислений s_2 от количества узлов в кластере Apache Ignite для различных объёмов вычислительной задачи (3, 5 и 10 % от общего количества сценариев нарушений). Сверхлинейное ускорение вычислений происходит вследствие того, что с ростом числа узлов каждому из них приходится обрабатывать меньший объём данных.

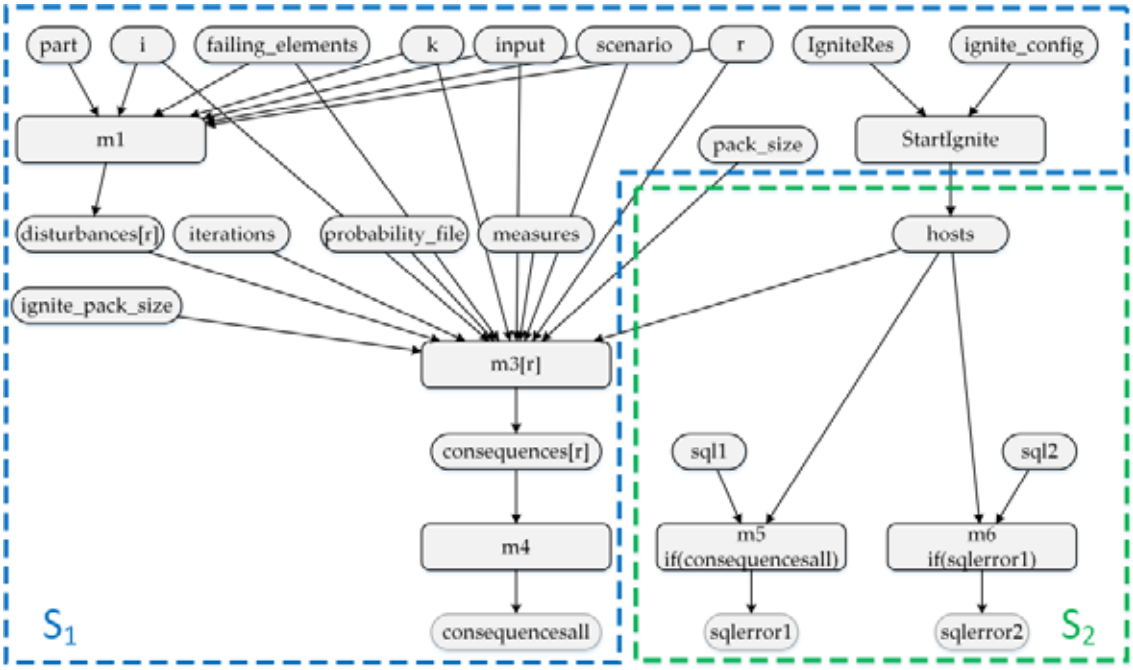

Рис. 4. Расчётная схема оценки уязвимости энергетической инфраструктуры

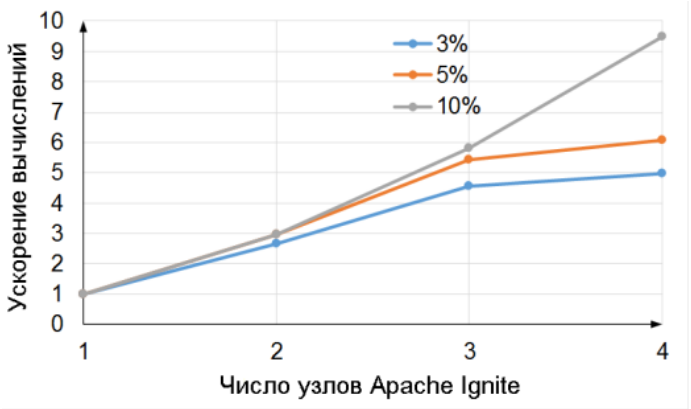

Рис. 5. Возможности масштабирования части s_2 расчётной схемы оценки уязвимости

Заключение

В статье рассмотрена поддержка анализа уязвимости энергетической инфраструктуры на глобальном и локальном уровнях. В первом случае анализируется способность системы адаптироваться к крупным возмущениям с нарастающей силой воздействия. Во втором случае производится поиск инфраструктурных объектов, отказ или отключение которых приводят к наихудшим последствиям для системы. Таким образом, анализ уязвимости может применяться для оценки эффективности функционирования инфраструктурных объектов в особо экстремальных условиях с целью формирования рекомендаций по мониторингу объекта и окружающей среды, а также предложений по дальнейшему развитию объектов и управлению ими с точки зрения защиты от крупных возмущений, таких как стихийные бедствия, техногенные катастрофы и преднамеренные (умышленные) нарушения.

На методическом уровне анализ уязвимости энергетической инфраструктуры состоит из двух частей. Первой является разносторонняя оценка последствий крупного возмущения, а вторая – вычислительная модель, в рамках которой в терминах параметров и операций описываются разнообразные алгоритмы анализа результатов оценки уязвимости.

На практическом уровне вычислительная модель анализа уязвимости энергетической инфраструктуры выступает ядром распределённого пакета прикладных программ, целью которого является обработка, хранение и анализ природно-климатических данных и параметров функционирования инфраструктурных объектов.

Работа выполнена при финансовой поддержке РФФИ и Правительства Иркутской области в рамках научного проекта № 20-47-380002-р_а.

Список литературы

1. Cheng Y., Elsayed E.A., Huang Z. Systems resilience assessments: a review, framework and metrics. International Journal of Production Research. 2021. P. 1–28.

2. Воропай Н.И. Направления и проблемы трансформации электроэнергетических систем // Электричество. 2020. № 7. С. 12–21.

3. Jonsson H., Johansson J., Johansson H. Identifying critical components in technical infrastructure networks. Proceedings of the Institution of Mechanical Engineers. Part O: Journal of Risk and Reliability. 2008. Vol. 222. No. 2. P. 235–243.

4. Svegrup L., Johansson J., Hassel H. Integration of Critical Infrastructure and Societal Consequence Models: Impact on Swedish Power System Mitigation Decisions. Risk Analysis. 2019. Vol.39. No. 9. P. 1970–1996.

5. Zio E. Challenges in the vulnerability and risk analysis of critical infrastructures. Reliability Engineering and System Safety. 2016. Vol. 152. P.137–150.

6. Еделев А.В., Феоктистов А.Г. Выбор подхода к моделированию взаимосвязанных критических инфраструктур // Современные проблемы и перспективные направления инновационного развития науки: Тр. Международной научно-практической конф. Казань: Изд-во АЭТЕРНА, 2021. С. 25–30.

7. Еделев А.В., Береснева Н.М. Подход к моделированию функционирования взаимосвязанных систем энергетики в условиях возмущений и его программная поддержка // Программные продукты и системы. 2021. № 3. С. 409–419.

8. Еделев А.В., Феоктистов А.Г. База данных для моделирования автономных энергетических комплексов // Техническая и технологическая модернизация России. Проблемы, приоритеты, перспективы: Тр. Международной научно-практической конф. Казань: Изд-во АЭТЕРНА, 2021. С. 3–9.

9. Karamov D.N. Formation of initial meteorological arrays with the use of long-term series FM 12 synop and METAR in systems energy studies. Bull Tomsk Polytech Univ Geo Assets Eng. 2018. Vol. 329. P. 69–88.

10. Sidorov I., Kostromin R., Feoktistov A. System for monitoring parameters of functioning infrastructure objects and their external environment. Proceedings of the 2nd International Workshop on Information, Computation, and Control Systems for Distributed Environments. CEUR-WS Proceedings. 2020. Vol. 2638. P. 252–264.

11. Феоктистов А.Г., Сидоров И.А., Горский С.А. Инструментальные средства разработки распределенных пакетов прикладных программ на основе модульного программирования // Марчуковские научные чтения. 2017. 2017. С. 950–956.

12. Senderov S.M., Vorobev S.V. Approaches to the Identification of Critical Facilities and Critical Combinations of Facilities in the Gas Industry in Terms of its Operability. Reliability Engineering & System Safety. 2020. Vol. 203. P. 107046.

13. Kovács P. Minimum-cost flow algorithms: an experimental evaluation. Optimization Methods and Software. 2015. Vol. 30. No. 1. P. 94–127.

14. Bhuiyan S., Zheludkov M., Isachenko T. High Performance in-memory computing with Apache Ignite. Morrisville: Lulu.com. 2017. P. 352.

15. Zhang H., Chen G., Ooi B.C., Tan K.L., Zhang M. In-memory big data management and processing: A survey. IEEE Transactions on Knowledge and Data Engineering. 2015. Vol. 27. No. 7. P. 1920–1948.