

Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ НАУКИ
ИНСТИТУТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ
И МАТЕМАТИЧЕСКОЙ ГЕОФИЗИКИ
СИБИРСКОГО ОТДЕЛЕНИЯ РОССИЙСКОЙ АКАДЕМИИ НАУК
(ИВМиМГ СО РАН)

УДК
Рег. № НИОКТР
Рег. № ИКРБС

УТВЕРЖДАЮ
Директор ИВМ и МГ СО РАН
д. ф.-м. н., профессор РАН
_____ М.А. Марченко
«____» _____ 2023 г.

ОТЧЕТ
О НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЕ

0251-2022-0005 Суперкомпьютерные технологии решения больших задач естествознания,
математические модели, методы анализа и оптимизации сложных информационных си-
стем

Руководитель НИР, глав-
ный научный сотрудник,
д.ф.-м.н.

И.О. Ф

Новосибирск 2023

СПИСОК ИСПОЛНИТЕЛЕЙ

Руководитель НИР, главный научный сотрудник,
д.ф.-м.н.

подпись, дата

И.О. Ф
(введение, заключение)

Исполнители:

д.т.н, с.н.с. А.С. Родионов

подпись, дата

к.ф.-м.н. М.П. Бакулина

подпись, дата

к.т.н., с.н.с. С.В. Бредихин

подпись, дата

К.А. Волжанкина

подпись, дата

Г.А. Капустина

подпись, дата

С.В. Кратов

подпись, дата

В.М. Ляпунов

подпись, дата

к.э.н. О.А. Ляхов

подпись, дата

к.ф.-м.н. Д.А. Мигов

подпись, дата

Моисеенко В.В.

подпись, дата

к.т.н., с.н.с. О.Г. Монахов.

подпись, дата

к.т.н., с.н.с. Э.А. Монахова

подпись, дата

к.т.н. С.В. Рудометов

подпись, дата

к.т.н. О.Д. Соколова

подпись, дата

К.В. Ткачёв

подпись, дата

к.т.н., доцент Г.Ы. Токтошов

подпись, дата

Л.В. Трофимова

подпись, дата

к.ф.-м.н. В.В. Шахов

подпись, дата

Н.Г. Щербаклва

подпись, дата

А.Н. Юргенсон

подпись, дата

А.М. Кальней

подпись, дата

РЕФЕРАТ

Отчет 40с., 1 кн., 5 рис., 2 табл., 30 источн., 0 прил.

ПЕРЧЕНЬ КЛЮЧЕВЫХ СЛОВ: сети, надёжность, информационные системы, имитационное моделирование, оптимизация

Объектом исследования или разработки являются модели и алгоритмы анализа и оптимизации сетей различного назначения и связанные с этим задачи анализа, кодирования и хранения данных.

Цель работы – построение эффективных алгоритмов анализа и оптимизации структур и поведения сложных сетевых систем на основе математических моделей.

Методы исследований основываются на математических теориях: системный анализ, прикладная теория вероятностей, теория кодирования, методы дискретной и многокритериальной оптимизации, теория информации.

Результаты работы и их новизна:

1. Продолжены исследования в области построения математических и имитационных моделей сетей различного назначения, в частности сетей на кристалле, сетей связи, транспортных и информационных, выполнены программные реализации.

2. Выполнен анализ программных продуктов, реализующих поддержку технологии единого входа (Single Sign-On (SSO), при использовании которой пользователи переходят из одной информационной системы в другую, не связанную с первой системой, без повторной аутентификации.

3. Предложен новый метод минимизации оперативных расходов сети мониторинга, критерием производительности которой является монотонно возрастающая функция от вероятности обнаружения заданного события.

Область применения результатов:

Результаты могут использоваться при оптимизации структуры и процессов управления в сетях различного назначения, прежде всего регулярных сетях на кристалле и в мультипроцессорных ЭВМ, а также сетях мониторинга и управления дорожным движением.

Предполагается расширение классов рассматриваемых реальных сетей, в частности виртуальных в среде Интернет.

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.....	5
ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ	6
ВВЕДЕНИЕ.....	7
ОСНОВНАЯ ЧАСТЬ.....	8
1 Список публикаций по теме за 2023 год	12
ЗАКЛЮЧЕНИЕ	14
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	15
ПРИЛОЖЕНИЕ А (обязательное) Проведение вычислений.....	18

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем отчете о НИР применяют следующие термины и определения:

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

В настоящем отчете о НИР применяют следующие сокращения и обозначения:

НИР – научно-исследовательская работа

ВВЕДЕНИЕ

Введение должно содержать оценку **современного** состояния решаемой научно-технической проблемы, основание и исходные данные для разработки темы, обоснование необходимости проведения НИР, сведения о планируемом научно-техническом уровне разработки, о патентных исследованиях и выводы из них, сведения о метрологическом обеспечении НИР. Во введении должны быть отражены актуальность и новизна темы, связь данной работы с другими научно-исследовательскими работами.

Во введении промежуточного отчета по этапу НИР должны быть указаны цели и задачи исследований, выполненных на данном этапе, их место в выполнении отчета о НИР в целом.

Во введении заключительного отчета о НИР приводят перечень наименований всех подготовленных промежуточных отчетов по этапам и их регистрационные номера.

ОСНОВНАЯ ЧАСТЬ

В части исследований регулярных больших сетей впервые созданы две базы данных (датасеты), содержащие параметры описаний оптимальных по диаметру хордальных кольцевых сетей (Chordal Ring Networks) с числом узлов до 60 тысяч, и двухконтурных кольцевых циркулянтных сетей (Double-Loop Networks) с числом узлов до 50 тысяч, используемых в качестве моделей топологий сетей связи для многопроцессорных суперЭВМ и сетей на кристалле. Полученные датасеты оптимальных сетей представлены для открытого доступа в Интернете. Для оптимизации кольцевых сетей реализованы параллельные версии алгоритма сокращенного перебора на кластере Kunpeng. Проведён анализ эффективности и получены экспериментальные оценки ускорения нескольких схем распараллеливания алгоритмов. Для анализа датасетов и поиска общих аналитических зависимостей параметров семейств оптимальных сетей разработано и реализовано два новых метода - темплейт-ориентированный и метод последовательного деления параметров сетей. Предложенные методы позволили открыть аналитические описания более 500 семейств оптимальных хордальных кольцевых сетей и более 2000, отличных от известных в литературе, семейств оптимальных двухконтурных кольцевых сетей с образующими линейного и квадратичного типов. Разработан и реализован параллельный генетический алгоритм для оптимизации больших циркулянтных сетей. Параллельная программа синтеза циркулянтных сетей зарегистрирована в Роспатенте.

В части исследования специальных коммуникационных сетей, включая сети на кристалле, предложены новые модели топологий сетей связи для многопроцессорных суперЭВМ и сетей на кристалле. Введён класс параметрически регулярных многоуровневых PRM сетей (Parametrically Regular Multi-level networks) с использованием гибкого, «нечёткого» темплейта с недоопределёнными параметрами. Для синтеза сетей нового класса разработаны и реализованы параллельные метаэвристические алгоритмы определения оптимальных параметров топологии сети связи для заданных числа узлов, числа уровней и степени узлов. Показано преимущество предложенных PRM сетей при соизмеримых затратах на число узлов и число связей системы по таким структурным характеристикам, как диаметр, среднее расстояние по сравнению с циркулянтами и торами различных степеней.

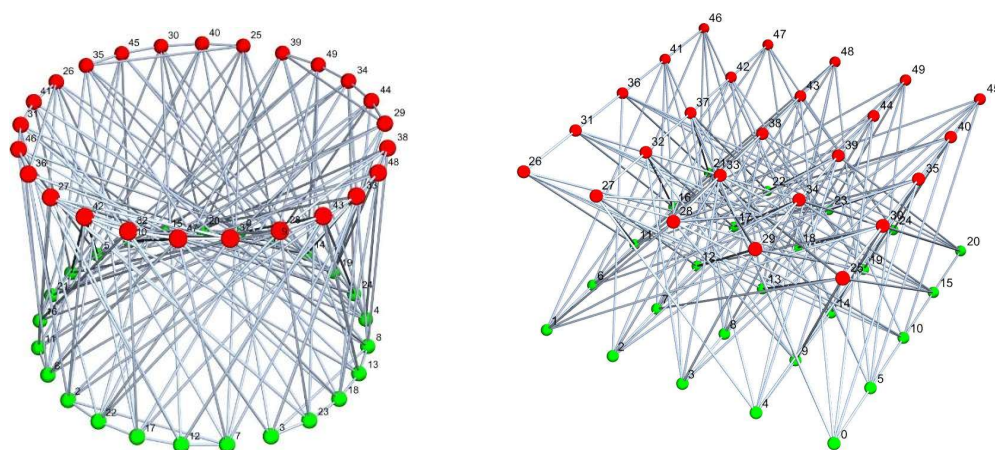


Рис. 1. Пример двухуровневой PRM сети, достигающей нижней границы диаметра $D=2$, для двух различных конфигураций с $N=50$, $v=7$, $L=2$, $g=5$, $S=5$.

В части решения динамических задач оптимального планирования (корректировки планов с учётом текущих отклонений) реализована часть комплекса программ расчета отклонений потребностей в ресурсах от их наличия и их перераспределения по временным интервалам для уменьшения дефицита ресурсов. Используются линейные модели для решения ресурсных задач календарного планирования проектов.

В текущем состоянии разрабатываемый комплекс программ позволяет для заданного расписания работ и данных о наличии ресурсов:

1. Подсчитать потребности в ресурсах и отклонения от имеющихся ресурсов;
2. Перераспределить ресурсы по временным интервалам по критерию минимизации несбалансированности ресурсов оставшейся части проекта.

Завершение программной реализации планируется в 2024 году.

В части исследования моделей и алгоритмов анализа и оптимизации сетей с мобильными узлами решались следующие задачи:

Проводились исследования возможностей Интернета вещей (Internet of Thing, IoT) для функционирования современных систем мониторинга. Предложен метод нахождения оптимального порогового количества датчиков, способных обнаружить мониторируемое событие. Метод на основе пороговых значений действует как локальный механизм принятия решений и используется для реализации концепции вычислений с множественным доступом. Периферийные вычисления с множественным доступом позволяют обрабатывать полученные от датчиков данные в непосредственной близости от пользователя, что уменьшает задержки в работе системы, обеспечивает более быстрый анализ ситуации. Уменьшение объема передаваемых данных повышает безопасность и конфиденциальность информации.

Разработана информационная система MoniPol, реализующая: транспортную модель движения автомобилей и автобусов на карте города; сбор данных о состоянии окружающей

среды с помощью датчиков, размещенных на транспорте; вычисление рисков заражения людей в зонах загрязнения. Имитационное моделирование сбора данных с помощью системы MoniPol позволяет решать оптимизационные задачи создания системы мониторинга атмосферы мегаполиса.

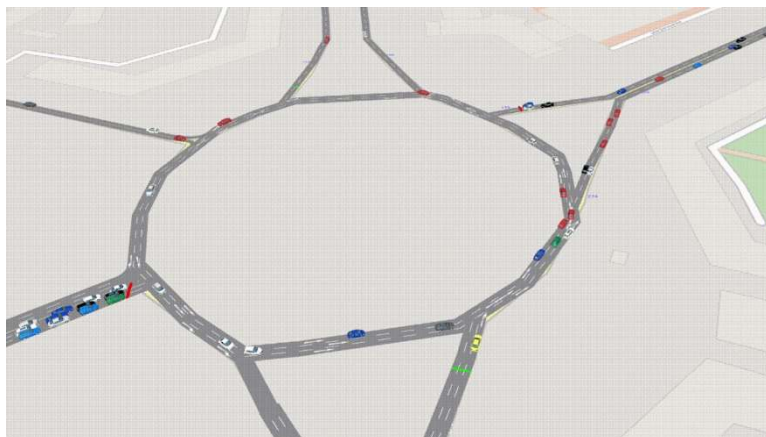


Рис. 2. Моделирование движения транспорта по пл. Калинина

В части решения задач анализа информационных сетей построена модель сети научного соавторства, основанная на групповых отношениях, возникающих между соавторами. Модель представлена в виде гиперграфа, вершины которого соответствуют авторам, а ребра – публикациям.

Гиперграф построен на реальных

данных, извлеченных из XML архива статей отечественного научного журнала. Измерены параметры гиперграфа и выявлены его топологические свойства. На основе реальных данных из архива журнала «Сахарный диабет» (ISSN 2072-0378) построена комплексная сеть (КС) научного соавторства, формальное описание которой опирается на двудольный граф. Апробированы методы анализа КС, измерены ее базовые параметры, определены основные свойства.

В решении задач анализа надёжности сложных систем сетевой структуры разработаны новые модификации метода факторизации, использующегося для точного расчёта вероятности связности случайного графа, основанные на декомпозиции сети по вершинному разрезу (сечению, сепаратору), образованному двумя вершинами.

Исследовались алгоритмы анализа надёжности сетей протяжённой структуры, что характерно для сетей, расположенных в шахтах, кораблях, а также линейных беспроводных сенсорных сетей, предназначенных для мониторинга различных протяженных объектов, таких как трубопроводы и железные дороги. Результаты численных экспериментов подтверждают эффективность предлагаемых алгоритмов.

В части программного обеспечения решения задач анализа ненадёжных структур реализована первая версия открытой библиотеки анализа показателей надёжности случайных графов.

Продолжались работы по информационным системам. Выполнен анализ программных продуктов, реализующих поддержку технологии единого входа (Single Sign-On (SSO), при использовании которой пользователи переходят из одной информационной системы в

другую, не связанную с первой системой, без повторной аутентификации. Произведен анализ существующих на сегодняшний день решений, сгруппированных с точки зрения их лицензий – проприетарные международные, проприетарные локальные и свободные и/или открытые международные. При анализе учитывались также и потенциальные проблемы, недостатки использования систем подобного класса. Обзорная и аналитическая части основаны в том числе на анализе актуальных научных публикаций по данной тематике. Сделаны выводы о целесообразности использования систем SSO в целом и конкретных типов систем с точки зрения потребностей научно-исследовательской организации.

В части развития теории имитационного моделирования исследовались различные модели использования средств и методов искусственного интеллекта в имитации сложных недоопределённых систем и решении задач имитационной оптимизации.

1 Список публикаций по теме за 2023 год

1. E. A. Monakhova, O. G. Monakhov, A. Yu. Romanov. Routing Algorithms in Optimal Degree Four Circulant Networks Based on Relative Addressing: Comparative Analysis for Networks-on-Chip // IEEE Transactions on Network Science and Engineering, 2023, 10 (1), pp. 413–425, - DOI: 10.1109/TNSE.2022.3211985, (WoS, Q1)
2. E. A. Monakhova and O. G. Monakhov, Constructing a Series of Families of Degree Six Circulant Networks // Journal of Applied and Industrial Mathematics, 2022, Vol. 16, No. 4, pp. 695–705. DOI: <https://doi.org/10.1134/S199047892204010X> (WoS RSCI, Scopus Q2, статья не вошла в отчет 2022г)
3. Oleg Monakhov, Emilia Monakhova, Sergey Kireev. Parallel Optimization and Performance Tuning on a Kunpeng Cluster of Genetic Algorithm for Synthesis of Circulant Networks // Lobachevskii J. Math, 44 (8), (august 2023), p. 3129-3138. DOI: 10.1134/S1995080223080425 (WoS RSCI, Scopus Q2)
4. Oleg Monakhov, Emilia Monakhova, Sergey Kireev, Parallel Generation and Analysis of Optimal Chordal Ring Networks Using Python Tools on Kunpeng Processors // Malyshev, V. (eds) Parallel Computing Technologies. PaCT 2023. Lecture Notes in Computer Science 14098, p. 126-135, Springer, 2023. DOI: https://doi.org/10.1007/978-3-031-41673-6_10 (Web of Science, Scopus)
5. Monakhova E., Monakhov O. Generation and analysis of optimal double-loop circulant networks dataset // CEUR Workshop Proceedings. 4. Сер. "SibDATA 2023 – Short Paper Proceedings of the 4th Inter. Siberian Scientific Workshop on Data Analysis Technologies with Applications 2023", 2023. – 9 С. (Scopus)
6. Э.А. Монахова, О.Г. Монахов. Открытие аналитических зависимостей параметров оптимальных хордальных сетей на основе анализа данных // Проблемы информатики, 2023, № 4. DOI: 10.24412/2073-0667-2023-4-37-48
7. Монахов О.Г., Монахова Э.А., Киреев С.Е. Параллельная программа синтеза оптимальных циркулянтных сетей с использованием генетического алгоритма. Роспатент 2023. Номер регистрации (свидетельства): 2023663623. Дата регистрации: 27.06.2023. Дата публикации и номер бюллетеня: 27.06.2023 Бюл. No 7. (РИНЦ)
8. О. А. Ляхов Учет нескладируемых ресурсов в целочисленных моделях календарного планирования проектов // Проблемы информатики. № 1, с.5-11, 2023. (БАК)
9. V. Shakhov; Insoo Koo; O. Sokolova. On Optimizing MEC Enabled Monitoring Systems // 9th International Asian School-Seminar on Optimization Problems of Complex Systems (OPCS) 2023, P. 100-103, doi: 10.1109/OPCS59592.2023.10275757.

10. K. Tkachev; O. Sokolova; A. Materukhin. Simulation of Air Pollution Monitoring using Geosensors Placed on Vehicles // Proceedings of the 19th International Asian School-Seminar on Optimization Problems of Complex Systems (OPCS) 2023, Pp. 110-113, doi: 10.1109/OPCS59592.2023.10275326.
11. Бредихин С.В., Щербакова Н.Г. Модель сети соавторства научного журнала. // Пробл. информ. 2023. № 3. С. 5–18. DOI: 10.24412/2073-0667-2023-3-5-18.
12. Бредихин С.В., Щербакова Н.Г. Юргенсон А. Н. Модели сети соавторства научного журнала. Часть 2. // Пробл. информ. 2023. № 4 (в печати).
13. Коробов А.В., Мигов Д.А. Алгоритмы расчета надежности сети на основе декомпозиционного подхода // Проблемы информатики, № 4(61), с.17-28. DOI: 10.24412/2073-0667-2023-4-17-28
14. V. Shakhov, I. Koo and O. Sokolova. On Optimizing MEC Enabled Monitoring Systems // Proceedings of the 19th International Asian School-Seminar on Optimization Problems of Complex Systems (OPCS) 2023, pp. 100-103, doi: 10.1109/OPCS59592.2023.10275757.
15. Kratov Sergey The Comparative Analysis of Technologies and Software for Single Sign-On // Proceedings of the International Asian School-Seminar Optimization Problems of Complex Systems (OPCS'23), P. 44 - 47
16. А.В. Подсадников, С.В. Кратов Программное обеспечение и сервисы информационной поддержки дистанционной работы в образовательных и научных центрах // Информатика и образование (БАК, в печати)
17. A. Rodionov. Little tricks leading to a significant acceleration of the calculation of the reliability of a random graph // Proceedings of the 17th International Conference on Ubiquitous Information Management and Communication (IMCOM), 2023, pp. 1-5, doi: 10.1109/IMCOM56909.2023.10035637.
18. A. Rodionov. Cognisant Simulation: New Age // Proceedings of the 19th International Asian School-Seminar on Optimization Problems of Complex Systems (OPCS), Novosibirsk, Moscow, Russian Federation, 2023, pp. 90-93, doi: 10.1109/OPCS59592.2023.1027574.
19. Кальней А.М. Hypernet_Reliability_Project. Роспатент 2023. Номер регистрации (свидетельства): 2023619172. Дата регистрации: 27.04.2023. Дата публикации и номер бюллетеня: 04.05.2023, Бюл. No 6

ЗАКЛЮЧЕНИЕ

В целом поставленные задачи выполнены. Разработаны новые математические модели и методы их исследования, зарегистрированы комплексы программ.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Colbourn Ch. J. The combinatorics of network reliability. N.Y: Oxford Univ. press. 1987. P. 160.
2. Hebert Perez-Roses. Sixty Years of Network Reliability // Mathematics in Computer Science. 2018. Vol. 12. P. 275-293.
3. Yeh W. C. Novel Binary-Addition Tree Algorithm (BAT) for Binary-State Network Reliability Problem // Reliability Engineering and System Safety. 2020. 208: 107448.
4. Valiant L. The complexity of enumeration and reliability problems. // SIAM Journal on Computing. 1979. Т. 8. № 3. P. 410–421.
5. Page L.B., Perry J.E. A Practical Implementation of the Factoring Theorem for Network Reliability // IEEE transactions on reliability. 1988. Т. 37, № 3. P. 259–267.
6. Rodionova O.K., Rodionov A.S Choo H. Network Probabilistic Connectivity: Exact Calculation with Use of Chains // ICCSA--2004, Springer Lecture Notes in Computer Sciences. 2004. Vol. 3046. P. 315--324.
7. Мигов Д.А., Нестеров С.Н., Родионов А.С. Методы ускорения расчета надежности сетей с ограничением на диаметр // Вестник СибГУТИ. № 1, 2014, с. 49-56.
8. Wood R. K. Triconnected decomposition for computing K--terminal network reliability // Networks. 1989. V.~19. P.~203--220.
9. Migov D.A., Rodionova O.K., Rodionov A.S., Choo H. Network Probabilistic Connectivity: Using Node Cuts // EUC Workshops, Springer Lecture Notes in Computer Sciences. 2006. Vol. 4097. P. 702--709.
10. Burgos JM, Amoza FR. Factorization of network reliability with perfect nodes I: Introduction and statements // Discrete Applied Mathematics. 2016, v. 198, pp. 82-90.
11. Д. Мигов. Декомпозиция сети по сечениям при расчёте её надёжности // Прикладная дискретная математика. 2020. №.47. С. 62-86.
12. Мур Э., Шеннон К. Надежные схемы из ненадежных реле // Кибернетически сб. М.: Иностран. лит. 1960. Вып. 1. С. 109–148.
13. Мигов Д.А. Формулы для быстрого расчета вероятности связности подмножества вершин в графах небольшой размерности // Проблемы информатики. № 6, 2010, с. 10-17.

14. A. Rodionov, D. Migov. Obtaining and Using Cumulative Bounds of Network Reliability // Chapter no 5 in: System Reliability. Edt. by Constantin Volosencu. ISBN 978-953-51-3705-4. Publisher: InTech. Rijeka, Croatia. 2017. P. 93-112.
15. S. Kratov, "On the approaches to the development of a scientific organization website," Proc. of the 3rd Russian-Pacific Conf. on Computer Tech. and Applications (RPC 2018), 8482177, 2018.
16. S. Kratov, "On improving the indexing of information systems based on Web technologies," J. Phys.: Conf. Ser., 1210, 012072, 2019.
17. P. Prashant, and T. N. Nisha, "Challenges in single sign-on," J. of Ph.: Conf. Series, 2021.
18. A. Tsuyoshi, N. Takayuki, and H. Yamaoka, "How to integrate on-premise authentication system into cloud services: single sign-on for Office365," Proc. ACM SIGUCCS User Services Conference, 2019.
19. M. Kihara, and S. Iriyama, "Security and performance of single sign-on based on one-time pad algorithm," Cryptography, 2020.
20. A. A. Shinkarev, "Using the ideal point method to search the best authentication method in corporate information systems," Bull. of the South Ural State University. Ser. Comp. Tech., Automatic Control & Radioelectronics, 2022.
21. G. Srivathsan, S. Morkonda, P. Chiasson, and C. V. Oorschot, "Empirical analysis and privacy implications in OAuth-based single sign-on systems," Proc. of the 20th Workshop on Privacy in the Electronic Society, 2021.
22. A. Ceccanti, E. Vianello, and D. Michelotto, "Token-based authorization in storm WebDAV," EPJ Web of Conf., 2020.
23. L. Wenzheng, W. Xiaofeng, and X. Qianqian, "Center-less single sign-on with privacy-preserving remote biometric-based ID-MAKA scheme for mobile cloud computing services," IEEE Access, 2019.
24. M. Héder, S. Tenczer, and A. Biancini, "Collaboration between SAML federations and Openstack clouds," SoftwareX, 2019.
25. G. B. Dobbs, "Cloud service authenticates via delegation - SAML," IDPro Body of Knowledge, 2021.
26. D. Yi, T. Donghui, and Z. Shuliang, "Application of authorization in smart grid based on the pass microservice architecture," IOP Conf. Series: Earth and Environmental Science, 2020.

27. A. Jun, C. W. Wang, and X. M. Wang, "Cross-domain single sign-on authentication of information security in network environment," *Int. J. of Inf. and Comm.Tech.*, 2021.
28. T. Waluyo, and Sutarman, "Comparative analysis of the performance of single sign-on authentication systems with OpenID and OAuth protocols," *Int. J. of Comp. and Inf. Tech.*, 2279-0764, 2022.
29. M. G. de Almeida, and E. D. Canedo, "Authentication and authorization in microservices architecture: a systematic literature review," *Appl. Sc.*, Switzerland, 2022.
30. C. Villarán, and M. Beltrán, "Protecting end user's privacy when using social login through GDPR compliance," *Proc. of the 18th Int. Conf. on Sec. and Crypt.*, 2021.
31. C. Villarán, and M. Beltrán, "User-centric privacy for identity federations based on a recommendation system," *Electronics*, 2022.
32. S. Nishioka, and Y. Okabe, "Centralized control of account migration at single sign-on in Shibboleth," *J. of Inf. Proc.*, 2021.
33. S. Kratov, "About leaks of confidential data in the process of indexing sites by search crawlers," *Lect. Notes in Comp. Sc. (LNTCS)*, vol. 11964, 2019.

ПРИЛОЖЕНИЕ

А

(обязательное)

Проведение вычислений

Проведены вычисления на основе предложенных моделей для анализа эффективности разработанных алгоритмов и программ. В части исследования сетей соавторства проведён анализ реальных данных архива авторитетного медицинского журнала.