ISSN 2686-679X

# ВЕСТНИК РГГУ

*Серия*
«Информатика.
Информационная безопасность.
Математика»

Научный журнал

# RSUH/RGGU BULLETIN

"Information Science.
Information Security. Mathematics"
*Series*

Academic Journal

Основан в 2018 г.
Founded in 2018

3
2023

VESTNIK RGGU. Seriya “Informatica. Informacionnaya bezopasnost. Matematica”

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” Series
Academic Journal

There are 4 issues of the printed version of the journal a year.

Founder and Publisher
Russian State University for the Humanities (RSUH)

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” series is included: in the Russian Science Citation Index; in the List of leading scientific magazines journals and other editions for publishing PhD research findings peer-reviewed publications fall within the following research area:

**1.1.6.** Computational Mathematics

**2.3.6.** Information security methods and systems, information security

**2.3.8.** Informatics and information processes

*Objectives and areas of research*

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” series publishes the results of research by scientists from RSUH and other universities and other Russian and foreign academic institutions. The areas covered by contributions include theoretical and applied computer science, up-to-date IT, means and technologies of information protection and information security as well as the issues of theoretical and applied mathematics including analytical and imitation models of different processes and objects. Special emphasis is put on articles and reviews covering research in indicated directions in the areas of social and humanitarian problems and also issues of personnel training for these directions.

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” series is registered by Federal Service for Supervision of Communications Information Technology and Mass Media. 25.05.2018, reg. No. FS77-72977

Editorial staff office: 6, Miusskaya sq., Moscow, Russia, 125047

e-mail: grnat@rambler.ru

ВЕСТНИК РГГУ. Серия «Информатика. Информационная безопасность. Математика»
Научный журнал

Выходит 4 номера печатной версии журнала в год.

Учредитель и издатель – Российский государственный гуманитарный университет (РГГУ)

ВЕСТНИК РГГУ, серия «Информатика. Информационная безопасность. Математика», включен: в систему Российского индекса научного цитирования (РИНЦ); в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук по следующим научным специальностям и соответствующим им отраслям науки:

**1.1.6.** Вычислительная математика

**2.3.6.** Методы и системы защиты информации, информационная безопасность

**2.3.8.** Информатика и информационные процессы

*Цели и область*

В журнале «Вестник РГГУ», серия «Информатика. Информационная безопасность. Математика» публикуются результаты научных исследований ученых и специалистов РГГУ, а также других университетов и научных учреждений России и зарубежных стран. Направления публикаций включают теоретическую и прикладную информатику, современные информационные технологии, методы, средства и технологии защиты информации и обеспечения информационной безопасности, а также проблемы теоретической и прикладной математики, включая разработку аналитических и имитационных моделей процессов и объектов различной природы. Особое внимание уделяется статьям и обзорам, посвященным исследованиям по указанным направлениям в области социальных и гуманитарных проблем, а также вопросам подготовки кадров по соответствующим специальностям для данных направлений.

ВЕСТНИК РГГУ. Серия «Информатика. Информационная безопасность. Математика», зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций 25.05.2018 г., регистрационный номер ПИ № ФС77-72977.

Адрес редакции: 125047, Россия, Москва, Миусская пл., 6

электронный адрес: grnat@rambler.ru

CONTENTS

СОДЕРЖАНИЕ

УДК 004.9
DOI: 10.28995/2686-679X-2023-3-8-19

# Об использовании предметно-ориентированных онтологий для поддержки принятия решения в профессиональной деятельности преподавателя

Алексей П. Сафроненков
*Российский государственный гуманитарный университет, Москва, Россия, safronenkov-alekseij@rambler.ru*

Ирина Б. Сафроненкова
*Федеральный исследовательский центр, Южный научный центр Российской академии наук, Ростов-на-Дону, Россия, safronenkova050788@yandex.ru*

Александр Е. Павленко
*Таганрогский институт имени А.П. Чехова (филиал) ФГБОУ ВО «Ростовский государственный экономический университет (РИНХ)», Ростов-на-Дону, Россия, alex_pavlenko@inbox.ru*

*Аннотация*. Данная работа рассматривает проблемы, связанные с организацией профессиональной деятельности педагога в части автоматизации поддержки принятия решений. Проведен анализ использования СППР (системы поддержки принятия решения) в различных областях человеческой деятельности. Результаты проведенного анализа показали, что ИСППР (интеллектуальные системы поддержки принятия решения) широко и эффективно применяются в сфере образования, однако, в силу разнообразия направлений педагогической деятельности, многие вопросы остаются нерешенными на настоящий момент. В данной работе предложено использовать такой класс систем для поддержки ЛПР (лица, принимающего решение), т. е. педагога, при выборе оптимальной стратегии или набора стратегий, направленных на повышение эффективности подготовки обучающегося к выполнению заданий «Письменная часть» единого государственного экзамена (ЕГЭ) по английскому языку. Авторами предложено в качестве каркаса Базы Знаний (БЗ) такой системы использовать предметно-ориентированные онтологические модели. Ввиду того что разработка

ИСППР – задача комплексная и сложная, целью данной работы является разработка предметно-ориентированной онтологической модели критериев оценивания задания с развернутым ответом «Электронное письмо личного характера» ЕГЭ в открытом редакторе онтологий Protégé 5.6.1.

*Ключевые слова:* предметно-ориентированная онтологическая модель, СППР, ИСППР, критерии оценивания, письмо

*Для цитирования: Сафроненков А.П., Сафроненкова И.Б., Павленко А.Е.* Об использовании предметно-ориентированных онтологий для поддержки принятия решения в профессиональной деятельности преподавателя // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2023. № 3. С. 8–19. DOI: 10.28995/2686-679X-2023-3-8-19

# On the use of subject-oriented ontologies to support decision-making in the professional activity of a teacher

Aleksei P. Safronenkov
*Russian State University for the Humanities, Moscow, Russia, safronenkov-aleksejj@rambler.ru*

Irina B. Safronenkova
*Federal Research Centre the Southern Scientific Center of the Russian Academy of Sciences, Rostov-on-Don, Russia, safronenkova050788@yandex.ru*

Aleksandr E. Pavlenko
*A.P. Chekhov Institute of Taganrog (branch of) Rostov State University of Economics, Rostov-on-Don, Russia, alex_pavlenko@inbox.ru*

*Abstract*. The work considers the issues associated with the organization of professional activity of a teacher in terms of automation of decision support. It carries out the analysis of the use of DSS (decision support system) in various fields of human activity. Results of the analysis showed that IDSS (intelligent decision support systems) are widely and effectively used in the field of Education, however, due to the diversity of areas of pedagogical activity, many issues remain unresolved at the moment. The work proposes to use such a class of systems to support the DM (decision-maker), i.e. the teacher, when choosing the optimal strategy or set of strategies aimed at improving the effectiveness of preparing the student to perform the tasks of the "Written part" of the Unified State Exam in English. The authors proposed using domain-oriented ontologi-

cal models as the framework for the Knowledge Base (KB) of such a system. Due to the fact that the development of IDSS is a complex task, the purpose of the present work is to develop a subject–oriented ontological model of task evaluation criteria with a detailed answer "Personal email" of the Unified State Exam in the open ontology editor Protégé 5.6.1.

*Keywords*: subject–oriented ontological model, DSS, IDSS, evaluation criteria, writing

*For citation:* Safronenkov, A.P., Safronenkova, I.B. and Pavlenko, A.E. (2023), "On the use of subject-oriented ontologies to support decision-making in the professional activity of a teacher", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 3, pp. 8–19, DOI: 10.28995/2686-679X-2023-3-8-19

## *Введение*

Система поддержки принятия решений широко используется для принятия многокритериальных решений в сложной информационной среде в самых разнообразных сферах человеческой деятельности. Согласно определению, СППР – компьютерная автоматизированная система, целью которой является помощь людям, принимающим решение в сложных условиях для полного и объективного анализа предметной деятельности [Попов 2008].

Например, такие СППР применяют в области бизнеса и менеджмента для определения стратегии развития [Гергулева 2010], в области медицины для диагностики и выбора лекарственных средств, а также методов лечения [Малых 2019], в финансовой сфере для мониторинга рыночной конъюнктуры и формирования оптимальных стратегий управления бюджетными ресурсами [Синицын, Толмачев 2019].

Если в СППР для принятия решения используют методы искусственного интеллекта, то такая система называется интеллектуальной системой поддержки принятия решений (ИСППР).

За последнее десятилетие такой класс систем плотно закрепился в области педагогических наук и оказывает поддержку лицу, принимающему решение (ЛПР), в данном случае педагогу, по следующим аспектам:

– выработка стратегии преподавания дисциплины [Ахмедьянова, Пищухин 2008; Жаров, Марданов, Окбаева 2022];
– принятие педагогом управленческих решений в образовательной деятельности [Медведева, Петрунина 2019];
– оценивание знаний студента [Анохина-Наумец 2011];

– прогнозирование характеристик и успеваемости обучающихся [Булдаев, Найханова, Евдокимова 2020];
– формирование рекомендаций обучающимся по выбору направления обучения в магистратуре в соответствии с их личными предпочтениями [Козловский, Мельник, Волощук, Хлусова 2021].

Обзор литературы показал, что использование СППР, в том числе ИСППР, с целью поддержки педагога при осуществлении его профессиональной деятельности является перспективной темой исследования. Это обусловлено тем, что деятельность педагога весьма разнообразна и сопряжена с решением широкого круга задач, начиная от проблем дисциплинарного характера, заканчивая вопросами, связанными с дидактикой.

Авторы данной работы предлагают использовать ИСППР для оказания автоматизированной поддержки педагогу в части выбора оптимальной стратегии/набора стратегий для подготовки обучающегося к выполнению заданий раздела «Письменная часть» ЕГЭ по английскому языку.

## *Неформальная постановка проблемы*

В настоящее время важным и актуальным вопросом в сфере образовательной деятельности является эффективная подготовка обучающегося к сдаче ЕГЭ, поскольку за последние несколько лет произошли существенные изменения как в формате заданий, так и в системе критериев оценивания. Специалисты в области подготовки к ЕГЭ по английскому языку отмечают, что произошло смещение акцентов в сторону оценивания уровня коммуникативной компетенции экзаменуемого, т. е. умения продуцировать речь в различных ситуациях, которое проверяется в заданиях со свободно конструируемым ответом [Колыхалова, Михайлова 2022]. Это, в свою очередь, приводит к необходимости корректировки применяемых в образовательной деятельности стратегий и методик.

Для решения описанной выше проблемы могут быть использованы ИСППР. Предполагается, что такие системы позволят автоматизировать процесс принятия решения при выборе оптимальной стратегии/набора стратегий для подготовки обучающегося к выполнению заданий раздела «Письменная часть» ЕГЭ по английскому языку, тем самым оказав поддержку ЛПР.

Предложенный класс систем характеризуется схожей архитектурой, включающей представление знаний и алгоритмов их обработки. В ИССПР используют различные стратегии поиска

в пространстве состояний, так же как и различные формы представления знаний [Пенькова, Вайнштейн 2019], выбор которых и их последующая интеграция обусловливают сложность и нетривиальность задачи, заключающейся в разработке архитектуры ИСППР. В связи с этим в рамках данной работы рассматривается проблема организации БЗ в таком классе систем, а именно предложено использовать предметно-ориентированные онтологические модели для систематизации информации о предметной области знания.

Онтологическая модель рассматриваемой предметной области должна описывать основные концепты, связанные с подготовкой обучающегося к выполнению заданий раздела «Письменная часть» ЕГЭ по английскому языку, свойства данных концептов и связи между ними. Анализ данной предметной области позволил выделить две группы концептов, оказывающих влияние на эффективность подготовки обучающегося: критерии оценивания и обучающие стратегии и методики, направленные на улучшение значений данных критериев.

В рамках настоящей работы будет рассмотрена первая группа – критерии оценивания, а именно аспекты, подлежащие оцениванию при выполнении заданий из раздела «Письменная речь» ЕГЭ по английскому языку, и предложена предметно-онтологическая модель, отражающая данные аспекты.

## *Разработка предметно-ориентированной онтологической модели критериев оценивания задания «Электронное письмо личного характера»*

Онтология – учение о бытии, также понимается, как раздел философии, изучающий фундаментальные принципы бытия, его наиболее общие сущности и категории. Термин «онтология» впервые был предложен в 1613 г. Р. Гоклениусом и позже закреплен в науке немецким философом Х. Вольфом [Гаврилова, Кудрявцев, Муромцев 2016]. В настоящее время использование данного термина вышло далеко за границы области философских наук и широко применяется в информационной сфере, где онтология рассматривается как форма репрезентации знаний о какой-либо предметной области с целью решения конкретных задач [Губанов 2018, с. 347].

Формально онтологическую модель рассматривают как систему, состоящую из набора понятий и набора утверждений об этих понятиях, на основе которых можно строить классы, объекты, отношения, функции и теории.

Формальная онтологическая модель имеет вид:

$$O = < C, P, R, A >,$$

где C – конечное множество понятий (классов сущностей) предметной области;
P – конечное множество свойств этих понятий (классов);
R – конечное множество связей между понятиями (классами);
A – множество аксиом, утверждений, построенных из этих понятий, их свойств и связей между ними

В зависимости от цели создания различают предметно-ориентированные (Domain-oriented), ориентированные на прикладную задачу (Task-oriented), общие онтологии (Top-level ontologies). Предметно-ориентированная онтология – это концептуализация мира в понятиях словаря для объектов, их качественных характеристик, отличительных особенностей и т. п. для данной предметной области [Лапшин 2010].

Анализ методических материалов, содержащих рекомендации по проверке заданий с развернутым ответом ЕГЭ по английскому языку, позволил выделить следующие критерии оценивания для задания «Электронное письмо личного характера»: критерий 1 – решение коммуникативной задачи (РКЗ), который включает в себя 6 аспектов; критерий 2 – организация текста, который включает в себя также 6 аспектов; критерий 3 – языковое оформление текста.

На языке предметно-ориентированных онтологий критерии и включенные в них аспекты выражаются в виде иерархии классов онтологии и имеют следующий вид, изображенный на рис. 1.

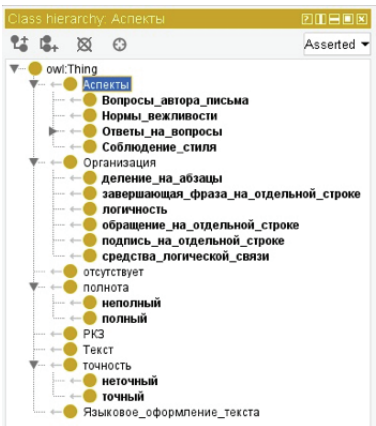


*Рис. 1.* Иерархия классов предметно-ориентированной онтологической модели, описывающей критерии оценивания при выполнении задания «Электронное письмо личного характера»

Теперь необходимо связать класс «РКЗ» и класс «Аспекты» через свойство «аспекты». Для этого зададим область определения (Domains) и области значения (Ranges) через вкладку “Object Properties”, как показано на рис. 2.

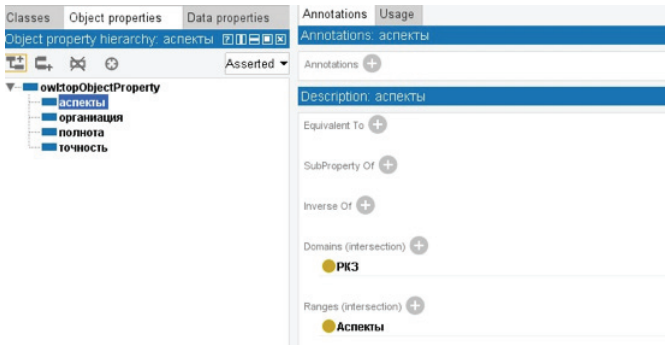


*Рис. 2.* Описание свойства через “Object Properties” в системе Protégé

Фрагмент графа, отражающий свойство «аспекты», представлен на рис. 3.

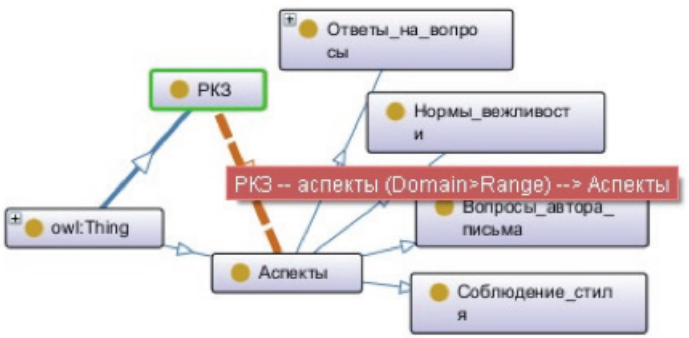


*Рис. 3.* Связь классов «РКЗ» и «Аспекты» через свойство «аспекты»

Аналогично связываются классы «Текст» и «Организация» через свойство «организация».

Предметно-ориентированная онтологическая модель критериев оценивания задания «Электронное письмо личного характера» представлена на рис. 4.

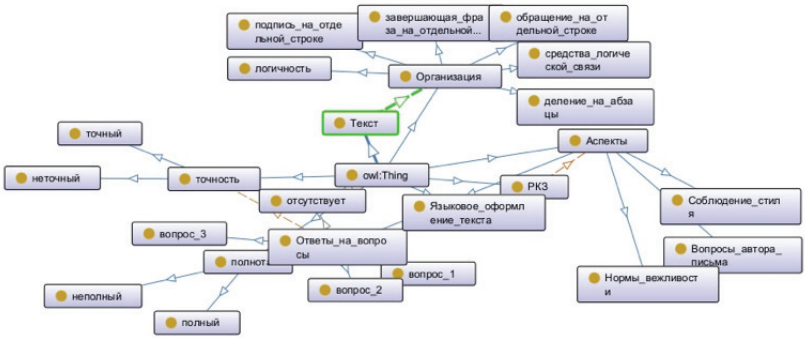


*Рис. 4.* Предметно-ориентированная онтологическая модель критериев оценивания задания «Электронное письмо личного характера»

Разработанная предметно-ориентированная онтологическая модель позволяет систематизировать знания о предметной области – системе критериев оценивания и формализовать эти знания для последующей их автоматизированной обработки в ИСППР.

## *Заключение*

В данной работе рассмотрена возможность использования ИСППР в профессиональной деятельности педагога с целью подбора наиболее эффективных стратегий или набора стратегий подготовки к выполнению заданий «Письменная речь» ЕГЭ по английскому языку, базу знаний которых составляют предметно-ориентированные онтологические модели. Проведен анализ методической литературы по подготовке к выполнению заданий «Письменная речь» ЕГЭ по английскому языку и на его основе разработана предметно-ориентированная онтологическая модель критериев оценивания задания с развернутым ответом «Электронное письмо личного характера» в среде Protégé 5.6.1.

*Литература*

Анохина-Наумец 2011 – *Анохина-Наумец А.В.* Интеллектуальная система оценивания знаний: модель студента и методика экспериментальной проверки алгоритма адаптации // Образовательные технологии и общество. 2011. № 2 (14). С. 346–362.

Ахмедьянова, Пищухин 2008 – *Ахмедьянова Г.Ф., Пищухин А.М.* Интеллектуальная система поддержки принятия педагогических решений // Научный журнал «Фундаментальные исследования». 2008. № 5. С. 48–51.

Булдаев, Найханова, Евдокимова 2020 – *Булдаев А.А., Найханова Л.В., Евдокимова И.С.* Модель системы поддержки принятия решений в учебном процессе университета, основанной на аналитике обучения // Программные системы и вычислительные методы. 2020. № 4. С. 42– 52.

Гаврилова, Кудрявцев, Муромцев 2016 – *Гаврилова Т.А., Кудрявцев Д.В., Муромцев Д.И.* Инженерия знаний. Модели и методы: Учебник. СПб.: Лань, 2016. 324 с.

Гергулева 2010 – *Гергулева П.В.* Системы поддержки принятия решений как составляющая эффективного управления предприятием // Современные тенденции в экономике и управлении: новый взгляд. 2010. № 5-2. С. 253–257.

Губанов 2018 – *Губанов Д.А.* Методы извлечения и анализа терминологических структур смежных предметных областей (на примере методологии) // Онтология проектирования. 2018. Т. 8. № 3 (29). С. 347–365.

Жаров, Марданов, Окбаева 2022 – *Жаров В.К., Марданов А.П., Окбаева Н.У.* К вопросу о моделировании методики преподавания дисциплин в педагогике // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2022. № 1. С. 120–136. DOI: 10.28995/2686-679X-2022-1-120-136.

Козловский, Мельник, Волощук, Хлусова 2021 – *Козловский А.В., Мельник Я.Э., Волощук В.И., Хлусова А.С.* Разработка экспертной системы подбора направления для поступающих в магистратуру // Известия ТулГУ. Технические науки. 2021. Вып. 12. С. 480–486.

Колыхалова, Михайлова 2022 – *Колыхалова О.А., Михайлова И.И.* Методические материалы для председателей и членов предметных комиссий субъектов Российской Федерации по проверке выполнения заданий с развернутым ответом экзаменационных работ ЕГЭ 2022 г. по английскому языку (письменная часть). М., 2022. 121 с.

Лапшин 2010 – *Лапшин В.А.* Онтологии в компьютерных системах. М.: Научный мир, 2010. 224 с.

Малых 2019 – *Малых В.Л.* Системы поддержки принятия решений в медицине // Программные системы: теория и приложения. 2019. № 2 (41). С. 155–184.

Медведева, Петрунина 2019 – *Медведева Н.В., Петрунина А.Д.* Роль педагогов в реализации управленческих решений // Образование в современном мире: Сб. научных статей. Саратов: Саратовский нац. исслед. гос. ун-т имени Н.Г. Чернышевского, 2019. С. 364–371.

Пенькова, Вайнштейн 2019 – *Пенькова Т.Г., Вайнштейн Ю.В.* Модели и методы искусственного интеллекта: Учеб. пособие. Красноярск: Сиб. федер. ун-т, 2019. 116 с.

Попов 2008 – *Попов А.Л.* Системы поддержки принятия решений: Учеб.-метод. пособие. Екатеринбург: Урал. гос. ун-т, 2008. 80 с.

Синицын, Толмачев 2019 – *Синицын Е.В., Толмачев А.В.* Модель системы поддержки принятия решений на финансовых рынках для предприятий на основе вероятностного анализа и машинного обучения // Вестник УрФУ. Серия: Экономика и управление. 2019. Т. 18. № 3. С. 378–393.

## *References*

Anohina-Naumets, A.V. (2011), "Intelligent knowledge assessment system. Model student and method of experimental verification adaptation algorithm", *Educational technologies and society*, vol. 2 (14), pp. 346–362.

Ahme'yanova, G.F. and Pishchukhin, A.M. (2008), "Intelligent pedagogical decision support system", *Basic Research*, no. 5, pp. 48–51.

Buldaev, A.A., Naikhanova, L.V. and Evdokimova, I.S. (2020), "Model of decision support system in educational process of a university on the basis of learning analytics", *Software systems and computational methods,* no. 4, pp. 42–52.

Gavrilova, T.A., Kudryavtsev, D.V. and Muromtsev, D.I. (2016), *Inzheneriya znanii. Modeli i metody: uchebnik* [Knowledge engineering. Models and methods. Textbook], Lan', Saint Petersburg, Russia.

Gerguleva, P.V. (2010), "Decision support systems as a component of effective enterprise management", *Modern trends in economics and management. A new look,* vol. 5-2, pp. 253–257.

Gubanov, D.A. (2018), "Methods for extracting and analyzing terminological structures of related subject areas (on the example of methodology)", *Design ontology*, vol. 8, no. 3 (29), pp. 347–365.

Kozlovskii, A.V., Mel'nik, Ya.E., Voloshchuk, V.I. and Khlusova, A.S. (2021), "Development of an expert system for selecting a direction for applicants to master's degree programs", *Proceedings of the TSU. Technical science*, vol. 12, pp. 480–486.

Kolykhalova, O.A. and Mihailova, I.I. (2022), Methodological materials for chairmen and members of the subject commissions of the constituent entities of the Russian Federation for checking the completion of assignments with a detailed answer to the exam papers of the USE 2022 in English (written part), Moscow, Russia.

Lapshin, V.A. (2010), *Ontologii v komp'yuternykh sistemakh* [Ontologies in computer systems], Nauchnyi mir, Moscow, Russia.

Malykh, V.L. (2019), "Decision support systems in medicine", *Program Systems: Theory and Applications*, vol. 10, pp. 155–184.

Medvedeva, N.V. and Petrunina, A.D. (2019), "The role of teachers in the implementation of management decisions", *Education in the modern world. Coll. of scientific articles, N.G. Chernyshevsky Saratov National Research State University, Saratov,* pp. 364–371.

Pen'kova, T.G., and Vainshtein, Yu.V. (2019), *Modeli i metody iskusstvennogo intellekta: Ucheb. posob.* [Models and methods of artificial intelligence. Teaching Manual], Sibirskii federal'nyi universitet, Krasnoyarsk, Russia.

Popov, A.L. (2008), *Sistemy podderzhki prinyatiya reshenii* [Decision support systems. Educational-methodical manual], Ural'skii gosudarstvennyi universitet, Ekaterinburg, Russia.

Sinitsyn, E.V. and Tolmachev, A.V. (2019), "Model of the decision support system in the financial markets for enterprises based on probability analysis and machine learning", *Bulletin of Ural Federal University. Series Economics and Management*, vol. 18, no. 3, pp. 378–393.

Zharov, V.K., Mardanov, A.P. and Okbaeva, N.U. (2022), "On the issue of modeling the methodology of teaching disciplines in pedagogy", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 1, pp. 120–136, DOI: 10.28995/2686-679X-2022-1-120-136.

## *Информация об авторах*

*Алексей П. Сафроненков,* магистрант, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; safronenkov-aleksejj@rambler.ru

*Ирина Б. Сафроненкова,* кандидат технических наук, младший научный сотрудник, Федеральный исследовательский центр Южный научный центр Российской академии наук, Ростов-на-Дону, Россия; 344006, Россия, Ростов-на-Дону, проспект Чехова, д. 41; safronenkova050788@yandex.ru

*Александр Е. Павленко*, доктор филологических наук, профессор, Таганрогский институт имени А.П. Чехова (филиал) ФГБОУ ВО «Ростовский государственный экономический университет (РИНХ)», Таганрог, Россия; 347900, Россия, Таганрог, ул. Петровская, д. 68; alex_pavlenko@inbox.ru

## *Information about the authors*

*Aleksei P. Safronenkov,* master student, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, Russia, 125047; safronenkov-aleksejj@rambler.ru

*Irina B. Safronenkova,* Cand. of Sci. (Mechanical Engineering), junior researcher, Federal Research Center The Southern Scientific Center of the Russian Academy of Sciences, Rostov-on-Don, Russia; bld. 41, Chekhov Str., Rostov-on-Don, Russia, 344006; safronenkova050788@yandex.ru

*Aleksandr E. Pavlenko,* Dr. of Sci. (Philology), professor, A.P. Chekhov Institute of Taganrog (Rostov State University of Economics branch), Rostov-on-Don, Russia; bld. 68, Petrovskaya Str., Taganrog, Russia, 347900; alex_pavlenko@inbox.ru

УДК 004.9
DOI: 10.28995/2686-679X-2023-3-20-37

# Особенности разработки информационной системы для сети автомобильных электрозаправочных станций

Марина С. Шаповалова
*Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия, mshapovalova84@gmail.com*

Александр А. Андреев
*Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия, andreev@indry.tech*

Валерия В. Чувашова
*Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия, chuvashova@indry.tech*

*Аннотация.* В статье анализируются технические требования, предъявляемые к электрозаправочным станциям с точки зрения определения возможности и особенностей проектирования информационной системы по их обслуживанию. Показаны основные особенности работы электрозаправочных станций, согласно стандартам, принятым в Европе, США и Китае. Рассмотрены их функциональные характеристики и специфика работы для удаленного управления с помощью информационной системы.

Сформулированы требования к информационной системе, которая может быть создана на основе микросервисной архитектуры. Показано, что для обеспечения взаимодействия между отдельными частями информационной системы должна быть обеспечена стабильность ее работы в режиме 24/7.

В ходе исследования определено, что:

– взаимодействие клиента с сервером может быть реализовано посредством некоторого приложения или web-интерфейса и должно быть стабильным и устойчивым;
– эта система будет включать в себя платежный модуль, электрическую балансировку, а обработка поступающих данных на сервер будет представлять собой распределенную систему обработки информации, имеющей в своей основе очередь с приоритетами;
– сама информационная система должна быть спроектирована на основе архитектуры, реализующей клиент-серверный принцип работы;
– специальная система мониторинга должна быть распределенной, что позволит своевременно обрабатывать поступающие запросы, видеть проблемы и своевременно решать их.

*Ключевые слова*: клиент, сервер, архитектура, электрозаправочные станции, микросервисы

*Для цитирования*: *Шаповалова М.С., Андреев А.А., Чувашова В.В.* Особенности разработки информационной системы для сети автомобильных электрозаправочных станций // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2023. № 3. С. 20–37. DOI: 10.28995/2686-679X-2023-3-20-37

# Features of development of an information system for a network of electric vehicle charging stations

Marina S. Shapovalova
*Bauman Moscow State Technical University, Moscow, Russia, mshapovalova84@gmail.com*

Aleksandr A. Andreev
*Bauman Moscow State Technical University, Moscow, Russia,andreev@indry.tech*

Valeriya V. Chuvashova
*Bauman Moscow State Technical University, Moscow, Russia, chuvashova@indry.tech*

*Abstract*. The article analyzes the technical requirements for electric vehicle charging stations from the perspective of determining the feasibility and features of designing an information system for their maintenance. The main features of the operation of electric vehicle charging stations are shown according to the standards adopted in Europe, the USA, and China. Their functional characteristics and specifics of remote control using an information system are considered. The article formulates requirements for an information system that can be created based on microservice architecture. It is shown that to ensure interaction between individual parts of the information system, its stable operation in 24/7 mode must be ensured. During the study, it was determined that:

- customer-server interaction can be implemented through some application or web interface and should be stable and resilient;
- this system will include a payment module, electric balancing while processing of incoming data on the server will represent a distributed information processing system based on a priority queue;
- the information system itself should be designed based on an architecture implementing the client-server operating principle;
- a special monitoring system should be distributed, allowing timely processing of incoming requests, identifying upsets and resolving them promptly.

*Keywords*: Electric Charging Station, client, server, architecture, charging stations, microservices

*For citation*: Shapovalova, M.S., Andreev, A.A. and Chuvashova, V.V. (2023), “Features of development of an information system for a network of electric vehicle charging stations”, *RSUH/RGGU Bulletin. “Computer Sience. Informaton security. Mathematics” Series*, no. 3, pp. 20–37, DOI: 10.28995/2686-679X-2023-3-20-37

За последние 15 лет количество электромобилей в мире выросло в 7 тыс. раз и, по прогнозам, еще через 10 лет составит 30% от всего автотранспорта. Растет и смежный, обслуживающий бизнес, в том числе станции по заправке таких автомобилей.

Десятки компаний, работающих с электрозаправочными станциями (ЭЗС – зарядная станция или электрозаправочная станция – элемент городской инфраструктуры, предоставляющий электроэнергию для зарядки аккумуляторного электротранспорта, такого как электромобили, электробусы, электроскутеры, электросамокаты, гироскутеры, сигвеи, электровелосипеды и т. п.), уже нашли своих клиентов, а в большинстве регионов они также являются объектами критической инфраструктуры и монополистами.

Поскольку заправка на ЭЗС, как правило, осуществляется в автономном режиме, очень важно определить принципы работы информационной системы, обслуживающей зарядные станции, управляющей проверкой и заправкой электромобилей. В этих условиях важно обеспечить требования информационной безопасности [Казарин, Шаряпов, Ященко 2018].

Данная статья направлена на описание технических требований с целью проектирования информационной системы, которая бы позволяла пользователям ЭЗС проводить заправку, а также особенностей ее будущей реализации.

Необходимо отметить, что такая система является объектом критически важной инфраструктуры, она является высоконагруженной системой повышенной опасности и должна автономно работать 24/7.

На международном рынке представлены три основных стандарта ЭЗС[1], каждый из которых отличается особой геометрией зарядного штекера электромобиля и зарядной розетки. Представленные стандарты используются в Северной Америке, Европе и Китае. Кроме того, конструкция штекера для зарядки перемен-

[1] Electrek. URL: https://electrek.co/2021/10/22/electric-vehicle-ev-charging-standards-and-how-they-differ (дата обращения 20 мая 2023).

ным током принципиально отличается от штекера для зарядки постоянным током.

Большой ассортимент оборудования для заправки автомобиля позволяет охватить все варианты применения (рис. 1). Стандарт по типу 1 для Северной Америки не предусматривает наличие инфраструктурного зарядного штекера.

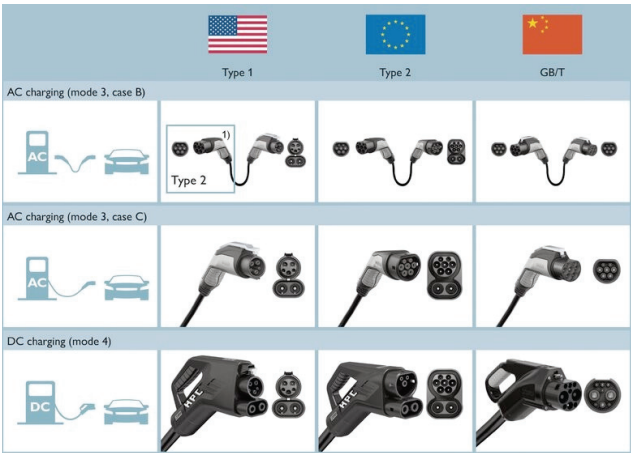


*Рис. 1.* Стандарты зарядки и типы штекеров по выбранным регионам

В Европе в этом случае используется переходной кабель, который состоит из зарядного штекера электромобиля по типу 1 и инфраструктурного зарядного штекера по типу 2[2].

В России распространены автомобили с зарядками всех трех типов. Поэтому необходимо, с одной стороны, унифицировать работу ЭЗС на аппаратном уровне, а с другой – обеспечить поддержку заряда для разного типа автомобилей. Однако полностью унифицировать виды зарядных устройств невозможно. Но при участии ведущих производителей автомобилей была разработана комбинированная система зарядки (CCS). Особенностью является зарядная розетка[3] (рис. 2) в электромобиле, которая подходит

[2] Dazetech. URL: https://www.dazetech.ology.com/charging-modes-for-ev/.Electric Vehicle Mode (дата обращения 20 мая 2023).

[3] Dalroad. URL: https://www.dalroad.com/resources/an-introduction-to-electric-vehicle-rapid-charging-standards (дата обращения 20 мая 2023).

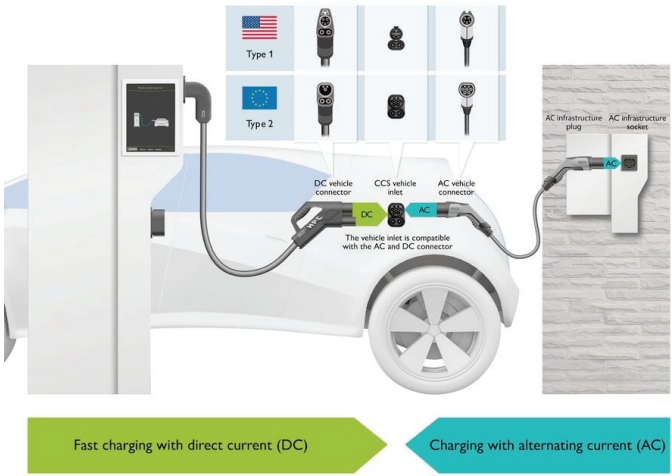


*Рис. 2.* Схема работы
комбинированного зарядного устройства

для зарядных штекеров как переменного, так и постоянного тока. В этом случае электромобилю требуется только один интерфейс для зарядки как переменным, так и постоянным током.

Оборудованием всех типов будут оснащены ЭЗС, осуществляющие автономную заправку электромобилей. Подачу тока для зарядки, контроль состояния ЭЗС, оплату заправки будет осуществлять информационная система.

С одной стороны, такая система должна быть автономной и не предполагать персонал, который бы занимался контролем подачи тока ЭЗС при зарядке электромобиля. С другой стороны, необходимо отслеживать состояние каждой зарядной станции в системе, чтобы контролировать процесс зарядки, проверять состояние: станция рабочая/нерабочая; проводить оплату клиентами за зарядку электромобиля, учитывать возможности расширения парка географически удаленных друг от друга зарядных устройств, большего количества клиентов с разными типами электромобилей.

Для разработки информационной системы сети автомобильной ЭЗС необходимо учитывать следующие требования (рис. 3):

– возможность обрабатывать большое количество запросов и постоянно отслеживать состояние каждой ЭЗС в системе;
– большая удаленность ЭЗС друг от друга;
– возможность работы с клиентами в разных регионах страны;
– наличие большого парка ЭЗС с разным типом зарядки;

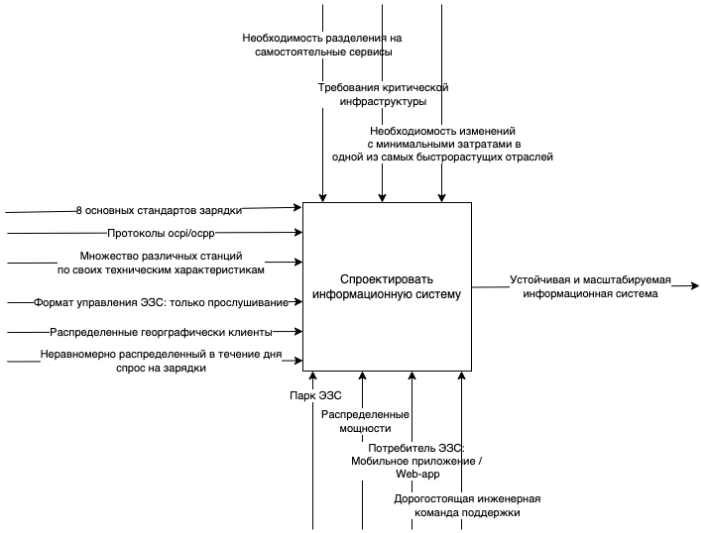


*Рис. 3.* Требования к информационной системе

– доступность системы 24/7;
– возможность интеграции информационной системы по спектру протоколов со сторонними организациями;
– возможный вариант реализации информационной системы как монолитной, с возможностью выделения отдельных сервисов для реализации клиент-серверной архитектуры и микросервисов для реализации отдельных функций.

Ключевым моментом программного отслеживания состояния ЭЗС является процесс зарядки электромобиля. При этом необходимо, чтобы:

1) происходила авторизация пользователя посредством радиочастотной идентификации;
2) отслеживалось состояние ЭЗС с помощью светодиодного индикатора;
3) производилось измерение дифференциального тока как показателя заправки электромобиля, так и корректной работы зарядной станции.

Стабильный процесс зарядки автомобиля от ЭЗС обеспечивается множеством систем на обеих сторонах безопасности – контроля и мониторинга, подсчета и калькуляции, которые в реальном режиме взаимодействуют между собой. Для обработки состояний ЭЗС предполагается использовать распределенную систему обработки

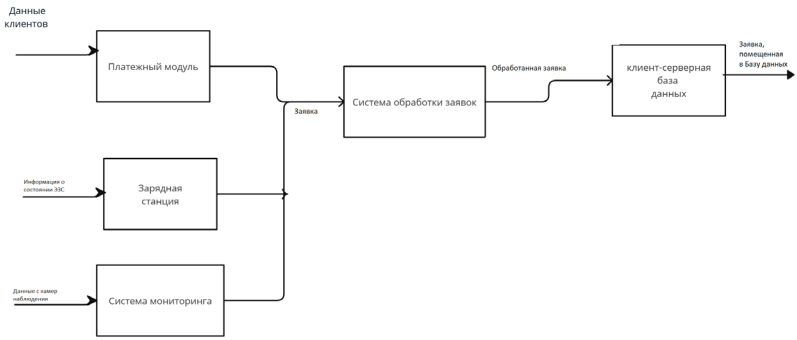


*Рис. 4.* Формирование заявки

информации. В этом случае состояние ЭЗС удобно рассматривать как заявку, которая будет иметь статусы: «ожидает бронирования», «забронирована», «выдана» (рис. 4).

Такой подход позволит рассматривать разрабатываемую информационную систему как автомат по обработке заявок. Состояние автомата удобно хранить в базе данных, а обрабатывать заявку (преобразовывать вход автомата в выход) следует в несколько потоков. Число потоков разумно выбирать в зависимости от вычислительных мощностей, а не от числа активных заявок.

Реализовать такую систему удобно с помощью нескольких рабочих потоков, каждый из которых обрабатывает события следующим образом:

– извлекает событие из очереди (например, внутреннее сообщение от подсистемы обмена);
– определяет, к какому автомату относится событие;
– считывает его состояние из постоянного хранилища (БД);
– обрабатывает событие;
– сохраняет в БД новое состояние автомата и удаляет событие из очереди событий.

В связи с особенностями существующих правил безопасности на большинстве ЭЗС нет возможности выполнить запрос серверу на выполнение того или иного действия, именно поэтому должна выполняться проверка состояния ЭЗС со стороны сервера по определенному протоколу и порту[4].

[4] *Leijon J., Boström C.* Charging Electric Vehicles Today and in the Future // World Electr. Veh. J. 2022, 13 (8), 139. URL: https://www.mdpi.com/2032-6653/13/8/139/htm (дата обращения 20 мая 2023).

Информационная система обработки заявок построена на серверной части на Python3 и представляет собой классическую СМО ДБА (система массового обслуживания с отказами). Она имеет разработанную систему единой конфигурации проекта, что позволит осуществлять установку и настройку независимо от программной или аппаратной части сервера и клиентского устройства. Интерфейс системы разработан с помощью функционала библиотеки Tkinter, что позволяет создавать графические интерфейсы для приложений на Python. Система обработки заявок работает следующим образом:

1. Пользователь отправляет заявку через интерфейс системы.
2. Заявка попадает в очередь на обработку.
3. Система выбирает свободный обработчик и отправляет ему заявку на обработку.
4. Обработчик начинает обработку заявки.
5. Если обработчик не может обработать заявку, он отправляет ее на повторную обработку или отклоняет.
6. При успешной обработке заявки система отправляет уведомление пользователю.

Таким образом, информационная система обработки заявок на Python3 является надежной и удобной в использовании. Она позволяет пользователям легко отправлять заявки и получать уведомления о статусе их обработки.

Большинство станций имеет возможность передавать все значения своих параметров одним пакетом. То есть при обращении к конкретной станции происходит создание файла в формате, аналогичном json. Он содержит несколько тысяч ключей, описывающих состояние данной ЭЗС, что сильно нагружает вычислительные мощности информационной системы.

В информационной системе будут рассматриваться два процесса генерации и обработки заявок с закрепленным для каждого клиента сервером и с динамическим выбором сервера. Оба процесса моделируют систему массового обслуживания с отказами, где заявки поступают в очередь на обработку и выбираются свободным обработчиком.

Однако в первом процессе каждый клиент закреплен за определенным сервером, а во втором процессе заявка распределяется на сервер с наименьшей загрузкой. В первом процессе клиенты генерируют заявки на обработку, которые поступают в очередь конкретного сервера, если у него есть свободное место. Если места нет, заявка отклоняется. Сервер выбирает заявку из очереди и начинает ее обработку. По завершении обработки заявка удаляется из очереди. Каждый клиент закреплен за определенным сервером,

что может повлиять на загруженность определенных серверов и время ожидания заявок.

Во втором процессе заявки генерируются клиентами и распределяются на сервер с наименьшей загрузкой. Заявка поступает в очередь выбранного сервера и выбирается свободным обработчиком для обработки. По завершении обработки заявка удаляется из очереди. Этот процесс позволяет более равномерно распределить нагрузку на серверы и уменьшить время ожидания заявок. Оба процесса могут быть смоделированы для исследования различных параметров, таких как время ожидания заявок, загруженность серверов, количество отклоненных заявок и др. Это позволяет оптимизировать систему обработки заявок и улучшить ее эффективность.

Структура заявки может выглядеть следующим образом (рис. 5):

– id (уникальный идентификатор заявки);
– время_поступления (время, когда заявка поступила в систему);
– тип_заявки (описание того, что нужно выполнить на сервере);
– статус (текущий статус заявки, например «в очереди», «выполняется», «выполнена»);
– id_сервера (идентификатор сервера, на который отправлена заявка);
– время_обработки (время, которое затратил сервер на выполнение заявки);

Форма заявки не будет зависеть от того, на каком сервере она будет обрабатываться: закрепленным за клиентом или с динамическим выбором. Заявки будет удобно хранить в базе данных.

Структура базы данных может выглядеть следующим образом (рис. 6):

Таблица «Серверы»:

– id (уникальный идентификатор сервера);
– название (название сервера);
– адрес (IP-адрес сервера);
– время_обработки_заявки (время, необходимое серверу для обработки одной заявки);
– текущая_загрузка (количество заявок, которые в данный момент обрабатывает сервер).

Таблица «Очереди»:

– id (уникальный идентификатор очереди);
– id_сервера (идентификатор сервера, к которому относится очередь);
– время_ожидания (время, которое заявка проведет в очереди перед обработкой).

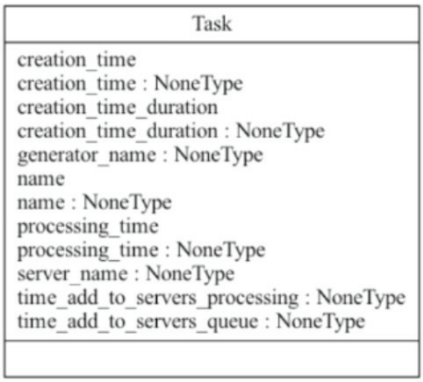


*Рис. 5.* Структура заявки

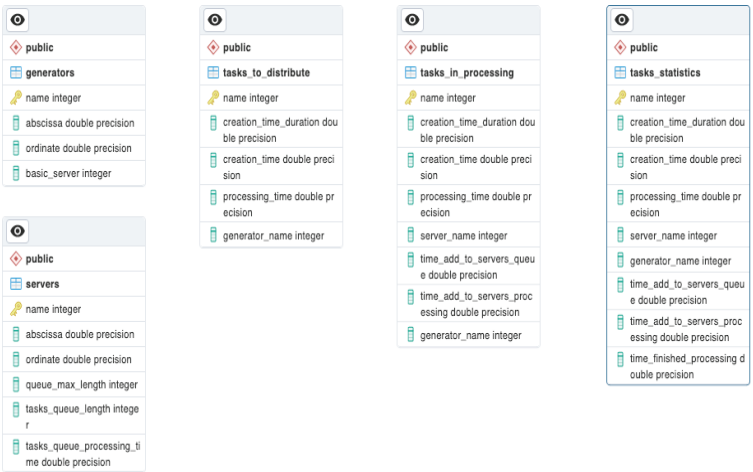


*Рис. 6.* Структура базы данных, обрабатывающей заявки

Таблицы, которые позволяют обработать заявку, – это данные по поступающим заявкам, обрабатываемым заявкам и статистике обработки заявок. Все эти таблицы имеют похожую структуру.

Таблица «Заявки на просмотр»:

– id (уникальный идентификатор);
– время_создания_заявки (будет использовано системное время);

– время_задержки (будет использовано системное время между созданием заявки и попаданием ее на сервер);
– время_ожидания (время, которое заявка проведет в очереди перед обработкой).

Таблица по обработке заявок, кроме представленных выше полей, будет содержать данные сервера, на который поступила обрабатываемая заявка, время поступления в очередь обработки и время обработки заявки.

Для получения статистики будет добавлено время завершения обработки заявки.

При поступлении новой заявки необходимо выбрать сервер с минимальным временем обработки существующей очереди, который готов принимать новую заявку.

Для этого можно использовать следующий алгоритм:

1. Получить список всех серверов из таблицы «Серверы».

2. Для каждого сервера вычислить время, необходимое для обработки всех заявок в его очереди (текущая_загрузка * время_обработки_заявки).

3. Отфильтровать список серверов, оставив только те, у которых время обработки очереди меньше или равно времени ожидания новой заявки.

4. Отсортировать отфильтрованный список по возрастанию времени обработки очереди.

5. Выбрать первый сервер из отсортированного списка и отправить на него новую заявку. При обработке заявок необходимо также обновлять информацию о текущей загрузке серверов в таблице «Серверы».

Реализация описанного выше алгоритма на языке Python представлена на рис. 7.

Такая распределенная система будет позволять эффективно обрабатывать данные даже при высокой нагрузке на серверы, что необходимо для объекта критической инфраструктуры.

Важно понимать, что ЭЗС является объектом критической инфраструктуры, поэтому ее работа должна быть обеспечена в режиме 24/7. Также необходимо организовать стабильное и устойчивое взаимодействие клиента с сервером посредством некоторого приложения или web-интерфейса. При этом разрабатываемая информационная система должна иметь платежный модуль (Celery) и электрическую балансировку (EnelX).

```
1 usage  new *
def __add_task_to_server_queue_dynamic(self, task_, generator_):
    self._connect()

    self._cursor.execute("SELECT name FROM servers WHERE queue_max_length > tasks_queue_length "
                         "ORDER BY SQRT((%s-abscissa)*(%s-abscissa) + (%s-abscissa)*(%s-abscissa))",
                         (generator_.abscissa, generator_.abscissa, generator_.ordinate, generator_.ordinate))

    servers_names_lst = self._cursor.fetchall()

    if len(servers_names_lst) > 0:
        self.insert_task_to_tasks_in_processing(name=task_.name,
                                                creation_time_duration=task_.creation_time_duration,
                                                creation_time=task_.creation_time,
                                                processing_time=task_.processing_time,
                                                server_name=servers_names_lst[0][0])
        self.delete_task_from_tasks_to_distribute(name=task_.name)

    self._disconnect()
```

*Рис. 7.* Реализация алгоритма
динамического выбора сервера

В соответствии с особенностями работы ЭЗС: увеличенной генерации трафика из-за постоянных проверок ее состояния, систему можно назвать высоконагруженной[5].

Более того, такую информационную систему следует сделать многомодульной. Это даст возможность перехода на более мощный сервер, позволит добавлять память и расширять интернет-каналы без потерь работоспособности системы.

Информационная система, построенная на основе макро- и микросервисов[6], представляет собой комплексное решение, которое позволяет обеспечить эффективное функционирование различных

[5] *Michaelson P., Holmberg D., Aasa B., Aasa U.* High load lifting exercise and low load motor control exercises as interventions for patients with mechanical low back pain: A randomized controlled trial with 24-month follow-up // Journal of rehabilitation medicine: official journal of the UEMS European Board of Physical and Rehabilitation Medicine. 2016. Vol. 48 (5). URL: https://www.researchgate.net/publication/301563842_High_load_lifting_exercise_nd_low_load_motor_control_exercises_as_interventions_for_patients_with_mechanical_low_back_pain_A_randomized_controlled_trial_with_24-month_follow-up (дата обращения 20 мая 2023).

[6] *Rad B.B., Bhatti H.J., Ahmadi M.* An Introduction to Docker and Analysis of its Performance // IJCSNS International Journal of Computer Science and Network Security. 2017. Vol. 17, no. 3. March. URL: https://www.researchgate.net/publication/318816158_An_Introduction_to_Docker_and_Analysis_of_its_Performance (дата обращения 20 мая 2023).

бизнес-процессов в организации. Макросервисы[7] – это крупные модули системы, которые выполняют функции, связанные с обработкой больших объемов данных, управлением процессами и взаимодействием с другими сервисами. Они обеспечивают высокую производительность и масштабируемость системы, а также позволяют управлять ее целостностью и безопасностью. Микросервисы – это небольшие модули системы, которые выполняют узкоспециализированные функции. Они могут быть разработаны независимо друг от друга и могут работать на разных платформах. Микросервисы позволяют быстро внедрять новые функции и изменения в систему, а также легко масштабировать ее при необходимости. Информационная система на базе макро- и микросервисов может включать в себя следующие функции:

– управление бизнес-процессами – система может автоматизировать различные бизнес-процессы, такие как управление заказами, инвентаризация, управление производственными процессами и т. д.;
– управление данными – система может обеспечивать хранение, обработку и анализ больших объемов данных, а также их интеграцию с другими системами;
– управление взаимодействием с клиентами – система может обеспечивать управление отношениями с клиентами, автоматизировать процессы продаж и маркетинга, а также обеспечивать высокий уровень обслуживания клиентов;
– управление ресурсами – система может обеспечивать управление ресурсами организации, такими как финансы, персонал, оборудование и т. д.;
– управление безопасностью – система может обеспечивать высокий уровень безопасности данных и процессов в организации;
– управление инфраструктурой – система может обеспечивать управление инфраструктурой организации, такой как сети, серверы, хранилища данных и т. д.

Таким образом, информационная система на базе макро- и микросервисов обеспечивает эффективное управление бизнес-процессами в организации, обеспечивая высокую производительность, масштабируемость, безопасность и гибкость системы.

Микросервисная архитектура позволяет это реализовать, однако она требует постоянного мониторинга изменений в конфигурационных метаданных программных систем, а также управления такими изменениями и инфраструктурой.

---

[7] *Rad B.B., Bhatti H.J., Ahmadi M.* An Introduction to Docker and Analysis of its Performance.

Микросервисная архитектура относится к распределенным системам. Согласно определению, распределенная система[8] – набор компьютерных программ, которые используют вычислительные ресурсы нескольких отдельных вычислительных узлов для достижения общей цели. Распределенные системы помогают повысить надежность и производительность и упрощают масштабирование системы. В случае большой нагрузки на систему можно добавить дополнительные узлы, которые могут организовать многопоточность обработки данных[9]. Управление конфигурацией помогает техническим командам создавать стабильные и надежные системы с помощью инструментов, которые автоматически управляют обновлениями конфигурационных данных и отслеживают их, что позволяет синхронизировать работу программного обеспечения в рамках микросервисной архитектуры, поскольку в центре конфигурации появляется достоверный источник информации. В готовую высоконагруженную систему мониторинг встроить нельзя, поэтому разработка системы должна иметь возможность встраивания датчиков мониторинга[10].

В процессе изучения особенностей отрасли ЭЗС стало ясно, что в большинстве структур имеются относительно большие приложения, которые нужно выносить на отдельные вычислительные мощности (рис. 8).

На рис. 7 показан пример разделения системы на отдельные макросервисы[11], такие как билинг, каждый из которых имеет свой набор микросервисов[12].

---

[8] *Rad B.B., Bhatti H.J., Ahmadi M.* An Introduction to Docker and Analysis of its Performance.

[9] Op. cit.

[10] Configuration Best Practices // The Kubernetes Authors. URL: https://kubernetes.io/docs/concepts/configuration/overview/ (дата обращения 20 мая 2023).

[11] *Fan Wei, Qian Zhang.* Research on the Application of Microservice Architecture in Administrative Law Enforcement Supervision System // Journal of Physics: Conf. Series. 2019. Vol. 1237. P. 022055. URL: https://iopscience.iop.org/article/10.1088/1742-6596/1237/2/022055/pdf (дата обращения 20 мая 2023).

[12] *Lewis J., Fowler M.* Microservices a definition of this new architectural term. 2014. 25 March. URL: https://netman.aiops.org/~peidan/ANM2022/7.TraceAnomalyDetection/LectureCoverage/Microservices.pdf (дата обращения 20 мая 2023).

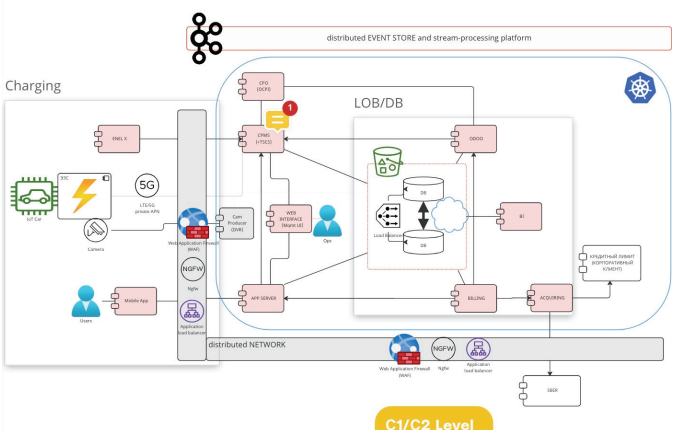


*Рис. 8.* Пример архитектуры информационной системы для ЭЗС

Микросервисное приложение для обслуживания и заправки электромобилей будет иметь следующие функции:

1. Синхронизация с мобильным приложением для клиентов: пользователи смогут использовать мобильное приложение для поиска ближайшей станции заправки, резервирования зарядного устройства и оплаты услуг.

2. Система оплаты: будет реализована платежная система, которая будет взаимодействовать с банком и обрабатывать платежи от клиентов.

3. Система мониторинга: будут установлены видеокамеры, которые будут следить за работой станции заправки и обеспечивать безопасность пользователей. Система мониторинга будет напрямую зависеть от видеокамер, поэтому ее можно изменять без влияния на работу клиент-серверной части.

4. Web-интерфейс: будет разработан web-интерфейс для управления станцией заправки, проверки работы устройств и их актуального состояния.

5. Система билинга: будет реализована система билинга, которая будет отвечать за проверку работы устройств и их актуального состояния.

6. Мобильное приложение под ios или Android: будет разработано мобильное приложение для клиентов с возможностью дальнейшей модификации.

7. Межсетевой экран: система макро- и микросервисов будет отделена от основной системы межсетевым экраном для предотвращения утечки пользовательских данных и изоляции работы основной части информационной системы.

8. Распределенная система обработки информации: для обеспечения стабильной работы системы клиент-серверной части при высокой нагрузке будет добавлена подсистема загрузки сервера и реализована как распределенная система обработки информации.

9. Система управления электрозаправкой будет следить за зарядными устройствами и автоматически управлять процессом зарядки электромобилей.

10. Система управления запасами будет следить за наличием необходимых материалов и запчастей для обслуживания станции заправки.

11. Система управления персоналом будет следить за работой сотрудников и обеспечивать эффективную работу станции заправки.

12. Система мониторинга качества необходима для отслеживания качества обслуживания клиентов и работы станции заправки в целом.

13. Система управления энергопотреблением будет оптимизировать потребление энергии и снижать затраты на электроэнергию.

14. Система управления техническим обслуживанием будет отслеживать состояние оборудования и проводить регулярное техническое обслуживание станции заправки.

15. Система управления аварийными ситуациями нужна для быстрого реагирования на возможные аварии и обеспечение безопасности пользователей.

Микросервисное приложение для обслуживания и заправки электромобилей будет синхронизировано с мобильным приложением для клиентов и системой оплаты. Они будут отделены от основной системы межсетевым экраном (fierwall) для предотвращения утечки пользовательских данных и изоляции работы основной части информационной системы, которая будет включать в себя систему мониторинга с камер, установленных рядом с ЭЗС.

В основной части также будут находиться web-интерфейс, система билинга, отвечающая за проверку работы устройств, а также их актуального состояния. К основной части также будет относиться платежная система, взаимодействующая с банком. Данные части информационной системы удобно реализовывать как микросервисы, поскольку они могут быть дополнены или изменены. Например, можно реализовать мобильное приложение под ios или Android с возможностью дальнейшей модификации, которая не будет существенно влиять на систему клиент-сервер, обрабатывающую запросы.

Система мониторинга может быть изменена, поскольку она будет напрямую зависеть от видеокамер. Устаревшая система наблюдения может быть заменена на новую, также без влияния на работу клиент-серверной части, содержащей базу данных. Клиент-серверную часть будет удобно разрабатывать как монолитную систему, которая должна стабильно работать даже при высокой нагрузке, поэтому необходимо добавить подсистему загрузки сервера и реализовать ее как распределенную систему обработки информации.

Таким образом, сформулированные технические требования показывают, что разрабатываемая информационная система по обеспечению работы ЭЗС будет учитывать особенности зарядных станций, их возможное удаленное расположение и доступность системы 24/7. Разрабатываемая система будет иметь гибридную архитектуру: Клиент-серверная часть будет реализована как монолитная структура, с возможностью подключения дополнительных серверов и распределения нагрузки на них. Остальные модули будут реализованы как микросервисы, что позволит расширить возможности системы в целом, подключая новые функции и модифицируя оборудование или приложения, не влияя на работу всей системы.

## *Литература*

Казарин, Шаряпов, Ященко 2018 – *Казарин О.В., Шаряпов Р.А., Ященко В.В.* Многофакторная классификация угроз информационной безопасности киберфизических систем // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2018. № 1 (1). С. 39–55.

## *References*

Kazarin, O.V., Sharyapov, R.A. and Yashchenko, V.V. (2018), “Multifactorial classification of threats to information security of cyber-physical systems”. *RSUH/RGGU Bulletin. “Information Science. Information Security. Mathematics” Series*, vol. 1 (1), pp. 39–55.

### *Информация об авторах*

*Марина С. Шаповалова*, кандидат педагогических наук, доцент, Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия; 105005, Россия, Москва, 2-я Бауманская ул., д. 5, стр. 1, mshapovalova84@gmail.com

*Александр А. Андреев*, студент, Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия; 105005, Россия, Москва, 2-я Бауманская ул., д. 5, стр. 1, andreev@indry.tech

*Валерия В. Чувашова*, студент, Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия; 105005, Россия, Москва, 2-я Бауманская ул., д. 5, стр. 1, chuvashova@indry.tech

## *Information about the authors*

*Marina. S. Shapovalova*, Cand. of Sci. (Pedagogy), associate professor, Bauman Moscow State Technical University, Moscow, Russia; bld. 5, 2nd Bauman Str., Moscow, Russia, 105005; mshapovalova84@gmail.com

*Aleksandr A. Andreev*, student Bauman Moscow State Technical University, Moscow, Russia; bld. 5, 2nd Bauman Str., Moscow, Russia, 105005; andreev@indry.tech

*Valeriya V. Chuvashova*, student Bauman Moscow State Technical University, Moscow, Russia; bld. 5, 2nd Bauman Str., Moscow, Russia, 105005; chuvashova@indry.tech

УДК 004.056
DOI: 10.28995/2686-679X-2023-3-38-48

# Об итогах VI Всероссийской научно-практической конференции «Информационная безопасность: вчера, сегодня, завтра»

Валерий В. Арутюнов
*Москва, Россия, warut698@yandex.ru*

Наталия В. Гришина
*Российский государственный гуманитарный университет, Москва, Россия, grnat@rambler.ru*

*Аннотация.* Анализируются итоги состоявшейся в Москва в Российском государственном гуманитарном университете (РГГУ) Всероссийской научно-практической конференции, на которой заслушано более 20 докладов из различных научных и образовательных организаций. Тематика докладов была посвящена общим вопросам обеспечения информационной безопасности, программно-аппаратным методам защиты информации; рассматривались также перспективы развития различных направлений обеспечения информационной безопасности. Тематика пленарных докладов включала: тенденции развития информационного противоборства в условиях глобальной информатизации, риски аутсорсинга и привлечения подрядчиков к внедрению системы информационной безопасности, импортонезависимость национальной ИКТ-инфраструктуры: этико-инжиниринговый взгляд, программно-алгоритмическое обеспечение оценки деструктивности телеграм-каналов, моделирование оценки эффективности системы контроля информационной безопасности открытых социотехнических систем, вопросы построения надежной системы обеспечения информационной безопасности предприятия и др. В докладах на трех секциях рассматривались: особенности обеспечения информационной безопасности объектов критической информационной инфраструктуры в области электроэнергетики, анализ методов взлома и разрушения стеганографического контейнера в файле изображения, анализ последствий нарушения безопасности персональных данных с позиций интересов злоумышленника, апробация моделей анализа и прогнозирования информационного противоборства в социуме в имитационной среде Anylogic и др.

*Ключевые слова:* информационная безопасность, защита информации, информационные технологии, аппаратные средства защиты, информационные системы, программные средства защиты, система защиты информации

*Для цитирования: Арутюнов В.В., Гришина Н.В.* Об итогах VI Всероссийской научно-практической конференции «Информационная безопасность: вчера, сегодня, завтра» // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2023. № 3. С. 38–48. DOI: 10.28995/2686-679X-2023-3-38-48

# On the results of the 6th All-Russian Scientific and Practical Conference "Information Security. Yesterday, Today, Tomorrow"

Valerii V. Arutyunov
*Moscow, Russia, warut698@yandex.ru*

Nataliya V. Grishina
*Russian State University for the Humanities, Moscow, Russia, grnat@rambler.ru*

*Abstract*. The article analyzes results of the All-Russian Scientific and Practical Conference held in Moscow at the Russian State University for the Humanities (RGGU), at which more than 20 reports from various scientific and educational organizations were heard. The reports dealt with general issues of information security, software and hardware methods of the information protection; prospects for the development of various areas of the information security were also considered.

The topics of the plenary reports included: trends in the development of the information warfare in the context of global informatization, the risks of outsourcing and attracting contractors to the implementation of an information security system, the import-independence of the national ICT infrastructure: an ethical and engineering view, software and algorithmic support for assessing the destructiveness of telegram channels, modeling the evaluation of the effectiveness of the information security control system of open sociotechnical systems, issues of building a reliable enterprise information security systems, etc.

The reports in three sections considered: features of ensuring the information security of critical information infrastructure facilities in the field of electric power, analysis of methods of hacking and destruction of a steganographic container in an image file, analysis of the consequences of a breach of personal data security from the standpoint of the intruder's interests, testing models of

analysis and forecasting of the information warfare in society in the simulation environment of Anylogic, etc.

*Keywords:* information security, data protection, information technology, hardware protection, information systems, information protection system

*For citation:* Arutyunov, V.V. and Grishina, N.V. (2023), "On the results of the 6th All-Russian Scientific and Practical Conference 'Information Security. Yesterday, Today, Tomorrow' ", *RSUH/RGGU Bulletin. "Information Scince. Information Security. Mathematics" series*, no. 3, pp. 38–48, DOI: 10.28995/2686-679X-2023-3-38-48

В Российском государственном гуманитарном университете (РГГУ) наряду с реализацией образовательного процесса для студентов, обучающихся по различным направлениям информационной безопасности, не остаются без внимания и вопросы привлечения их к участию в различных форумах, на которых обсуждаются вопросы защиты информации на предприятиях и которые происходят как в других организациях, так и в самом университете[1,2,3].

12 апреля 2023 г. в РГГУ состоялась VI Всероссийская научно-практическая конференция «Информационная безопасность: вчера сегодня, завтра», для участия в которой зарегистрировалось около 90 ученых и специалистов из более 30 организаций страны: от Орла до Хабаровска и от Санкт-Петербурга до Донецка. На конференцию было представлено более 20 докладов для трех секций: Общие вопросы обеспечения информационной безопасности, Программно-аппаратные методы и средства защиты информации,

[1] Всероссийская студенческая Олимпиада 2023 по информационной безопасности. URL: https://www.rsuh.ru/anons/vserossiyskaya-studencheskaya-olimpiada-po-informatsionnoy-bezopasnosti/ (дата обращения 18 апреля 2023).

[2] Программа Всероссийской конференция 2023 – Программа Всероссийской научно-практической конференции «Информационная безопасность: вчера, сегодня, завтра». URL: https://www.rsuh.ru/anons/konferentsiya-informatsionnaya-bezopasnost-vchera-segodnya-zavtra2/ (дата обращения 9 апреля 2023).

[3] Программа Международной конференции «Взаимодействие вузов, научных организаций и учреждений культуры в сфере защиты информации и технологий безопасности». URL: https://www.rsuh.ru/anons/mezhdunarodnaya-konferentsiya-vzaimodeystvie-vuzov-nauchnykh-organizatsiy-i-uchrezhdeniy-kultury-v-sfere-zashchity-informatsii-i-tekhnologiy-bezopasnosti4/ (дата обращения 10 апреля 2023).

Практика и перспективы развития направлений информационной безопасности.

Основная цель прошедшей конференции – обеспечение обмена опытом и новыми научными знаниями в области информационной безопасности между учеными и специалистами, работающими в различных областях защиты информации.

Одной из отличительных особенностей конференции стало практически двукратное превышение количества докладов, представленных на первую и третью секции, по сравнению со второй. При этом отмечается активное участие в конференции не только ожидаемых представителей из организаций РАН, Московского государственного технического университета им. Н.Э. Баумана (МГТУ), университетов силовых ведомств России, но также участников из гуманитарных вузов страны: Московского государственного лингвистического университета (МГЛУ), Российского государственного социального университета (РГСУ), Международной академии бизнеса и управления и др. Для конференции в этом году было характерно также превалирование числа докладов, авторами которых являлись не менее двух участников конференции (число этих докладов составляло около 70% от общего числа работ, одобренных Оргкомитетом конференции).

Ниже приводится краткий обзор основных пленарных и секционных докладов, представляющих интерес для специалистов в области информационной безопасности.

В докладе доктора технических наук В.В. Арутюнова (РГГУ) «*Вестник РГГУ, серия "Информатика. Информационная безопасность. Математика": к пятилетию выпуска в свет первого номера журнала*» рассматриваются тематические особенности публикаций за пятилетний период в журнале «Вестник РГГУ, серия "Информатика. Информационная безопасность. Математика"». Приводятся динамика изменения количества статей в разделах журнала, распределение статей по основным разделам журнала и организациям – источникам публикаций, лидером среди которых в области информационной безопасности и математики является РГГУ, а в области информатики – МГТУ.

Автором анализируются основные изданные в журнале статьи в области информационной безопасности, в число которых вошли работы по следующей тематике: использование технологии блокчейн в области защиты информации, применение генетических алгоритмов в криптографии, квантовая криптография: история возникновения, современное состояние и перспективы развития, обеспечение информационной безопасности детей в Российской Федерации, особенности формирования политики информацион-

ной безопасности российских вузов, наукометрические показатели результатов исследований российских ученых в области информационной безопасности и др.; отмечается, что, по данным РИНЦ, число просматриваемых специалистами статей журнала возросло только за последние три года более чем в шесть раз: со 140 в 2019 г. до 930 в 2021 г.

Доклад доктора технических наук С.И. Неизвестного (Финансовый университет при Правительстве РФ) *«Риски аутсорсинга и привлечения подрядчиков к внедрению системы информационной безопасности»* посвящен рассмотрению особенностей ограниченных ресурсов предприятий, которые вынуждают их руководство часть функций предприятия передавать на аутсорсинг внешним организациям. Эта же нехватка ресурсов диктует необходимость привлечения подрядчиков для выполнения ряда работ, в частности, для внедрения информационных систем. При этом и использование аутсорсинга, и привлечение подрядчиков увеличивают риск обеспечения информационной безопасности, в связи с чем в работе анализируются проблемы минимизации информационных рисков при использовании организацией аутсорсинга и подрядных работ. Особого внимания, по мнению автора, заслуживает рассмотрение защиты информации при работе с использованием договорных отношений с подрядчиками по форме EPCM, а также отмечается, что на уровне взаимодействия между организациями проблема обеспечения информационной безопасности при использовании аутсорсинга и подрядчиков в целом является проблемой корпоративной культуры и установления истинных доверительных отношений между участниками бизнеса.

В докладе доктора физико-математических наук Ю.В. Пруса, В.В. Серикова (ВНИИ по проблемам гражданской обороны и чрезвычайных ситуаций), Е.С. Зиновьевой (Владимирский государственный университет имени А.Г. и Н.Г. Столетовых) *«Тенденции развития информационного противоборства в условиях глобальной информатизации»* обсуждаются новые виды внешних и внутренних угроз в информационной сфере, порождаемые развитием «цифровых» технологий; сформулированы понятия информационного противоборства, а также информационных войн и информационного терроризма как его крайних форм. Авторы классифицируют субъекты и объекты информационного противоборства, а также отмечают, что развитие «цифровых» технологий порождает новые риски и проблемы, связанные с обострением внешних и внутренних угроз в информационной сфере для личности, общества и государства. Противоборство в информационной сфере между государственными, общественными, коммерческими структурами,

социальными и политическими группами по мере развития «цифровых» технологий обостряется до крайних форм своего проявления – информационных войн и информационного терроризма.

При этом в период проведения специальной военной операции для России проблемы информационного противоборства и его крайних проявлений в форме информационной войны и информационного терроризма приобрели особую остроту.

Тенденции развития новых средств и способов информационного противоборства имеют глобальный характер, однако геополитическое и экономическое положение государств может способствовать ускорению негативных процессов и повышению уровня угроз в информационной сфере.

В докладе доктора технических наук В.А. Минаева, А.Д. Черных (Московский университет МВД России им. В.Я. Кикотя), А.В. Симонова (Московский государственный технический университет им. Н.Э. Баумана) *«Программно-алгоритмическое обеспечение оценки деструктивности телеграм-каналов»* констатируется, что цель работы состоит в разработке программно-алгоритмического обеспечения, позволяющего автоматизировать систему оценки телеграм-каналов для контроля наличия в них текстового контента экстремистского характера. Авторами сформированы текстовые корпуса для обучения классификатора на основе модели глубокой искусственной нейронной сети BERT, выполнена предварительная обработка текстового контента, оценены итоги работы на основе этой модели. Посредством разработки телеграм-бота были собраны материалы для апробации результатов моделирования и тестирования программного продукта на экспериментальных данных; исследованы топ-10 каналов, ранжированных по доле размещенного в них экстремистского контента.

Проведенные эксперименты показали эффективность разработанного метода оценки деструктивности телеграм-каналов. Метод реализован в соответствующем программном продукте, предназначенном для использования в работе государственных структур, занимающихся выявлением контента противоправного характера.

Определены перспективы применения разработанного программно-алгоритмического обеспечения.

Доклад кандидата юридических наук Ю.А. Белевской (Орловский государственный университет им. И.С. Тургенева), доктора технических наук А.П. Фисуна, кандидата технических наук А.Б. Басукинского (Управление по Орловской области, филиал ФГУП «ГРЧЦ» в ЦФО), Р.А. Фисуна (Отделение по Смоленской области Главного управления ЦБ России***)*** *«Моделирование оценки эффективности системы контроля информационной безопасности*

*открытых социотехнических систем»* посвящен оценке эффективности системы контроля информационной безопасности (СКИБ) открытых социотехнических систем, основанной на количественных методах измерения состояния их информационной безопасности, обеспечивающих эффективное управление функционированием компонентов информационно-телекоммуникационных сетей и систем в целом.

Как отмечают авторы, по итогам выполненных расчетов определяющими факторами полноты оценок эффективности системы контроля информационной безопасности являются производительность средств СКИБ и соответствующая ей полнота, достоверность информации в СКИБ, а также обеспечение СКИБ измерение заданного объема контролируемых показателей системы обеспечения информационной безопасности.

В докладе доктора технических наук С.Б. Вепрева (Российская академия народного хозяйства и государственной службы при Президенте РФ) *«А возможно ли отключить Интернет от России?»* рассматриваются вопросы современного состояния и возможности использования сети Интернет как средства передачи данных с учетом проблемы защиты информационных ресурсов отдельных пользователей и автоматизированных информационных систем. В работе отмечается, что в настоящее время в сети имеются 13 DNS серверов высшего уровня, девять серверов из которых контролируются госучреждениями США и являются закрытыми. Остальные четыре сервера также контролируются США, но являются открытыми, и к ним подключены все страны мира, в том числе и Россия; таким образом обеспечивается возможность контроля всего трафика по сети Интернет.

По мнению автора, одной из основ обеспечения национальной безопасности России в условиях ведения против нее гибридной войны является импортонезависимость экономики страны.

Автор также отмечает, что высокого уровня результативности в системе обеспечения отечественной импортонезависимости от иностранных средств информационных технологий трудно достичь без целенаправленной этической подготовки кадров социальной инженерии, задачами которой являются системное нравственное воспитание, конструирование новых трудовых, правовых, нравственных отношений, традиций в научной, трудовой деятельности. При этом наиболее эффективными путями в обеспечении импортонезависимости от иностранных средств информационных технологий являются: организация возврата в страну отечественных научных кадров; открытие высокооплачиваемых рабочих мест для иностранных специалистов; активиза-

ция работы разведывательных структур для поиска и вовлечение в отечественное производство иностранных инновационных технологий; создание в Министерстве экономического развития РФ, Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций специальных структур управления обеспечением импортонезависимости от иностранных средств информационных технологий и ряд других.

Доклад кандидата технических наук А.С. Мосолова (Российский химико-технологический университет им. Д.И. Менделеева), доктора технических наук Ю.В. Пруса (ВНИИ по проблемам гражданской обороны и чрезвычайных ситуаций), Н.В. Мальцева, Н.А. Урбана (Российский государственный социальный университет) «*К вопросу построения надежной системы обеспечения информационной безопасности предприятия*» посвящен вопросу обеспечения информационной безопасности на опасных производственных объектах с использованием метода анализа угроз на основе результатов применения метода определения приоритетного сценария развития аварийной ситуации.

Авторы отмечают, что для повышения потенциального уровня защищенности информационной системы предприятия надо оптимизировать отчетность, необходимую для принятия решений по реагированию, противодействию компьютерным атакам и нейтрализации последствий этих атак.

Проектирование системы обнаружения вторжений основано на применении искусственного интеллекта. Диагностика состояния защищенности компьютерных систем производится с помощью модели искусственного интеллекта, которая имитирует биологическую иммунную систему. Обнаружение вредоносной информации обеспечивается благодаря алгоритму отрицательного отбора, который активно используется в искусственных иммунных системах.

Описанная в работе система обнаружения сетевых атак с моделированием искусственной иммунной системы, по мнению авторов, является эффективным инструментом для обеспечения сетевой информационной безопасности и повышает надежность систем при их использовании совместно со стандартными защитными мерами.

В докладе Ю.В. Капарулиной, кандидата исторических наук И.А. Русецкой (РГГУ) «*Особенности обеспечения информационной безопасности объектов критической информационной инфраструктуры в области электроэнергетики*» отмечается, что в современном мире одним из основных инструментов информационного воздействия являются компьютерные атаки на критически важные информационные и автоматизированные объекты государства. Электроэнергетическая сфера является одной из составляющих

сфер жизнеобеспечения общества, так как от нее зависят социальная, экономическая, политическая стабильность страны, а также ее национальная безопасность, поэтому обеспечение безопасности объектов критической информационной инфраструктуры в данной области носит обязательный для государства характер.

Стратегическая цель государства, направленная на обеспечение энергетической безопасности, определяет основные задачи и направления деятельности в области информационной безопасности объектов ТЭК. Главной особенностью при этом является категорирование объектов ТЭК по критериям потенциальной опасности и критической важности. При рассмотрении категорирования объектов критическая информационная инфраструктура (КИИ) электроэнергетики первым делом выделяется социальная значимость всех информационных систем, так как они предназначены для бесперебойного и надежного функционирования электросетевого комплекса. Кроме того, немаловажной особенностью является то, что большинство объектов КИИ ТЭК являются автоматизированными системами, направленными на сбор, обработку и анализ технологических данных, из чего вытекают специальные требования к безопасности таких объектов и мерам обеспечения информационной безопасности. Требования включают обеспечение физической защиты объектов энергетики, строгие и обязательные требования к системе управления персоналом в энергетической компании, а также обеспечение безопасности объектов КИИ.

Доклад кандидата технических наук А.В. Крыжановского, Е.И. Корчака (Поволжский государственный университет телекоммуникаций и информатики) *«Анализ методов взлома и разрушения стеганографического контейнера в файле изображения»* посвящен анализу методов разрушения стеганоконтейнера в графическом изображении и оценке эффективности их применения. Авторами была выполнена серия двухэтапных экспериментов, включающих формирование стегоконтейнера, содержащего конфиденциальную информацию, и моделирование атак, разрушающих стегоконтейнер, с целью проверки устойчивости стеганосистемы. В экспериментах использованы программные реализации для скрытия стегоконтейнера в графическом неподвижном изображении форматов JPEG и BMP.

Полученные авторами результаты экспериментов позволяют сделать вывод, что ни один из используемых алгоритмов не оказался робастным к геометрическим и негеометрическим атакам.

В докладе кандидата технических наук С.И. Сиротского (Национальный исследовательский Московский государственный строительный университет) *«Анализ последствий нарушения*

*безопасности персональных данных с позиций интересов злоумышленника»* анализируются возможные негативные последствия для субъектов персональных данных с позиций взаимосвязи их с действиями и интересами злоумышленников. Проводится выявление мотивов злоумышленников, направленных на несанкционированное завладение информацией, содержащей персональные данные, и сопоставляются возможные первичные цели злоумышленников, действующих в собственных интересах, с совокупностью вредных последствий, которые могут проявиться в отношении субъектов персональных данных. Отмечается, что в данном контексте вредные последствия для субъектов персональных данных являются не первоначальной целью, а следствием. Представлена модель, устанавливающая взаимосвязь действий и целей злоумышленника с совокупностью возможных последствий для субъектов персональных данных, исходя из которой следует, что характер и масштабы вредных последствий для операторов и субъектов персональных данных будут определяться конкретным составом персональных данных, которые в результате действий злоумышленника получают незаконное распространение.

Доклад кандидата технических наук К.М. Бондаря, Д.В. Чемарева (Дальневосточный юридический институт МВД России) *«Апробация моделей анализа и прогнозирования информационного противоборства в социуме в имитационной среде Anylogic»* посвящен описанию результатов апробации агентной модели распространения информации при помощи платформы имитационного моделирования Anylogic. Авторами для исследования актуальных вопросов информационных воздействий и информационного противоборства, использования открытого информационного пространства для организации и проведения деструктивных кампаний выбрана модель анализа и прогнозирования этих конфликтов в социуме с использованием метода агентного моделирования.

Проведенные авторами в процессе исследования эксперименты показали, что модель диффузии инноваций наиболее применима для описания процессов информационного «заражения», позволяя с достаточной точностью описывать процессы распространения информации и прогнозировать их динамику. Это позволяет сделать выводы, что модель диффузии инновации может быть применена для создания комплекса моделей, описывающих информационное противоборство.

Тексты докладов, одобренные Оргкомитетом конференции, к началу конференции изданы в Сборнике статей VI Всероссийской научно-практической конференции, индексируемом в РИНЦ [Информационная безопасность 2023].

## *Литература*

Информационная безопасность 2023 – Информационная безопасность: вчера, сегодня, завтра: Сб. ст. по материалам VI Всерос. научно-практич. конф. Москва, 12 апреля 2023 г. / Сост. Н.В. Гришина; отв. ред. В.В. Арутюнов. М.: РГГУ, 2023. 133 с.

## *References*

Grishina, N.V. (comp.) and Arutyunov, V.V. (rep. ed.) (2023), *Information security. Yesterday, today, tomorrow, Proceedings of the 6th All-Russian Scientific and Practical. Conf.*, Moscow, April 12, 2023, RGGU, Moscow, Russia, 133 p.

### *Информация об авторах*

*Валерий В. Арутюнов,* доктор технических наук, профессор, независимый исследователь, Россия, Москва; warut698@yandex.ru

*Наталия В. Гришина,* кандидат технических наук, доцент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; grnat@rambler.ru

### *Information about the author*

*Valerii V. Arutyunov,* Dr. of Sci. (Computer Science), professor, independent researcher, Moscow, Russia; warut698@yandex.ru

*Nataliya V. Grishina,* Cand.of Sci. (Computer Science), associate professor, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, Russia, 125047; grnat@rambler.ru

УДК 004.056
DOI: 10.28995/2686-679X-2023-3-49-60

# Проблемы управления рисками в сфере информационной безопасности

Игорь Б. Бакин
*Финансовый университет при Правительстве РФ, Москва, Россия, recuptw@gmail.com*

Камилла Ш. Ниязова
*Финансовый университет при Правительстве РФ, Москва, Россия, kamilla.niyazova@gmail.com*

София М. Шведова
*Финансовый университет при Правительстве РФ, Москва, Россия, Shvedova.2003@inbox.ru*

*Аннотация.* Данная статья посвящена проблемам управления рисками в сфере информационной безопасности (ИБ). В статье рассматриваются основные факторы, которые могут привести к нарушению требований информационной безопасности, такие как уязвимости в системе, ошибки персонала и действия злоумышленников, различные подходы к управлению рисками ИБ, включая технические и организационные меры. Особое внимание уделено значимости системы управления рисками для бизнеса в целом и для отдельных организаций в частности. В статье предложены практические рекомендации по управлению рисками ИБ и оценке эффективности такой системы. Результаты и выводы, представленные в статье, могут быть использованы для оптимизации системы управления рисками ИБ в организациях различных отраслей. Важным аспектом, подчеркиваемым в статье, является постоянная адаптация и обновление системы управления рисками в информационной безопасности в соответствии с изменяющейся ситуацией и технологическим развитием.

С помощью предложенных рекомендаций и оценок эффективности системы управления рисками ИБ организации могут повысить свою способность предотвращать инциденты безопасности, минимизировать потери данных, защитить репутацию и соблюсти законодательные требования. В конечном итоге эффективная система управления рисками ИБ становится неотъемлемой частью стратегии бизнеса, способствуя устойчивому развитию и обеспечению долгосрочного успеха.

*Ключевые слова:* аудит информационной безопасности; риски информационной безопасности; информационная безопасность, защита информации, управление рисками

*Для цитирования: Бакин И.Б., Ниязова К.Ш., Шведова С.М.* Проблемы управления рисками в сфере информационной безопасности // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2023. № 3. С. 49–60. DOI: 10.28995/2686-679X-2023-3-49-60

# Issues of risk management in the field of information security

Igor B. Bakin
*Financial University under the Government of the Russian Federation, Moscow, Russia, recuptw@gmail.com*

Kamilla Sh. Niyazova
*Financial University under the Government of the Russian Federation, Moscow, Russia, kamilla.niyazova@gmail.com*

Sofiya M. Shvedova
*Financial University under the Government of the Russian Federation, Moscow, Russia, Shvedova.2003@inbox.ru*

*Abstract.* The deals in issues of the risk management in the field of information security (IS). It considers the main factors that can lead to a violation of information security requirements, such as vulnerabilities in the system, human errors and actions of intruders, various approaches to IS risk management, including technical and organizational measures. Special attention is paid to the importance of the risk management system for business in general and for individual organizations in particular. The article offers practical recommendations for managing IS risks and evaluating the effectiveness of such a system. The results and conclusions presented in the article can be used to optimize the IS risk management system in organizations of various industries. An important aspect emphasized in the article is the ongoing adapting and updating the risk management system in information security according to the changing situation and technological development.

Through the suggested recommendations and assessments of the effectiveness of the IS risk management system, organizations can improve their ability to prevent security incidents, minimize data loss, protect reputation and comply with legal requirements. Ultimately, an effective IS risk management system becomes an integral part of the business strategy, contributing to sustainable development and ensuring long-term success.

*Keywords:* information security audit; information security risks; information security; information protection; risk management

*For citation:* Bakin, I.B., Niyazova, K.Sh. and Shvedova, S.M. (2023), "Issues of risk management in the field of information security", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 3, pp. 49–60, DOI: 10.28995/2686-679X-2023-3-49-60

## *Введение*

Исследование рисков информационной безопасности имеет большое значение, поскольку информационные технологии занимают все более важное место в нашей жизни, и значительная часть бизнес-процессов осуществляется в сети Интернет. Рост числа информационных технологий и возросшая зависимость от них приводят к увеличению рисков, связанных с нарушением [Наврузов 2022] информационной безопасности (ИБ). Уязвимости в системе, ошибки персонала, действия злоумышленников и другие факторы могут привести к серьезным последствиям для организаций и их клиентов, включая финансовые потери, утечку конфиденциальной информации, нарушение репутации и другие негативные последствия [Крючков, Прус, Резниченко 2018; Надеждин 2012; Гришина 2022].

Исследование рисков ИБ позволяет выявить уязвимости и оценить уровень рисков, связанных с использованием информационных технологий (ИТ), и разработать соответствующие меры для их уменьшения или предотвращения. Также исследование рисков ИБ помогает определить эффективность системы управления рисками и ее соответствие требованиям законодательства и стандартов.

Для того чтобы понимать, какой уровень защиты должен быть у защищаемой информационной системы, применяется процесс анализа рисков.

Анализ рисков ИБ – это процесс оценки потенциальных угроз для информационной системы (ИС) и выработки мер по их предотвращению, смягчению или уменьшению возможных негативных последствий[1].

[1] *Астахов А.* Как управлять рисками информационной безопасности? // ISO27000.ru URL: http://www.iso27000.ru/chitalnyi-zai/upravlenie-riskami-informacionnoi-bezopasnosti/kak-upravlyat-riskami-informacionnoi-bezopasnosti (дата обращения 20 апреля 2023).

Процесс анализа рисков в ИБ включает в себя следующие этапы:

1. Идентификация рисков – процесс выявления потенциальных угроз ИБ, которые могут возникнуть в ИС и привести к нежелательным последствиям. Этот шаг включает в себя анализ уязвимостей системы, анализ предшествующих инцидентов и оценку возможных угроз.

2. Оценка рисков – процесс определения вероятности возникновения угроз и их потенциальных последствий для ИС и организации в целом. Оценка рисков проводится с помощью квалифицированных специалистов в области ИБ и используемых ими методик.

3. Разработка мер по управлению рисками – процесс выработки стратегии по управлению рисками, которая включает в себя выбор мер по предотвращению, смягчению или уменьшению возможных негативных последствий угроз. Эти меры могут быть техническими, организационными или комбинированными.

4. Реализация мер по управлению рисками – процесс внедрения выбранных мер в рамках ИС и организации. Может включать в себя установку программного и аппаратного обеспечения, проведение тренингов и обучения персонала, создание политик и процедур и т. д.

5. Мониторинг и управление рисками – процесс постоянного контроля и оценки эффективности принятых мер по управлению рисками, их модификации и обновления в соответствии с изменением ситуации в ИС и организации [Колосок, Гурина 2019].

Важно отметить, что анализ рисков в ИБ является непрерывным процессом и должен проводиться регулярно для обеспечения максимального уровня защиты ИС и организации в целом.

При анализе рисков ИБ рассматривается информационная система в ее исходном состоянии, оцениваются ожидаемые потери от инцидентов за определенный период времени. После всех этих действий проводится оценка, которая показывает влияние мер и систем обеспечения безопасности на снижение рисков, оценка стоимости на затрачиваемые ресурсы. Предпосылки для управления рисками возникли еще в 1950-х гг. Тогда была предложена идея управления рисками Клементса–Хоффмана. Эта идея базируется на предпосылке, что риск является неизбежным элементом любой деятельности и не может быть полностью устранен. Вместо этого риск должен быть управляемым и контролируемым.

Основными предпосылками концепции управления рисками Клементса–Хоффмана являются[2]:

[2] Реализация системы оценки безопасности критически важных и потенциально опасных объектов. URL: https://cyberleninka.ru/article/n/

1. Необходимость управления рисками – риск существует в любой деятельности, и его невозможно полностью исключить. Поэтому необходимо управлять рисками, чтобы минимизировать возможные негативные последствия и обеспечить защиту организации.

2. Идентификация рисков – для управления рисками необходимо определить и оценить возможные угрозы и их потенциальные последствия. Это позволяет разработать эффективные стратегии по управлению рисками.

3. Оценка рисков – оценка рисков позволяет определить вероятность возникновения угроз и их потенциальные последствия. Эта информация необходима для выбора эффективных мер по управлению рисками.

4. Управление рисками – управление рисками предполагает разработку и внедрение мер по уменьшению или предотвращению негативных последствий угроз. Эти меры могут быть техническими, организационными или комбинированными.

5. Непрерывный процесс – управление рисками является непрерывным процессом, который должен проводиться регулярно. Это необходимо для того, чтобы обеспечить максимальный уровень защиты организации и адаптировать меры управления рисками к изменяющейся ситуации [Коротков, Зиновьева 2011].

Идея управления рисками Клементса–Хоффмана является основой для многих современных методик и подходов к управлению рисками, в том числе в сфере информационной безопасности.

Модель управления рисками Клементса–Хоффмана (Clements–Hoffman model) – это процесс управления рисками, который включает в себя несколько этапов и используется для определения, оценки и управления рисками в организации. Модель была окончательно доработана и предложена Л.Дж. Хоффманом в 1970-х годах и стала широко применяться в различных отраслях, включая сферу информационной безопасности.

Основные этапы модели Клементса–Хоффмана включают в себя:

– идентификацию рисков – определение потенциальных угроз и их источников в организации. В этом этапе необходимо проанализировать все аспекты деятельности организации и выявить возможные уязвимости;
– оценку рисков – определение вероятности возникновения угроз и их потенциальных последствий. В этом этапе необхо-

---

realizatsiya-sistemy-otsenki-bezopasnosti-kriticheski-vazhnyh-i-potentsialno-opasnyh-obektov (дата обращения 20 апреля 2023).

димо определить степень влияния каждой угрозы на организацию и вероятность их возникновения;
- разработку стратегии управления рисками – выбор наиболее эффективных методов управления рисками. Это может быть внедрение технических средств защиты, изменение организационных процессов, обучение персонала и т. д.;
- внедрение мер управления рисками – реализацию выбранных стратегий управления рисками. В этом этапе необходимо внедрить меры, которые были выбраны на предыдущем этапе;
- мониторинг и анализ – постоянный мониторинг эффективности мер управления рисками и их анализ. Это необходимо для корректировки выбранных стратегий и мер управления рисками в случае необходимости [Курбатов 2019].

Следует отметить, что данная модель была несколько идеализирована. Ее суть состояла в предположении о необходимости наличия хотя бы одного средства обеспечения безопасности на каждом возможном пути воздействия на защищаемую ИС. В дальнейшем в ней был выявлен ряд недостатков. В частности – необходимость оценки угроз.

В ходе анализа классической модели Клементса–Хоффмана было выявлено, что данная модель носит «утопический» характер. В ней не учитывается стоимость внедряемых средств защиты, а также соотношение этой стоимости к возможным потерям при реализации конкретной угрозы. Учитывая, что у нас всегда существуют не только как материальные, так и временные ограничения при создании системы обеспечения ИБ, построить систему с полным перекрытием не представляется возможным.

Поиск всех возможных воздействий злоумышленника на объект зачастую не может быть выполнен. Поскольку помимо известных способов реализации угроз в будущем могут появиться новые, то и обеспечить защиту системы от всех угроз невозможно. Таким образом, встает вопрос о выборе конкретных угроз, от которых мы будем защищать систему.

Каждый барьер защиты в реальности обеспечивает лишь некоторую степень сопротивляемости угрозам безопасности. Поэтому для обеспечения ИБ требуется построение комплексной системы защиты, направленной на существующие угрозы безопасности, которые ранжируются в зависимости от степени опасности, а также определяются оптимальные меры по их обработке.

Как было показано выше, модель Клементса–Хоффмана не гарантирует защиту от всех актуальных угроз, а следовательно, система защиты и методика управления рисками должны строиться на основе системного подхода.

Современные методики управления рисками в сфере информационной безопасности предполагают решение следующих задач: анализ рисков, оценку уязвимостей, управление угрозами и меры защиты [Резниченко, Сиротский 2021].

Дадим краткий обзор известных методик управления рисками ИБ.

Методика управления рисками ISO 27001. Это стандарт управления рисками информационной безопасности, который определяет требования к системам управления информационной безопасностью (СУИБ). Эта методика основывается на подходе PDCA (Plan-Do-Check-Act) и включает в себя анализ рисков, выбор мер защиты, реализацию и мониторинг СУИБ.

Методика управления рисками NIST. Это стандарт, разработанный Национальным институтом стандартов и технологий США, который определяет требования к управлению рисками в области информационной безопасности. Методика NIST включает в себя 5 этапов: идентификация, защита, обнаружение, реагирование и восстановление.

Существует множество программных продуктов, которые предназначены для управления рисками в сфере информационной безопасности. Они включают в себя:

*RSA Archer*. Это платформа управления рисками и соответствием, которая позволяет организациям управлять рисками, соответствовать нормативным требованиям и принимать решения на основе аналитики.

*IBM QRadar*. Это система управления рисками и безопасностью, которая обеспечивает мониторинг и анализ событий в режиме реального времени, а также позволяет проводить анализ угроз и оценивать риски.

Кроме зарубежных программных продуктов, существуют и русскоязычные решения для управления рисками в сфере информационной безопасности. Укажем некоторые из них:

«*КриптоПРО Risk Manager*». Это решение, которое позволяет оценивать риски и разрабатывать меры по управлению ими. С помощью этого инструмента можно анализировать уязвимости системы, оценивать риски и проводить мониторинг безопасности.

«*Антириск*». Это программное обеспечение для управления рисками, которое позволяет оценивать риски на основе стандартов ISO 27001 и ГОСТ Р ИСО/МЭК 27005. В состав решения входят модули по анализу угроз, оценке рисков, планированию мероприятий и мониторингу выполнения задач.

«*Меридиан-Риск*». Это решение, которое позволяет проводить анализ рисков и разрабатывать планы мероприятий по управлению

ими. С помощью этого инструмента можно оценить уровень риска, выявить уязвимости системы и определить необходимые меры по их устранению.

«*РискМенеджер*». Это решение, которое позволяет проводить анализ рисков и разрабатывать меры по их управлению. В состав решения входят модули по оценке рисков, анализу угроз, мониторингу выполнения задач и созданию отчетов.

«*Информационная безопасность*». Это комплексное решение для управления рисками и обеспечения безопасности информации. В состав решения входят модули по анализу угроз, оценке рисков, планированию мероприятий и мониторингу выполнения задач.

Каждое из предложенных программных решений имеет свои преимущества и недостатки. Предложенный ряд отечественных решений помогает компаниям определить полный анализ рисков как на техническом, так и на организационном уровне.

Эти программные продукты разработаны российскими компаниями, открывают организациям возможности эффективно управлять рисками и обеспечивать безопасность информационных ресурсов в соответствии с национальными стандартами. На практике для выбора наиболее подходящего продукта необходимо провести анализ требований политики корпоративной безопасности и сравнить функциональность различных программных продуктов.

На основе проведенного анализа программных продуктов для управления рисками на техническом уровне лучше всего подходит «КриптоПРО Risk Manager». Программный продукт применяется в различных областях, где важна защита информации и управление рисками. Выделим несколько из них: финансовая сфера (банки и другие финансовые учреждения), государственные учреждения (для защиты госсистем, баз данных), здравоохранение.

В ходе нашего исследования проведен анализ подходов финансирования и планирования бюджета ИБ у российских компаний и компаний из западных стран. Отметим существенные различия в подходах к финансированию и планированию бюджета ИБ. В российских компаниях финансирование ИБ часто осуществляется только в случае реализации угрозы в виде инцидента. Только после этого происходит значительная работа по совершенствованию системы ИБ, устранению недостатков и выделению больших бюджетов. Однако польза и эффективность такого подхода к финансированию ИБ крайне низкие. Важно отметить, что финансирование ИБ обычно осуществляется из отдела ИТ и не может являться оптимальным решением, так как цели и задачи этих отделов различны. Цель ИТ заключается в обеспечении доступности и

эффективности поддержки бизнес-процессов, а ИБ направлена на обеспечение конфиденциальности и целостности и доступности данных. При управлении ИБ следует учитывать риски, связанные с обеспечением данного процесса в бизнесах разного уровня. Например, у развивающегося бизнеса риски могут быть выше и вопросы ИБ должны находиться в приоритете. В этом контексте в сфере ИБ решение вопросов категоризации и классификации информации по степени ее критичности для бизнеса, определение и распределение ответственности в области ИБ, а также обеспечение процессов и техническая архитектура систем ИБ являются первостепенными.

Для решения обозначенных проблем важно понимание и необходимость улучшения существующей системы управления ИБ, а также ее финансирование. Это будет способствовать обеспечению непрерывности всех процессов и предотвращению инцидентов. В то же время зачастую для руководства организаций финансирование системы управления ИБ имеет низкий приоритет. Нередко руководители не видят необходимости в выделении дополнительных ресурсов на обеспечение требований ИБ, поскольку считают, что это не приносит непосредственной выгоды. Как показала практика, это опасное заблуждение, поскольку ущерб от нарушения информационной безопасности может превысить затраты на ее обеспечение в несколько раз[3].

Для решения проблемы финансирования системы управления ИБ нужно повышение осведомленности организаций о необходимости обеспечения ИБ и привлечение соответствующих инвестиций. Кроме того, возможным решением может быть создание государственных программ поддержки, которые бы стимулировали организации к инвестированию в системы управления ИБ.

## *Выводы*

1. Управление рисками в сфере информационной безопасности является актуальной и важной проблемой, которая стоит перед каждой организацией. Недостаток внимания к этой проблеме

[3] *Резниченко С.А., Дмитриева Т.В., Подкосов С.В., Евдокимов О.Г., Семухин С.Д.* Проблемы управления информационной безопасностью в кредитно-банковской системе передачи данных // Московский экономический журнал. 2022. № 2. URL: https://qje.su/ekonomicheskaya-teoriya/moskovskij-ekonomicheskij-zhurnal-2-2022-36/ (дата обращения 20 апреля 2023).

может привести к серьезным последствиям в виде утечек конфиденциальной информации, атак злоумышленников и других угроз информационной безопасности.

2. Для эффективного управления рисками в системе управления ИБ необходимо использовать современные программно-аппаратные решения и методики, которые позволят оценить уровень рисков и принять меры по их снижению.

3. По-прежнему остаются актуальным, вопросы с финансированием системы управления ИБ. Для решения этой проблемы необходимо повышение осведомленности организаций о важности обеспечения информационной безопасности и привлечение соответствующих инвестиций.

4. Информационная безопасность является важным аспектом деятельности любой организации, и вложения в нее должны быть рассмотрены как инвестиции в долгосрочную стабильность и развитие организации. Только эффективное управление рисками в сфере информационной безопасности может повысить уровень защиты от внешних и внутренних угроз и сохранности конфиденциальной информации.

*Литература*

Гришина 2022 – *Гришина Н.В.* Анализ динамики утечки персональных данных в условиях реализации программы «Цифровая экономика Российской Федерации» // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2022. № 4. С. 34–43.

Крючков, Прус, Резниченко 2018 – *Крючков А.В., Прус Ю.В., Резниченко С.А.* Технологические основы национальной информационной безопасности // Информационная безопасность: вчера, сегодня, завтра: Междунар. научно-практ. конф. (Москва, 12 апреля 2018): Сб. статей. М.: РГГУ, 2018. С 58–62.

Колосок, Гурина 2019 – *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.

Коротков, Зиновьева 2011 – *Коротков А.В., Зиновьева Е.С.* Безопасность критических информационных инфраструктур в международном гуманитарном праве // Вестник МГИМО. 2011. Т. 4. С. 154–162.

Курбатов 2019 – *Курбатов Н.М.* О формировании правовых и научных основ обеспечения безопасности критической информационной инфраструктуры Российской Федерации // Вестник Удмуртского ун-та. 2019. Т. 29 (5). С. 644–654.

Наврузов 2022 – *Наврузов Е.Р.* О формировании баз прецедентов для решения задач информационной безопасности // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2022. № 3. С. 66–84. DOI: 10.28995/2686-679X-2022-3-66-84.

Надеждин 2012 – *Надеждин Е.Н.* Проблемные вопросы управления рисками информационной безопасности в сфере образования // Научный поиск. 2012. № 2.6. С. 50–57.

Резниченко, Сиротский 2021 – *Резниченко С.А., Сиротский А.А.* Формализованная модель аудита информационной безопасности организации на предмет соответствия требованиям стандартов // Безопасность информационных технологий. 2021. № 2. С. 98–112.

## *References*

Grishina, N.V. (2022), "Analysis of the dynamics of personal data leakage in the context of the implementation of the program 'Digital Economy of the Russian Federation' ", *RSUH/RGGU Bulletin. "Information Scince. Information Security. Mathematics" Series*, no. 4, pp. 34–43.

Kolosok, I.N. and Gurina, I.N. (2019), "Assessment of cybersecurity risks for the information and communication infrastructure of the intelligent energy system", *Information and mathematical technologies in science and management*, vol. 2 (14), pp. 40–51.

Korotkov, A.V. and Zinov'eva, E.S. (2011), "Security of critical information infrastructures in international humanitarian law", *Bulletin of MGIMO*, vol. 4, pp. 154–162.

Kryuchkov, A.V., Prus, Yu.V. and Reznichenko, S.A. (2018), "Technological foundations of national information security", *Information Security. Yesterday, Today, Tomorrow. Proceedings of the All-Russian Scientific and Practical. Conf. (Moscow, April 12, 2018), Collection of articles*, Moscow, Russia, pp. 58–62.

Kurbatov, N.M. (2019), "On the formation of legal and scientific bases for ensuring the safety of critical information infrastructure of the Russian Federation", *Bulletin of Udmurt University*, vol. 29, no. 5. pp. 644–654.

Nadezhdin, E.N. (2012), "Problematic issues of information security risk management in the field of education", *Scientific Search*, no. 2.6., pp. 50–57.

Navruzov, E.R. (2022), "On forming the precedent bases for solving problems of the information security", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 3, pp. 66–84, DOI: 10.28995/2686-679X-2022-3-66-84.

Reznichenko, S.A. and Sirotskii, A.A. (2021), "A formalized model of an organization's information security audit for compliance with the requirements of standards", *Information Technology Security*, no. 2. pp. 98–112.

*Информация об авторах*

*Игорь Б. Бакин*, студент, Финансовый университет при Правительстве РФ, Москва, Россия; 125993, Россия, Москва, Ленинградский проспект, д. 49; recuptw@gmail.com

*Камилла Ш.* Ниязова, студент, Финансовый университет при Правительстве РФ, Москва, Россия; 125993, Россия, Москва, Ленинградский проспект, д. 49; kamilla.niyazova@gmail.com

*София М. Шведова*, студент, Финансовый университет при Правительстве РФ, Москва, Россия; 125993, Россия, Москва, Ленинградский проспект, д. 49; Shvedova.2003@inbox.ru

*Information about the authors*

*Igor B. Bakin*, student, Financial University under the Government of the Russian Federation, Moscow, Russia; bld. 49, Leningradskii Av., Moscow, 125993, Russia; recuptw@gmail.com

*Camilla Sh. Niyazova*, student, Financial University under the Government of the Russian Federation, Moscow, Russia; bld. 49, Leningradskii Av., Moscow, 125993, Russia; kamilla.niyazova@gmail.com

*Sofia M. Shvedova*, student, Financial University under the Government of the Russian Federation, Moscow, Russia; bld. 49, Leningradskii Av., Moscow, 125993, Russia; Shvedova.2003@inbox.ru

УДК 004.021
DOI: 10.28995/2686-679X-2023-3-61-70

# Сравнительный анализ языков программирования на основе решения тестовой задачи сортировки данных

Владислав Д. Волков
*Российский государственный гуманитарный университет, Москва, Россия, volkov99vlad@gmail.com*

Анна Б. Клименко
*Российский государственный гуманитарный университет, Москва, Россия, anna_klimenko@mail.ru*

*Аннотация*. Целью данного исследования является сравнение эффективности популярных языков программирования на примере временных характеристик алгоритмов сортировки. Алгоритмы сортировки выбраны в связи с высокой частотой использования их как вспомогательных алгоритмов при решении различных задач, например при реализации бинарного поиска.

Поскольку алгоритмы сортировок являются трудозатратными, скорость их реализации, в свою очередь, критична для оценивания эффективности многих проектов, а также при оценивании выбора того или иного языка программирования.

В данной статье было проведено сравнение временных характеристик реализации распространенных алгоритмов сортировок на различных языках программирования высокого уровня.

Результаты экспериментального исследования позволяют сделать выводы о целесообразности использования тех или иных языков программирования в задачах реализации сортировок в зависимости от имеющихся временных ограничений. Время работы сортировок на большинстве языков программирования сильно зависит от способа решения задачи, и в разных языках могут оказаться более эффективными разные способы, а некоторые, весьма эффективные на первый взгляд решения могут привести к неожиданному замедлению программы. В то же время языки программирования Lisp и Lua качественно оптимизируют код и позволяют добиваться максимальной скорости.

*Ключевые слова*: алгоритмы, сортировка, языки программирования, быстродействие

*Для цитирования*: *Волков В.Д., Клименко А.Б.* Сравнительный анализ языков программирования на основе решения тестовой задачи сортировки данных // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2023. № 3. С. 61–70. DOI: 10.28995/2686-679X-2023-3-61-70

# The comparative analysis of the programming languages based on the test data sorting task

Vladislav D. Volkov
*Russian State University for the Humanities, Moscow, Russia, volkov99vlad@gmail.com*

Anna B. Klimenko
*Russian State University for the Humanities, Moscow, Russia, anna_klimenko@mail.ru*

*Abstract*. The purpose of the study is to compare the efficiency of popular programming languages using the time characteristics of sorting algorithms as an example. Sorting algorithms were chosen due to the high frequency of their use as auxiliary algorithms in solving various problems, for example, in the implementation of binary search.

Since sorting algorithms are labor-intensive, the speed of their implementation, in turn, is critical for evaluating the effectiveness of many projects, as well as when evaluating the choice of one or another programming language.

The present article is a comparison in the time characteristics of the implementation of common sorting algorithms in various high-level programming languages.

The results of the experimental study allow drawing conclusions about the expediency of using certain programming languages in the problems of sorting implementation, depending on the existing time constraints. The running time of sorts in most programming languages is highly dependent on the way the problem is solved, and different ways may be more efficient in different languages, and some solutions that seem very effective at first glance can lead to an unexpected slowdown of the program. At the same time, the Lisp and Lua programming languages optimize the code qualitatively and allow achieving the maximum speed.

*Keywords*: algorithms, sorting, programming languages, performance

*For citation*: Volkov, V.D. and Klimenko, A.B. (2023), "The comparative analysis of the programming languages based on the test data sorting task", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no.. 3, pp. 61–70, DOI: 10.28995/2686-679X-2023-3-61-70

## *Введение*

В современном мире требуется обрабатывать значительные объемы данных, и, как следствие, существует необходимость в алгоритмах с низкой (желательно линейной) вычислительной сложностью. На предварительно отсортированных данных можно использовать алгоритмы с меньшей вычислительной сложностью. Также следует учесть, что есть множество алгоритмов, которые работают только на отсортированных данных. Кроме того, отсортированные данные приобретают свойства монотонности, что может быть полезным в процессе обработки.

При разработке программного обеспечения также важно учитывать, что предварительная сортировка имеет смысл, если данные будут подвергаться многократной обработке или если сложность алгоритма на неотсортированных данных велика (больше суммы сложностей алгоритма на отсортированных и сортировки).

Отметим некоторые алгоритмы, для которых желательно получать предварительно отсортированные входные данные:

- бинарный поиск работает лишь на отсортированных данных [Седжвик 2003];
- все алгоритмы сложения большого объема дробных чисел разных порядков с высокой точностью (например, алгоритм Кэхэна). Обычно их качество существенно возрастает на отсортированных данных [Muller et al. 2018];
- квантильная функция в статистике сортирует данные[1];
- функция распределения случайной величины в большинстве реализаций содержит сортировку[2].

Учитывая сказанное выше, реализация алгоритмов сортировок актуальна для последующей реализации достаточно широкого круга задач. При этом важен выбор языка программирования, частная реализация которого позволяла бы произвести сортировку наиболее быстрым способом. Такая информация практически отсутствует, однако, являясь важной. Следовательно, актуальными становятся экспериментальные исследования временных характеристик алгоритмов сортировок, реализованных на различных языках программирования высокого уровня, что и сделано в данной статье.

Целью данной статьи является экспериментальное исследование и сравнение скоростей сортировки, которые обеспечивают

---

[1] *Ihaka R., Gentleman R.* R: A language for data analysis and graphics, 1996. URL: https://www.stat.auckland.ac.nz/~ihaka/downloads/R-paper.pdf (дата обращения 3 января 2023).

[2] Op. cit.

отобранные языки программирования в рамках реализаций также отобранных алгоритмов.

В результате анализа предметной области были отобраны следующие исследования, близкие по смыслу [Durrani, Hayan 2023][3], [Syed Muqeet Aqib et al. 2021]. Представленное в данной статье исследование ориентировано на более широкий охват анализируемых языков, что делает его более информативным по сравнению с аналогичными. Следует отметить, что результаты экспериментов по взятым идентичным языкам совпадают, что позволяет говорить о корректности проведенных нами экспериментов. Кроме того, данная статья содержит результаты в том числе для наихудших случаев сортируемых данных, что не представлено в близких по смыслу и тематике статьях.

### *Рассматриваемые алгоритмы сортировок и описание методики измерений*

Каждая сортировка характеризуется несколькими параметрами, которые отражают эффективность ее работы [Седжвик 2003]:

- сложностью в лучшем случае (в большинстве сортировок это будет упорядоченное множество);
- сложностью в большинстве случаев (в рамках работы использовалась последовательность $a_i : \sin(i)$);
- сложностью в худшем случае (в большинстве тестов будет упорядоченное в обратную сторону множество);
- потреблением памяти.

Обычно худшие в смысле вычислительной сложности сортировки показывают лучшее время на малых объемах данных. Поэтому в современных сортировках часто используются смеси базовых алгоритмов; например, timsort является производной сортировок пузырьком и слиянием[4]. Но измерения на малых объемах данных являются затруднительными в связи с тем, что дублирующийся код может убраться или оптимизироваться в результате работы компи-

[3] *McMillan M.* Comparing Programming language efficiency in 4 programming languages. URL: https://levelup.gitconnected.com/comparing-programming-language-efficiency-in-4-programming-languages-timing-selection-sort-29badc8a744f (дата обращения 3 января 2023).

[4] *Auger N., Nicaud C., Pivoteau C.* Merge Strategies: from Merge Sort to TimSort, 2015. URL: https://www.researchgate.net/publication/282679394_Merge_Strategies_from_Merge_Sort_to_TimSort (дата обращения 3 января 2023).

лятора/интерпретатора; в то же время повторные запуски одной и той же программы влекут временные затраты на запуск (в частности, интерпретатора, виртуальной машины или переработка кода в байт-код), что делает не очень эффективным использование тестов при небольшой длине сортируемой последовательности. В связи с этим фактором все тестирования проводились на массивах данных размером в 10 000 элементов по 10 запусков (чтобы снизить влияние случайных компонент), результаты приведены в таблице, как время 10 обработок 10 000 элементов.

В данной работе рассмотрены и исследованы временные характеристики следующих алгоритмов сортировок [Седжвик 2003]:

– сортировка пузырьком (рекурсия раскрыта в цикл);
– сортировка вставкой;
– сортировка выбором;
– сортировка расческой;
– сортировка слиянием;
– сортировка быстрая (для лучшего и среднего выбиралась полусумма первого и последнего элементов, а для худшего – первый элемент);
– сортировка коктейльная.

В данной работе проводились замеры результатов работы следующих реализаций языков программирования; данные реализации были выбраны как самые популярные:

- R – одноименный интерпретатор;
- Common Lisp: интерпретатор sbcl (запускался с отключенной отладочной информацией и требованием к максимальной скорости);
- Lua – одноименный интерпретатор;
- Perl – одноименный интерпретатор;
- Python – одноименный интерпретатор для Python3;
- Ruby – одноименный интерпретатор.

### *Особенность проведения оценок и измерений*

Временные характеристики языка зависят от используемого интерпретатора/компилятора, и влияние самого языка и его семантики на результат измерения может стать пренебрежимо мало. Поэтому правильнее говорить скорее о производительности популярных реализаций языков программирования.

Малое влияние собственно языка типично в основном для компилируемых языков, где посредством сложных и длительных

оптимизаций компилятор может самостоятельно избавиться от неэффективных операций, даже если они являются частью синтаксиса.

Для интерпретируемых языков следует иметь в виду, что они используют генерацию байт-кода или даже JIT-компиляцию (которая генерирует машинный код или смесь байт-кода и ассемблера). И как следствие здесь стоит отметить, что языки, активно использующие JIT-компиляцию (например, Julia), по свойствам ближе к компилируемым: очень быстрая скорость выполнения и долгая компиляция. Так что использование тестов на скорость для таких языков (а точнее, интерпретаторов) затруднительно, так как при большом количестве вызовов быстрых программ их производительность в сотни раз меньше других языков; но при вызове времязатратных программ они обгоняют даже некоторые компиляторы.

Для интерпретируемых языков также может проявляться некая нестабильность, вызванная неполной обработкой кода, и как следствие разными стратегиями оптимизации (например, у R реализована медленная/неэффективная работа с рекурсией).

Результаты замеров скорости зависят от наличия трудозатратных фоновых процессов в системе на момент исследования. Система с запущенным браузером и виртуальной машиной будет обрабатывать программу медленнее, чем система, выполняющая лишь замеры скоростей программы. Так что важно проводить замеры в одинаковом состоянии системы и желательно в одно и то же время (в данной работе для каждой сортировки и входных данных тестировалась сразу вся группа языков).

Также следует учитывать, что человеку трудно уследить за всеми необходимыми тестами, и, как следствие, возникает необходимость в автоматизации замеров, желательно на уровне каждого языка или хотя в наборе системных скриптов, ускоряющих и контролирующих замеры.

Поэтому, учитывая все сказанное выше, при проведении эксперимента необходимо:

– грамотное разделение языков программирования на группы по признакам интерпретируемости/компилируемости;
– наличие системного скрипта для замера временных характеристик;
– обеспечение идентичных условий для всех экспериментов;
– достаточный объем выборки исходных данных для сортировки.

*Результаты эксперимента*

Для интерпретируемых языков скорости выполнения существенно зависят от реализации алгоритма, и на практике в большинстве случаев однозначно сказать, что один язык быстрее другого во всех тестах, нельзя. Тем не менее те языки, которые производят оптимизацию в большей степени исходного кода, при запуске показывают лучшие результаты, и достаточно стабильно.

*Таблица 1*

Тестирование на последовательности,
сгенерированной в соответствии с функцией sin(x),
в секундах

| | R | Lisp | Lua | Perl | Python | Ruby |
|---|---|---|---|---|---|---|
| пузырьком | 102.32 | 1.20 | 29.63 | 196.96 | 330.83 | 100.11 |
| вставкой | 50.83 | 0.58 | 19.04 | 48.57 | 91.73 | 17.80 |
| выбором | 29.79 | 1.48 | 12.59 | 49.976 | 113.57 | 41.84 |
| расческой | 2.01 | 0.33 | 0.14 | 0.67 | 1.92 | 0.81 |
| слиянием | 7.21 | 0.28 | 0.13 | 0.71 | 2.48 | 0.80 |
| быстрая | 4.12 | 0.27 | 0.08 | 0.39 | 1.63 | 0.73 |
| коктейльная | 70.54 | 0.83 | 14.45 | 126.25 | 171.83 | 74.08 |

При замерах (табл. 1) лучшие результаты у Common Lisp и Lua. Хорошие у Ruby и чуть похуже у Perl. R хорошо показывает себя на многих тестах, но, судя по замерам, имеет проблемы при работе с рекурсиями.

При замерах на отсортированной последовательности (табл. 2) (являющейся лучшим случаем для сортировок) лучшие результаты у Common Lisp, Lua, Perl. Хорошие у Ruby и чуть хуже у Python (хотя у Python худшие результаты сортировки выбором, которая, стоит отметить, не имеет лучшего случая). R показывает наихудшие результаты при работе с рекурсиями.

*Таблица 2*

Тестирование на предварительно отсортированной последовательности, в секундах

| | R | Lisp | Lua | Perl | Python | Ruby |
|---|---|---|---|---|---|---|
| пузырьком | 1.72 | 0.25 | 0.02 | 0.05 | 1.38 | 1.23 |
| вставкой | 1.65 | 0.24 | 0.02 | 0.05 | 1.01 | 1.11 |
| выбором | 37.70 | 1.65 | 12.34 | 50.35 | 106.31 | 38.32 |
| расческой | 2.26 | 0.36 | 0.12 | 0.60 | 1.97 | 1.50 |
| слиянием | 6.51 | 0.32 | 0.08 | 0.44 | 1.80 | 1.38 |
| быстрая | 2.49 | 0.25 | 0.04 | 0.02 | 1.40 | 0.53 |
| коктейльная | 2.32 | 0.28 | 0.03 | 0.05 | 1.21 | 0.58 |

*Таблица 3*

Тестирование на убывающей последовательности (худший случай)

| | R | Lisp | Lua | Perl | Python | Ruby |
|---|---|---|---|---|---|---|
| пузырьком | 160.54 | 1.60 | 35.18 | 255.60 | 311.33 | 110.93 |
| вставкой | 93.11 | 1.03 | 38.74 | 94.37 | 93.38 | 32.42 |
| выбором | 31.67 | 1.65 | 13.80 | 53.39 | 108.64 | 38.52 |
| расческой | 1.88 | 0.32 | 0.11 | 0.51 | 1.86 | 1.29 |
| слиянием | 7.63 | 0.26 | 0.10 | 0.53 | 1.78 | 2.40 |
| быстрая | overflow | 0.58 | 8.03 | 30.23 | overflow | overflow |
| коктейльная | 133.95 | 1.10 | 22.23 | 217.16 | 178.56 | 82.79 |

При замерах на убывающей последовательности (табл. 3) (являющейся худшим случаем для сортировок) лучшие результаты у Common Lisp, Lua. У Ruby хорошие показатели, но, что примечательно, не во всех тестах (сортировка слиянием худшая после R). У R проблемы с рекурсиями, но в остальном результаты неплохие. У Perl и Python по результатам эксперимента худшие результаты.

Также здесь стоит отметить, что у R, Python, Ruby произошло переполнение стека рекурсивных вызовов для быстрой сортировки, что говорит о неэффективности ее применения на них в связи с малой надежностью.

## *Выводы*

Целью данного исследования являлось экспериментальное сравнение временных характеристик выбранных алгоритмов сортировки, реализованных на разных языках программирования. Задача актуальна во многих областях и связана с необходимостью работы с заранее отсортированными данными, что актуализирует тему исследования.

Лучшие результаты показали языки с развитой системой оптимизации кода: Common Lisp и Lua. Языки с менее развитыми системами оптимизации имеют худшие временные характеристики и более нестабильны: в различных задачах они могут показывать результаты как выше, так и ниже конкурентов; возможны прерывания программы из-за превышения программного стека. Также отметим, что у языка программирования R относительно неэффективно реализована работа с рекурсивными вызовами, следовательно, его не следует применять для реализации тех сортировок, для которых рекурсия характерна (например, для быстрой сортировки).

## *Литература*

Седжвик 2003 – *Седжвик Р.* Фундаментальные алгоритмы на C. СПб.: ДиаСофтЮП, 2003. С. 672.

Durrani, Hayan 2023 – *Durrani O.K., Hayan S.A.* Asymptotic performances of popular programming languages for popular sorting algorithms // Bandaoti Guangdian/ Semiconductor Optoelectronics. 2023. Vol. 42 (1). P. 149–169.

Muller et al. 2018 – *Muller J.M., Brunie N., Dinechin F., Jeannerod C.P., Joldes M., Lefèvre V., Melquiond G., Revol N., Torres S.* Handbook of Floating-Point Arithmetic. Basel: Birkhäuser, 2018. P. 179.

Syed Muqeet Aqib et al. 2021 – *Syed Muqeet Aqib et al.* Analysis of Merge Sort and Bubble Sort in Python, PHP, JavaScript, and C language // International Journal of Advanced Trends in Computer Science and Engineering. 2021. Vol. 10 (2). P. 680–686.

## *References*

Durrani, O. and Hayan, S. (2023), "*Asymptotic performances of popular programming languages for popular sorting algorithms*", Bandaoti Guangdian, Semiconductor Optoelectronics, vol. 42 (1), pp. 149–169.

Muller, J., Brunie, N., Dinechin, F., Jeannerod, C., Joldes, M., Lefèvre, V., Melquiond, G., Revol, N. and Torres, S. (2018), *Handbook of Floating-Point Arithmetic,* Birkhäuser, Basel, Switzerland, p. 179.

Sedgewick, R. (2003), *Basic algorithms in C*. DiaSoftYuP, St. Petersburg, Russia, p. 672.

Syed Muqeet Aqib et al. (2021), "Analysis of Merge Sort and Bubble Sort in Python, PHP, JavaScript, and C language", *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 10 (2), pp. 680–686.

## *Информация об авторах*

*Владислав Д. Волков*, студент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; volkov99vlad@gmail.com

*Анна Б. Клименко*, кандидат технических наук, доцент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; anna_klimenko@mail.ru

## *Information about the author*

*Vladislav D. Volkov*, student, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, Russia, 125047; volkov99vlad@gmail.com

*Anna B. Klimenko*, Cand. of Sci. (Engineering), associate professor, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, Russia, 125047; anna_klimenko@mail.ru

УДК 004
DOI: 10.28995/2686-679X-2023-3-71-83

# Экспериментальное исследование эффективности температурных схем имитации отжига в задаче распределения нагрузки

Эльвира М. Алиева
*Российский государственный гуманитарный университет, Москва, Россия, marun4ka@gmail.com*

Андрей Е. Сальников
*Российский государственный гуманитарный университет, Москва, Россия, andrejs03_21@mail.ru*

Анна Б. Клименко
*Российский государственный гуманитарный университет, Москва, Россия, anna_klimenko@mail.ru*

*Аннотация*. В настоящее время задача распределения нагрузки в распределенных вычислительных средах решается практически повсеместно. Это связано с распространением таких концепций построения вычислительных систем, как облачные, туманные и краевые вычисления. Последние предполагают относительно частое перераспределение нагрузки между вычислительными узлами по причине высокой динамики данных слоев сети. Это актуализирует вопрос о периодическом перераспределении вычислительных задач в относительно сжатые сроки, поскольку многие приложения работают в режиме реального времени (например, приложения дополненной реальности). Поскольку задача распределения задач по параллельным независимым машинам относится к классу np, в настоящее время получили широкое распространение эвристические, метаэвристические и nature-inspired алгоритмы. Однако существует весьма малое количество данных об эффективности метаэвристик применительно к решению задачи распределения работ по машинам, что особенно актуально в условиях дефицита времени.

В работе проведено экспериментальное исследование алгоритмов со следующими законами понижения температуры: Больцмановское, Коши, экспоненциальное, мультипликативное. Полученные результаты позволяют сделать выводы о целесообразности применения того или иного закона понижения температуры в заданных условиях. Также получены оценочные значения количеств итераций, достаточных для останова рабо-

ты алгоритма, что позитивно сказывается на времени получения решения задачи распределения работ по машинам.

*Ключевые слова:* метод имитации отжига, оптимизация, глобальный минимум, методы понижения температуры, распределение вычислительной нагрузки, параллельно независимые машины

*Для цитирования: Алиева Э.М., Сальников А.Е., Клименко А.Б.* Экспериментальное исследование эффективности температурных схем имитации отжига в задаче распределения нагрузки // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика» 2023. № 3. С. 71–83. DOI: 10.28995/2686-679X-2023-3-71-83

# Experimental research of the efficiency of temperature schemes for simulating annealing in the problem of load distribution

Elvira M. Alieva
*Russian State University for the Humanities, Moscow, Russia, marun4ka@gmail.com*

Andrei E. Sal'nikov
*Russian State University for the Humanities, Moscow, Russia, andrejs03_21@mail.ru*

Anna B. Klimenko
*Russian State University for the Humanities, Moscow, Russia, anna_klimenko@mail.ru*

*Abstract.* Currently, the problem of load distribution in distributed computing environments is solved almost everywhere. That is due to the spread of such concepts of building computing systems as cloud, fog and edge computing. The latter assume a relatively frequent redistribution of the load between computing nodes due to the high dynamics of these network layers. That actualizes the issue of periodic redistribution of computing tasks in a relatively short time, since many applications work in real time (for example, augmented reality applications). Since the problem of distributing tasks among parallel independent machines belongs to the np class, heuristic, metaheuristic, and nature-inspired algorithms are now widely used. However, there is a very small amount of data on the effectiveness of metaheuristics in relation to solving the problem of distributing work among machines, which is especially important in conditions of time pressure.

In the work, an experimental study of algorithms with the following laws of temperature decrease was carried out: Boltzmann, Cauchy, exponential, multi-

plicative. The results obtained lead to conclusions about the expediency of applying one or another law of temperature decrease under given conditions. We also got estimates for the number of iterations sufficient to stop the algorithm, which has a positive effect on the time to obtain a solution to the problem of distributing work among machines.

*Keywords:* simulated annealing method, optimization, global minimum, temperature reduction methods, distribution of computing load, parallel independent machines

*For citation:* Alieva, E.M., Sal'nikov, A.E. and Klimenko, A.B. (2023), "Experimental research of the efficiency of temperature schemes for simulating annealing in the problem of load distribution", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 3, pp. 71–83, DOI: 10.28995/2686-679X-2023-3-71-83

## *Введение*

В настоящее время все большее количество информационных систем, в том числе реального времени, строится на базе таких концепций, как краевые и туманные вычисления: [Jumani, Shi, Laghari, Hu, Nabi, Qian 2023; Karampudi et al. 2023; Almahlawi, Mikki 2023].

Особенностью последних является то, что топология сети обретает динамику, в результате чего однократное распределение вычислений по вычислительным устройствам становится недостаточным. То же справедливо и для систем, работающих на основе облачных вычислений, поскольку горизонтальное масштабирование предполагает возможность перемещения задач по вычислительным узлам.

В связи с этим достаточно большой круг работ посвящен вопросам распределения и перераспределения ресурсов в слоях сети с высокой динамикой, например: децентрализованное управление распределенной системой при выполнении потока заданий [Каляев, Мельник 2011], умные города будущего[1]. Кроме того, для многих систем поднимается вопрос о том, что перераспределение нагрузки на узлы должно быть произведено наиболее быстрым и наименее трудозатратным способом: [Клименко 2022; Melnik, Klimenko, Korobkin 2020; Melnik, Klimenko 2020].

[1] *Смирнов А., Голохваст К., Тумялис А.* Развитие «Интернета вещей», дополненной реальности и коммуникационных технологий. URL: https://arxiv.org/ftp/arxiv/papers/1902/1902.08008.pdf (дата обращения 24 апреля 2023).

Среди современных работ, посвященных этой тематике, отмечают следующие: планирование задач IoT с учетом сроков и энергоэффективности в туманных вычислениях системы [Azizi, Shojafar, Abawajy, Buyya 2022], эффективный подход к многоцелевому планированию задач на основе популяции в системах туманных вычислений [Movahedi, Defude, Hosseininia 2021].

Отметим, что для решения задач распределения нагрузки актуальны метаэвристики, такие как имитация отжига, генетические алгоритмы и др., по причине того, что позволяют получить допустимое по качеству решение за приемлемое время.

В результате анализа работ, посвященных исследованию распределения вычислительной нагрузки, в работе [Klimenko, Klimenko, Melnik 2015] произведено сравнение имитации отжига и одной из реализаций генетического алгоритма, а в качестве целевой функции при оптимизации распределения задач взято выравнивание нагрузки процессоров.

Цель данной работы – сравнительный анализ алгоритмов семейства имитации отжига в аспекте временных затрат на получение приемлемого по качеству решения.

В данной работе проводится экспериментальное исследование итерационного метода «имитация отжига» на предмет перспективности его использования в задачах распределения нагрузки в рамках динамической распределенной вычислительной системы. На основе проведенных экспериментов могут быть сформированы рекомендации по применению того или иного закона изменения температуры.

## *Задача распределения вычислительной нагрузки в гетерогенной вычислительной среде*

Пусть имеется множество задач $X = \{x_i\}$, где i – номер задачи, $i > 0$, $x_i$ – трудоемкость i-той задачи. Пусть также имеется множество машин $M = \{m_j\}$, где j – номер машины, $j > 0$, $m_j$ – производительность j-той машины.

Тогда $t_{ij}$ – время завершения j-той машиной i-й задачи, которая была распределена на нее.

При этом временем выполнения комплекса работ будет $MAX(t_{ij})$.

Для каждого варианта распределения найдется то устройство, выполнение работ которым будет самым длительным по времени.

Необходимо распределить задачи по машинам таким образом, чтобы минимизировать время выполнения комплекса задач, т. е. целевой функцией является $F = MAX(t_{ij}) \rightarrow \min$, где $i > 0, j > 0$.

Пусть I – номер задачи, распределенной на машину j; $x_I/m_j$ – время, затраченное на выполнение задачи I машиной j. Тогда $\forall$ I, j будут выполняться следующие условия: $t_{I-1,j} < t_{Ij} - x_I/m_j$ и $t_{Ij} < t_{I+1,j} - x_{I+1}/m_j$.

Формализованная таким образом задача является:

1. Задачей теории расписаний: осуществляется построение допустимого расписания, при котором все ограничения соблюдены (по одной работе на машину, и каждая последующая работа, прикрепленная к той же машине, что и предыдущая, не может быть начата раньше, чем закончится предшествующая работа), и нахождение оптимального допустимого расписания производится по определенному критерию оптимальности, а именно – времени завершения комплекса работ.

2. Задачей комбинаторной оптимизации, поскольку речь идет о получении экстремума функции, заданной на конечном множестве вариантов исходных данных, что формирует поисковое пространство.

3. Задачей нелинейной оптимизации, так как целевая функция (минимакс) не является линейной.

В силу того что множество различных распределений работ по машинам конечно, можно перебрать все допустимые варианты решения. Но в реальных задачах количество возможных вариантов может быть настолько велико, что сравнение всех вариантов значения функции сложно осуществить за приемлемое время, которое было бы актуально для реконфигурации вычислительной системы.

В связи с этим применяются различные алгоритмы, позволяющие получить приемлемое по качеству решение за ограниченное время. К таким алгоритмам относят известные метаэвристические методы, которые обладают двумя важными особенностями: в результате их работы последовательно строятся несколько решений, построение каждого нового решения основывается на предыдущих полученных решениях[2].

Среди метаэвристик выделяют два наиболее широких класса методов – это итерационные и эволюционные. К примерам итерационных относят, как правило, метод имитации отжига и поиск

[2] *Лазарев А.А., Гафаров Е.Р.* Теория расписаний. Задачи и алгоритмы. URL: https://www.ipu.ru/sites/default/files/publications/12896/406-12896.pdf (дата обращения 20 апреля 2023).

с запретами (tabu search)[3,4]: [Ingber, Petraglia, Petraglia, Soares Machado 2012].

Среди эволюционных методов наиболее распространенными являются генетические алгоритмы [Awange, Palancz, Lewis, Volgyesi 2023].

Следует отметить, что генетические алгоритмы, несмотря на признанную эффективность, обладают высокими требованиями к памяти, а также могут занимать достаточно долгое время при обработке больших популяций. Учитывая, что для приложений реального времени время обработки является критичным, использование метода имитации отжига видится более перспективным, особенно в случае ограничений на вычислительные ресурсы.

### *Метод имитации отжига*

Алгоритм основывается на имитации физического процесса, который происходит при кристаллизации вещества, например металлов. Для данного процесса характерны переходы отдельных атомов из одной ячейки кристаллической решетки в другую, причем вероятность перехода с понижением температуры уменьшается.

Эта метаэвристика является рандомизированным методом локального поиска, позволяющим избежать «плохих» локальных оптимумов. Метод имитации отжига – это стохастический метод поиска, в котором на каждом шаге текущее решение заменяется другим, случайно выбранным из окрестности и улучшающим значение целевой функции решением[5].

Алгоритм имитации отжига состоит в следующем.

Пусть $S = \{S_k\}$ – множество всех состояний, k – количество итераций поиска решения (длительность отжига), T – функция

---

[3] *Atiya A., Parlos A., Ingber L.* A Reinforcement Learning Method Based on Adaptive Simulated Annealing, 2004. URL: https://www.ingber.com/asa03_reinforce.pdf (дата обращения 26 апреля 2023).

[4] *Sakabe M., Yagiura M.* An efficient tabu search algorithm for the linear ordering problem, 2022. URL: https://www.jstage.jst.go.jp/article/jamdsm/16/4/16_2022jamdsm0041/_pdf/-char/en (дата обращения 24 апреля 2023).

[5] *Щербина О.А.* Метаэвристические алгоритмы для задач комбинаторной оптимизации (обзор). URL: https://cyberleninka.ru/article/n/metaevristicheskie-algoritmy-dlya-zadach-kombinatornoy-optimizatsii-obzor/viewer (дата обращения 24 апреля 2023).

изменения температуры с течением времени, $T_{max}$ и $T_{min}$ – максимальная и минимальная температуры отжига соответственно.

1. Определяются $S_0$ (начальное размещение) и $T_0 = T_{max}$ (начальная температура). Они могут быть получены случайным образом.
2. Пока $T_k > T_{min}$:
   – генерируется новое состояние $S_k$;
   – вычисляется параметр изменения энергии $\Delta E = S_c - S_k$, равный разности предыдущего подходящего состояния и нового. В зависимости от полученного значения осуществляется переход. При $\Delta E \leqslant 0$ $S_c = S_k$ (система переходит в новую точку, так как вероятность перехода равна 1). При $\Delta E > 0$ вычисляется вероятность перехода в новое состояние;
   – понижается текущая температура с учетом какого-либо закона изменения температуры.
3. Последнее подходящее состояние является искомым.

Существуют различные законы изменения температуры. Рассмотрим следующие:

1. Отжиг Больцмана. Изменение температуры задается в виде:

$$T(k) = T_0/\ln(1 + k),\ k > 0.$$

2. Отжиг Коши происходит по формуле

$$T(k) = T_0/ k,\ k > 0.$$

3. Экспоненциальное мультипликативное охлаждение:

$$T(k) = T_0 * a^k,$$ где а принадлежит промежутку [0.8; 0.9].

## *Экспериментальное исследование*

Для всех экспериментов будем брать производительность $m_j$ каждой машины от 1 до 100 и трудоемкость $x_i$ каждой задачи от 1 до 100; параметр $a = 0.89$, $T_{min} = 0.25$.

Эксперимент 1.

Для начала возьмем 10 задач и будем распределять их по 5 машинам. За начальную температуру примем $T_0 = 100$. Применим различные способы понижения температуры и сделаем срез полученных значений целевой функции на 100 итерациях (рис. 1) и на 1000 итерациях (рис. 2).

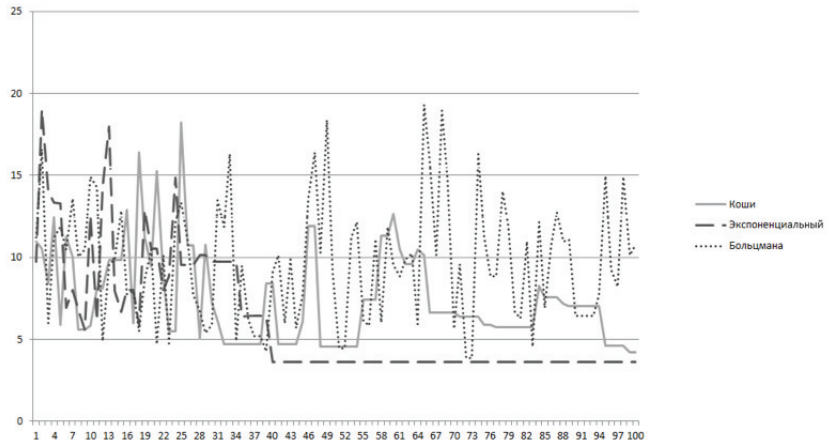


*Рис. 1.* Графики для 10 задач, 5 машин, $T_0=100^0$, 100 итераций

Как мы видим, экспоненциальный метод быстрее остальных «остыл» до наиболее стабильного состояния (начиная с 40-й итерации).

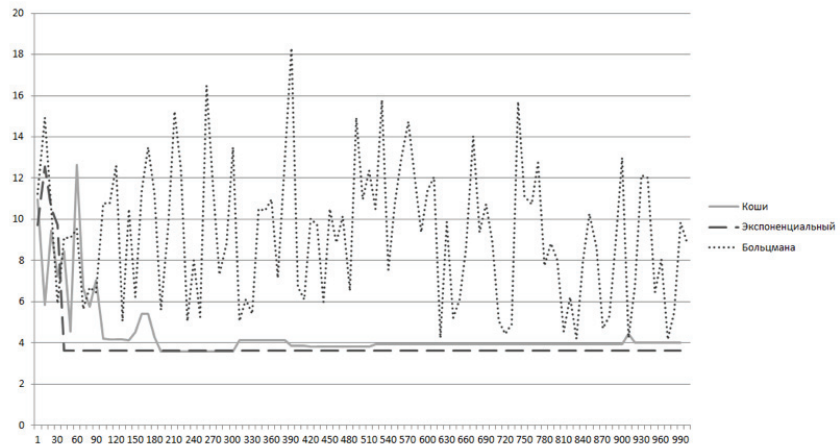


*Рис. 2.* Графики для 10 задач, 5 машин, $T_0=100^0$, 1000 итераций

Можно заметить, что для 1000 итераций для метода Коши сильные скачки температуры прекратились примерно со 190-й итерации. Для перехода в равномерное изменение температуры методу Больцмана не хватило даже 1000 итераций.

Эксперимент 2.

Проведем тот же эксперимент для большого объема работ. Возьмем 150 задач и будем распределять их по 20 машинам. За начальную температуру примем $T_0 = 100$. Применим различные способы понижения температуры и сделаем срез полученных значений целевой функции на 100 итерациях (рис. 3) и на 1000 итерациях (рис. 4).

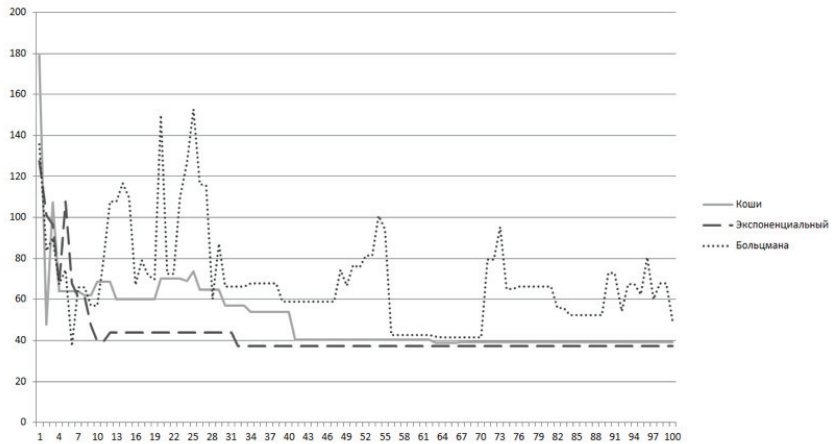


*Рис. 3*. Графики для 150 задач, 20 машин, $T_0=100^0$, 100 итераций

Очевидно, что экспоненциальный метод приводит целевую функцию к довольно стабильному состоянию уже с 32-й итерации, а метод Коши – с 41-й.

При большом объеме работ значения температуры для метода Больцмана не приходят к стабильности. Можно заметить, что метод Коши по истечении 1000 итераций оказался ближе к минимальному значению, т. е. оказался точнее.

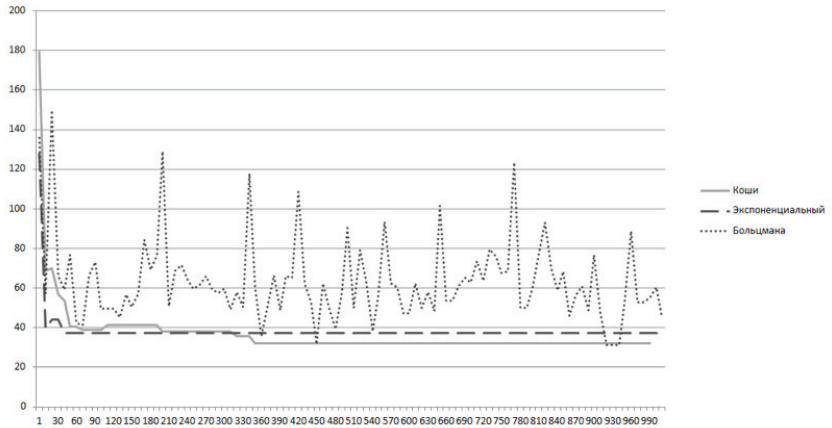


*Рис. 4*. Графики для 150 задач, 20 машин, $T_0=100^0$, 1000 итераций

## *Заключение*

Алгоритм имитации отжига – универсальная метаэвристика, которая применяется при решении сложных задач в самых различных предметных областях: робототехнике (например, решение TSP), в задачах распределения нагрузки для широкого класса технических задач, в прикладных задачах, включая транспорт, медицину и т. д. Его преимуществом является то, что он может избегать локальных минимумов функции путем выбора новых значений, временно ухудшающих получаемый результат. В настоящее время существует несколько различных законов, по которым происходит снижение температуры. Но далеко не все из них являются эффективными для систем, работающих в условиях дефицита времени. Проведенные эксперименты позволяют сделать вывод о том, что экспоненциальное мультипликативное охлаждение обладает наибольшей скоростью снижения температуры, в большинстве экспериментов он оказался точнее метода Коши примерно на 10,9%, в сравнении с законом Больцмана лучше на 99,4%, кроме того, для данного закона целесообразно будет брать не более 500 итераций. Метод Коши также обладает довольно большой скоростью остывания и достаточно хорошей точностью при небольшом количестве итераций, он оказался лучше закона Больцмана на 85,8% и только при больших объемах работ и 1000 итерациях он достиг более точного значения, чем экспоненциальный метод, с разницей в 15,1%. Метод Больцмана «остывает» гораздо медленнее, чем дру-

гие, в связи с этим для него требуется большое количество итераций для получения приемлемых результатов.

## *Литература*


Каляев, Мельник 2011 – *Каляев И.А., Мельник Э.В.* Децентрализованные системы компьютерного управления. Ростов н/Д.: ЮНЦ РАН, 2011. 196 с.

Клименко 2022 – *Клименко А.* Базовые элементы методологии снижения расхода остаточного ресурса вычислительных устройств систем распределенных вычислений на основе туманных и краевых вычислений // Информатика, вычислительная техника и управление. 2022. № 26 (3). С. 151–167.

Almahlawi, Mikki 2023 – *Almahlawi S., Mikki M.* A Comparison Study of Cloud Computing and Fog Computing // International Journal of Engineering and Information Systems (IJEAIS). 2023. Vol. 7, issue 2. P. 79–83.

Awange, Palancz, Lewis, Volgyesi 2023 – *Awange J., Palancz B., Lewis R., Volgyesi L.* Genetic Algorithms // Awange J., Palancz B., Lewis R., Volgyesi L. Mathematical Geosciences Hybrid Symbolic-Numeric Methods. Cham: Springer, 2023. P. 209–237.

Azizi, Shojafar, Abawajy, Buyya 2022 – *Azizi S., Shojafar M., Abawajy J., Buyya R.* Deadline-aware and energy-efficient IoT task scheduling in fog computing systems: A semi-greedy approach // Journal of Network and Computer Applications. 2022. Vol. 201. P. 1–13.

Ingber, Petraglia, Petraglia, Soares Machado 2012 – *Ingber L., Petraglia A., Petraglia M., Soares Machado M.-A.* Adaptive Simulated Annealing // Stochastic Global Optimization and Its Applications with Fuzzy Adaptive Simulated Annealing. 2012. Vol. 35, issue 1. P. 33–62.

Jumani, Shi, Laghari, Hu, Nabi, Qian 2023 – *Jumani A., Shi J., Laghari A., Hu Z., Nabi A., Qian H.* Fog computing security: A review // Security and privacy. Chichester: John Wiley & Sons, 2023. P. e313.

Karampudi et al. 2023 – *Karampudi R., Reddy Gudipati P., SaiSidhartha Reddy K., Aditya M., Priyanshu.* Resource management and allocation in fog computing // International Journal of Advanced Research in Computer Science. 2023. Vol. 14, no. 1. P. 23–35.

Klimenko, Klimenko, Melnik 2015 – *Klimenko A., Klimenko V., Melnik E.* The parallel simulated annealing-based reconfiguration speedup algorithm for the real time distributed control system fault-tolerance providing // Proceedings of the 9th IEEE International Conference on Application of Information and Communication Technologies (AICT), 14–16 October, 2015, Rostov-on-Don, Russia. Piscataway, NJ: Curran Associates, Inc., 2015. P. 277–280.

Melnik, Klimenko, Korobkin 2020 – *Melnik E., Klimenko A., Korobkin V.* Fault-Tolerant Management for the Edge Devices on the Basis of Consensus with Elected Leader // Software engineering perspectives in intelligent systems. CoMeSySo 2020. Advances in Intelligent Systems and Computing. 2020. Vol. 1294. P. 464–474.

Melnik, Klimenko 2020 – *Melnik, E., Klimenko A.* A condition of reliability improvement of the system based on the fog-computing concept // Journal of Physics: Conference Series. 2020. Vol. 1661 (1). P. 012007.

Movahedi, Defude, Hosseininia 2021 – *Movahedi Z., Defude B., Hosseininia A.-M.* An efficient population-based multi-objective task scheduling approach in fog computing systems // Journal of Cloud Computing. 2021. Vol. 10, issue 1. P. 53.

## *References*

Almahlawi, S. and Mikki, M. (2023), "A Comparison Study of Cloud Computing and Fog Computing", *International Journal of Engineering and Information Systems (IJEAIS)*, vol. 7, issue 2, pp. 79–83.

Awange, J., Palancz, B., Lewis, R. and Volgyesi, L. (2023), Genetic Algorithms, in Awange, J. at al. *Mathematical Geosciences Hybrid Symbolic-Numeric Methods*, Springer, Cham, Switzerland, pp. 209–237.

Azizi, S., Shojafar, M., Abawajy, J. and Buyya, R. (2022), "Deadline-aware and energy-efficient IoT task scheduling in fog computing systems: A semi-greedy approach", *Journal of Network and Computer Applications*, vol. 201, pp. 1–13.

Ingber, L., Petraglia, A., Petraglia, M. and Soares Machado, M.-A. (2012), "Adaptive Simulated Annealing", *Stochastic Global Optimization and Its Applications with Fuzzy Adaptive Simulated Annealing*, vol. 35, issue 1, pp. 33–62.

Jumani, A., Shi, J., Laghari, A., Hu, Z., Nabi, A. and Qian, H. (2023), "Fog computing security: A review", *Security and privacy*, John Wiley & Sons, Chichester, UK, p. e313.

Kalyaev I. and Melnik E. (2011), Decentralized computer control systems, SSC RAS, Rostov on/D., Russia, 196 p.

Karampudi at al. (2023), "Resource management and allocation in fog computing", *International Journal of Advanced Research in Computer Science*, vol. 14, no 1, pp. 23–35.

Klimenko, A., Klimenko, V. and Melnik, E. (2015), "The parallel simulated annealing-based reconfiguration speedup algorithm for the real time distributed control system fault-tolerance providing", *Proceedings of the 9th IEEE International Conference on Application of Information and Communication Technologies (AICT)*, 14–16 October, Rostov-on-D., Russia, Curran Associates, Inc., Piscataway, NJ, USA, pp. 277–280.

Klimenko, A. (2022), "The Basic Elements of Devices Resource Consumption Decreasing Metodology for Distributed Systems on the Basis of Fog- and Edge-Computing", *Informatics, Computer Science and Management*, vol. 26, no. 3, pp. 151–167.

Melnik, E., Klimenko, A. and Korobkin, V. (2020), "Fault-Tolerant Management for the Edge Devices on the Basis of Consensus with Elected Leader", *Software engineering perspectives in intelligent systems*, CoMeSySo 2020, *Advances in Intelligent Systems and Computing*, vol. 1294, pp. 464–474.

Melnik, E. and Klimenko, A. (2020), "A condition of reliability improvement of the system based on the fog-computing concept", *Journal of Physics: Conference Series*, vol. 1661 (1), pp. 012007.

Movahedi, Z., Defude, B. and Hosseininia, A.-M. (2021), "An efficient population-based multi-objective task scheduling approach in fog computing systems", *Journal of Cloud Computing*, vol. 10, issue 1, p. 53.

### *Информация об авторах*

*Эльвира М. Алиева*, студент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; marun4ka@gmail.com

*Андрей Е. Сальников*, студент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; andrejs03_21@mail.ru

*Анна Б. Клименко*, кандидат технических наук, доцент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; anna_klimenko@mail.ru

### *Information about the author*

*Elvira M. Alieva*, student, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, Russia, 125047; marun4ka@gmail.com

*Andrei E. Sal'nikov*, student, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, Russia, 125047; andrejs03_21@mail.ru

*Anna B. Klimenko*, Cand. of Sci. (Engineering), associate professor, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, Russia, 125047; anna_klimenko@mail.ru

Дизайн обложки
*Е.В. Амосова*

Корректор
*Н.В. Москвина*

Компьютерная верстка
*Н.В. Москвина*

Подписано в печать 31.07.2023.
Формат 60×90 1/16.
Уч.-изд. л. 5,2. Усл. печ. л. 5,3.
Тираж 1050 экз. Заказ № 1787

Издательский центр
Российского государственного
гуманитарного университета
125047, Москва, Миусская пл., 6
www.rsuh.ru