



Том 10. № 3
2024

ISSN 1813-324X (Print)
ISSN 2712-8830 (Online)

ТРУДЫ УЧЕБНЫХ ЗАВЕДЕНИЙ СВЯЗИ

Темы номера:

- ✓ Алгоритм защиты роевых робототехнических систем
- ✓ Оценка визуальных интерфейсов SIEM-систем
- ✓ Интерференция поднесущих частот в системе DRM

Vol. 10. Iss. 3
2024

PROCEEDINGS
OF TELECOMMUNICATION UNIVERSITIES

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича» (СПбГУТ)

Научный журнал

ТРУДЫ
УЧЕБНЫХ ЗАВЕДЕНИЙ СВЯЗИ

Том 10. № 3

Proceedings of Telecommunication Universities

Vol. 10. Iss. 3

Санкт-Петербург

2024

Описание журнала

Научный журнал. Включен в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук (распоряжение Минобрнауки России № 21-р от 12.02.2019), по специальностям (распоряжение № 33-р от 01.02.2022):

- 1.2.2. Математическое моделирование, численные методы и комплексы программ
- 2.2.6. Оптические и оптико-электронные приборы и комплексы
- 2.2.13. Радиотехника, в том числе системы и устройства телевидения
- 2.2.14. Антенны, СВЧ-устройства и их технологии
- 2.2.15. Системы, сети и устройства телекоммуникаций
- 2.2.16. Радиолокация и радионавигация
- 2.3.1. Системный анализ, управление и обработка информации, статистика
- 2.3.6. Методы и системы защиты информации, информационная безопасность

Журнал позиционирует себя как научный, в связи с этим его целями являются ознакомление научной общественности (научного сообщества) с результатами оригинальных исследований, выполненных ведущими учеными и специалистами и их коллективами, а также апробация научных результатов, полученных при подготовке кандидатских и докторских диссертаций для повышения качества (уровня) проводимых исследований. Издание ставит перед собой задачу расширения инфокоммуникативного пространства взаимодействия российских и зарубежных ученых. Целевой аудиторией журнала являются ученые и специалисты-практики в области связи и телекоммуникаций и смежных направлениях науки и техники, а также профессорско-преподавательский состав и студенты, обучающиеся по программам аспирантуры, магистратуры, специалитета и бакалавриата профильных вузов и кафедр.

Выпускается с 1960 года. Выходит 6 раз в год. Издается на русском и английском языках.

Редакционный совет

Киричек Р.В. д.т.н., проф., Санкт-Петербургский государственный университет телекоммуникаций
Главный редактор им. проф. М.А. Бонч-Бруевича (СПбГУТ), г. Санкт-Петербург, Россия

Владыко А.Г. к.т.н., доцент, Санкт-Петербургский государственный университет телекоммуникаций
Зам. Главного редактора им. проф. М.А. Бонч-Бруевича (СПбГУТ), г. Санкт-Петербург, Россия

Буйневич М.В. д.т.н., проф., Санкт-Петербургский университет государственной противопожарной
службы МЧС России, г. Санкт-Петербург, Россия

Зеневич А.О. д.т.н., проф., Белорусская государственная академия связи, г. Минск, Республика Беларусь

Розанов Н.Н. д.ф.-м.н., проф., чл.-корр. РАН, АО «Государственный оптический институт
им. С.И. Вавилова» (ГОИ), г. Санкт-Петербург, Россия

Дукельский К.В. д.т.н., доцент, АО «Государственный оптический институт им. С.И. Вавилова» (ГОИ),
г. Санкт-Петербург, Россия

Кучерявый Е. PhD, Технологический университет Тампере, г. Тампере, Финляндия

Каримов Б.Т. к.т.н., доцент, Институт электроники и телекоммуникаций, Кыргызский государственный
технический университет И. Раззакова (КГТУ), г. Бишкек, Кыргызстан

Тиамийу О.А. PhD, Университет Илорина, г. Илорин, Нигерия

Козин И.Д. д.ф.-м.н., проф., Алматинский университет энергетики и связи, г. Алма-Аты, Казахстан

Самуйлов К.Е. д.т.н., проф., Российский университет дружбы народов (РУДН), г. Москва, Россия

Степанов С.Н. д.т.н., проф., Московский технический университет связи и информатики (МТУСИ),
г. Москва, Россия

Росляков А.В. д.т.н., проф., Поволжский государственный университет телекоммуникаций
и информатики (ПГУТИ), г. Самара, Россия

Кучерявый А.Е. д.т.н., проф., Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича (СПбГУТ), г. Санкт-Петербург, Россия

Канаев А.К. д.т.н., проф., Петербургский университет путей сообщения имени Александра I (ПГУПС),
г. Санкт-Петербург, Россия

Новиков С.Н. д.т.н., проф., Сибирский государственный университет телекоммуникаций и информатики
(СибГУТИ), г. Новосибирск, Россия

Дворников С.В. д.т.н., проф., Военная академия связи им. Маршала Советского Союза С.М. Буденного (ВАС),
г. Санкт-Петербург, Россия

Коржик В.И. д.т.н., проф., Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича (СПбГУТ), г. Санкт-Петербург, Россия

Ковалгин Ю.А. д.т.н., проф., Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича (СПбГУТ), г. Санкт-Петербург, Россия

Description

Scientific journal. The journal is included in the List of reviewed scientific publications, in which the main scientific results of dissertations for the degree of candidate of science and for the degree of doctor of science should be published (order of the Ministry of Education and Science of Russia No 21-r of 12 February 2019) in the field of (order of the Ministry of Education and Science of Russia No 33-r of 01 February 2022):

1.2.2. Mathematical modeling, numerical methods and complexes of programs

2.2.6. Optical and optoelectronic devices and complexes

2.2.13. Radio engineering, including television systems and devices

2.2.14. Antennas, microwave devices and its technologies

2.2.15. Systems, networks and telecommunication devices

2.2.16. Radiolocation and radio navigation

2.3.1. System analysis, management and information processing, statistics

2.3.6. Methods and systems of information security, cybersecurity

The journal positions itself as a scientific one, in this regard, its goals are to familiarize the scientific community (scientific community) with the results of original research carried out by leading scientists and specialists and their teams, as well as approbation of scientific results obtained in the preparation of candidate and doctoral dissertations to improve the quality (level) of ongoing research. The publication sets itself the task of expanding the infocommunicative space of interaction between Russian and foreign scientists. The target audience of the journal are scientists and practitioners in the field of communications & telecommunications and related fields of science & technology, as well as faculty and students enrolled in postgraduate, master's, specialisation and bachelor's programs of profiled universities and departments.

Since 1960. Published 6 times per year. Published in Russian and English.

Editorial Board

R.V. Kirichek DSc, prof., The Bonch-Bruevich Saint-Petersburg State University
Editor-in-chief of Telecommunications (SPbSUT), Saint-Petersburg, Russia

A.G. Vladyko PhD, associate prof., The Bonch-Bruevich Saint-Petersburg State University
Deputy editor-in-chief of Telecommunications (SPbSUT), Saint-Petersburg, Russia

M.V. Buinevich DSc, prof., Saint-Petersburg University of State Fire Service of EMERCOM of Russia,
Saint-Petersburg, Russia

A.O. Zenevich DSc, prof., Belarusian State Academy of Communications, Minsk, Republic of Belarus

N.N. Rozanov DSc, prof., member-corr. RAS, Open Joint Stock Company «S.I. Vavilov State Optical Institute» (SOI),
Saint-Petersburg, Russia

K.V. Dukel'skii DSc, associate prof., Open Joint Stock Company «S.I. Vavilov State Optical Institute» (SOI),
Saint-Petersburg, Russia

Y. Koucheryayv PhD, Tampere University of Technology, Tampere, Finland

B.T. Karimov PhD, Institute of Electronics and Telecommunications, Kyrgyz State Technical University
named after I. Razzakov, Bishkek, Kyrgyzstan

O.A. Tihamiyu PhD, University of Ilorin, Ilorin, Nigeria

I.D. Kozin DSc, prof., Almaty University of Power Engineering and Telecommunications, Almaty, Kazakhstan

K.E. Samuilov DSc, prof., Peoples' Friendship University (RUDN), Moscow, Russia

S.N. Stepanov DSc, prof., Moscow Technical University of Communication and Informatics (MTUCI),
Moscow, Russia

A.V. Roslyakov DSc, prof., Povolzhskiy State University of Telecommunications and Informatics (PSUTI), Samara,
Russia

A.E. Koucheryayv DSc, prof., The Bonch-Bruevich Saint-Petersburg State University of Telecommunication (SPbSUT),
Saint-Petersburg, Russia

A.K. Kanaev DSc, prof., Emperor Alexander I-st Petersburg State Transport University (PSTU),
Saint-Petersburg, Russia

S.N. Novikov DSc, prof., Siberian State University of Telecommunications and Information Sciences (SibSUTIS),
Novosibirsk, Russia

S.V. Dvornikov DSc, prof., Military Academy of Telecommunications named after Marshal Union S.M. Budyonny,
Saint-Petersburg, Russia

V.I. Korzhik DSc, prof., The Bonch-Bruevich Saint-Petersburg State University of Telecommunication (SPbSUT),
Saint-Petersburg, Russia

Yu.A. Kovalgin DSc, prof., The Bonch-Bruevich Saint-Petersburg State University of Telecommunication (SPbSUT),
Saint-Petersburg, Russia

РЕГИСТРАЦИОННАЯ ИНФОРМАЦИЯ / REGISTRATION INFORMATION

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций: ПИ № 77-77501 от 17.01.2020 г. (пред. рег. № 77-17986 от 07.04.2004 г.)

Размещение в РИНЦ (elibrary.ru) по договору: № 59-02/2013R от 20.02.2013

Registered by Federal Service for Supervision of Communications, Information Technology and Mass Media on 17.01.2020: PI No. 77-77501 (prev. reg. on 04.07.2004: No. 77-17986)

Accommodation in RINC (elibrary.ru) by agreement on 20.02.2013: No. 59-02/2013R



Товарный знак № 929373.

Правообладатель:

Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» (СПбГУТ)

191186, Санкт-Петербург, наб. реки Мойки, 61, литера А

Trademark No. 929373.

Copyright holder:

Federal State Budget-Financed Educational Institution of Higher Education «The Bonch-Bruevich Saint- Petersburg State University of Telecommunications» (SPbSUT)

191186, St. Petersburg, emb. Moika River, 61, letter A

КОНТАКТНАЯ ИНФОРМАЦИЯ / CONTACT INFORMATION

Учредитель и издатель: Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» (СПбГУТ)

Адрес учредителя: 191186, Санкт-Петербург, набережная реки Мойки, д. 61, литера А

Адрес редакции: 193232, Санкт-Петербург,

пр. Большевиков, 22/1, к. 334/2

Тел.: +7 (812) 326-31-63, м. т. 2022, +79643759970

E-mail: tuzs@sut.ru

Web: <http://tuzs.sut.ru>

ВК: <http://vk.com/spbtuzs>

Ответственный редактор **Татарникова И.М.**
Выпускающий редактор **Яшугин Д.Н.**
Дизайн: **Коровин В.М.**

Publisher: Federal State Budget-Financed Educational Institution of Higher Education «The Bonch-Bruevich Saint-Petersburg State University of Telecommunications» (SPbSUT)

Publisher address: 191186, Saint Petersburg, Moika river embankment, 61-A

Post address: 193232, Saint Petersburg, Prospekt Bolshevikov, 22/1

Phone: +7 (812) 326-31-63, local 2022, +79643759970

E-mail: tuzs@sut.ru

Web: <http://tuzs.sut.ru>

Executive Editor **Tatarnikova I.M.**
Commissioning Editor **Yashugin D.N.**
Design: **Korovin V.M.**

ВЫХОДНЫЕ ДАННЫЕ / IMPRINT

Дата выхода в свет: 08.07.2024
Тираж: 1000 экз. Цена свободная.

Отпечатано в типографии
Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»

Release date: 08.07.2024
Circulation: 1000 copies. Free price.

Printed in the printing office
Federal State Budget-Financed Educational Institution of Higher Education «The Bonch-Bruevich Saint- Petersburg State University of Telecommunications»



СОДЕРЖАНИЕ

CONTENTS

КОМПЬЮТЕРНЫЕ НАУКИ И ИНФОРМАТИКА

<p>Плотников П.В., Владыко А.Г. Анализ подходов к оптимизации V2X-систем: кластеризация, граничные и туманные вычисления</p>	7	<p>Plotnikov P.V., Vladyko A.G. Analysis of approaches to optimization of V2X systems: clustering, edge and fog computing</p>
---	---	--

ЭЛЕКТРОНИКА, ФОТОНИКА, ПРИБОРОСТРОЕНИЕ И СВЯЗЬ

<p>Волков А.Н. Динамические туманные вычисления и бессерверная архитектура: на пути к зеленым ИКТ</p>	24	<p>Volkov A.N. Dynamic fog computing towards green ICT</p>
--	----	---

<p>Ковалгин Ю.А. Интерференция между поднесущими частотами в системе DRM</p>	35	<p>Kovalgin Yu.A. Interference between subcarrying frequencies in DRM system</p>
---	----	---

<p>Кукунин Д.С. Кодовое разделение на основе двойного расширения спектра сигнала</p>	45	<p>Kukunin D.S. Code division based on double spread spectrum signal</p>
---	----	---

<p>Маколкина М.А., Шарлаева М.В. Исследование средней задержки в сетях связи, предоставляющих телемедицинские услуги</p>	59	<p>Makolkina M.A., Sharlaeva M.V. Research of average delay in telecommunication networks providing telemedicine services</p>
---	----	--

<p>Тупикин А.А., Пахотин В.А., Потапов Д.С. Методика автоматического профилирования электрических характеристик подстилающей поверхности на трассе распространения радиоволн ОНЧ-диапазона</p>	66	<p>Tipikin A.A., Pakhotin V.A., Potapov D.S. Technique for automatic profiling of underlying surface electric parameters on the very low frequencies radio path</p>
---	----	--

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

<p>Зикратов И.А., Зикратова Т.В., Новиков Е.А. Алгоритм защиты роевых робототехнических систем от атак вредоносных роботов с координированной стратегией поведения</p>	75	<p>Zikratov I.A., Zikratova T.V., Novikov E.A. Swarm robotics system algorithm for defense against coordinated behavior strategy attacks</p>
---	----	---

<p>Николаев В.В., Саенко И.Б. Оптимизация распределения информационных ресурсов в едином информационном пространстве</p>	87	<p>Nikolaev V.V., Saenko I.B. Optimization of information resources distribution in a common information space</p>
---	----	---

<p>Шелухин О.И., Рыбаков С.Ю., Ванюшина А.В. Оценка характеристик мультифрактального спектра фрактальной размерности сетевого трафика и компьютерных атак IoT</p>	104	<p>Sheluhin O.I., Rybakov S.Y., Vanyushina A.V. Estimation of the multifractal spectrum characteristics of fractal dimension of networks traffic and computer attack in IoT</p>
--	-----	--

<p>Чечулин А.А. Оценка визуальных интерфейсов систем управления информационной безопасностью</p>	116	<p>Chechulin A.A. Evaluation of visual interfaces in information security management system</p>
---	-----	--

КОМПЬЮТЕРНЫЕ НАУКИ И ИНФОРМАТИКА

1.2.2 – Математическое моделирование, численные методы и комплексы программ

Обзорная статья

УДК 621.391:004.75

<https://doi.org/10.31854/1813-324X-2024-10-3-7-22>

Анализ подходов к оптимизации V2X-систем: кластеризация, граничные и туманные вычисления

Павел Владимирович Плотников , plotnikov.pv@sut.ru

Андрей Геннадьевич Владыко, vladyko@sut.ru

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича,
Санкт-Петербург, 193232, Российская Федерация

Аннотация

В обзорной статье ставится **задача** по анализу существующих решений для систем связи на основе технологии Vehicle-to-Everything (V2X) при использовании механизмов кластеризации и периферийных вычислений с **целью** определения концептуальной модели V2X-системы и наиболее значимых показателей качества обслуживания (QoS) с учетом применения указанного комплекса технологических решений. **Новизна** работы состоит в том, что исследование направлено на выявление возможностей интеграции механизмов кластеризации, граничных и туманных вычислений для определения оптимальных решений по развертыванию объектов придорожной сетевой инфраструктуры с сохранением высоких показателей QoS для техники средств связи данного типа. **Результат** заключается в том, что предложен научно-обоснованный технологический подход к построению концептуальной модели V2X-системы с заданными показателями QoS. **Практическая и теоретическая значимость.** Полученные результаты могут быть использованы при проектировании и развертывании V2X-систем.

Ключевые слова: Vehicle-to-Everything, кластеризация, граничные вычисления, туманные вычисления, QoS

Источник финансирования: Работа выполнена при финансовой поддержке Российского научного фонда по гранту № 24-29-00304.

Ссылка для цитирования: Плотников П.В., Владыко А.Г. Анализ подходов к оптимизации V2X-систем: кластеризация, граничные и туманные вычисления // Труды учебных заведений связи. 2024. Т. 10. № 3. С. 7–22. DOI:10.31854/1813-324X-2024-10-3-7-22. EDN:TRWNON

Review article

<https://doi.org/10.31854/1813-324X-2024-10-3-7-22>

Analysis of Approaches to Optimization of V2X Systems: Clustering, Edge and Fog Computing

Pavel V. Plotnikov , pavplot@gmail.com

Andrey G. Vladyko, vladyko@sut.ru

The Bonch-Bruevich Saint Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Annotation

The review sets the **task** of analyzing existing solutions for communication systems based on Vehicle-to-Everything (V2X) technology using clustering and edge computing mechanisms in **order** to determine the conceptual model of the V2X system and the most significant indicators of quality of service (QoS), taking into account the application of the specified complex of technological solutions. The **novelty** of the work lies in the fact that the research is aimed at identifying the possibilities of integrating clustering mechanisms, edge and fog computing to determine optimal solutions for the deployment of roadside network infrastructure objects while maintaining high QoS indicators for communication equipment of this type. The **result** is that a scientifically based technological approach to constructing a conceptual model of a V2X system with specified QoS indicators has been proposed. **Practical and theoretical relevance.** The results obtained can be used in the design and deployment of V2X systems.

Keywords: Vehicle-to-Everything, clustering techniques, edge computing, fog computing, QoS

Funding: The work was supported by the Russian Science Foundation, contract number 24-29-00304.

For citation: Plotnikov P.V., Vladyko A.G. Analysis of Approaches to Optimization of V2X Systems: Clustering, Edge and Fog Computing. *Proceedings of Telecommunication Universities*. 2024;10(3):7–22. (in Russ.) DOI:10.31854/1813-324X-2024-10-3-7-22. EDN:TRWNON

Введение

В последние годы коммуникационная технология «транспортное средство – окружающая среда» (V2X, аббр. от англ. Vehicle-to-Everything) в интеллектуальных транспортных системах (ИТС) приобрела огромный интерес, так как она потенциально позволяет обеспечить современные потребности ИТС, уменьшить нагрузку на транспортную сеть, повысить безопасность дорожного движения, обеспечить комфорт вождения, предложить альтернативную систему экстренной связи в случае стихийных бедствий, а также обеспечить высокую степень автоматизации транспортных средств (ТС) [1–3]. Для достижения отмеченных показателей V2X-технология должна обеспечивать низкую задержку и высокую надежность, энергоэффективность и оптимальное распределение вычислительных ресурсов. При этом необходимо учитывать специфику сети передачи данных, ее высокую динамичность, постоянные изменения топологии сети и обмен большими объемами данных. В случае, если указанные требования не будут выполнены, критически важные для безопасности приложения не смогут реагировать в потенциально опасных ситуациях. Дополнительно стоит отметить, что большой интерес представляет создание некоего комплекса управления V2X-системой в целом.

Для проектирования транспортных систем с высокими уровнями автоматизации (eyes-off и mind-off) ТС должно иметь возможность обрабатывать большие объемы данных в реальном времени, связанных с распознаванием близлежащих объектов, дорожных аварий, решением навигационных задач и т. д. Однако вычислительные ресурсы некоторых существующих ТС ограничены для запуска таких приложений. При этом, любое нарушение функционирования и устойчивости системы может под-

вергнуть опасности людей и техники на дороге, а также создать высокие затраты на восстановление и поддержку системы, что выводит вопросы надежности передаваемых данных и обеспечения высокой производительности ИТС на первый план. Следует отметить, что указанные особенности находят свое решение при использовании механизмов кластеризации для развертывания придорожной инфраструктуры, а также применения граничных и туманных вычислений.

Отсутствие комплексных моделей предметной области, научно-обоснованных подходов, концепций, методов и алгоритмов целенаправленной деятельности по обеспечению требуемого уровня автоматизации ИТС и баланса между ключевыми характеристиками при работе V2X-технологий также препятствуют ее эффективному внедрению, что позволяет констатировать высокую научную значимость и актуальность решения обозначенной проблемы. Научная новизна исследований в области анализа V2X-систем заключается в учете условий, в которых функционирует ИТС, таких как ограниченные вычислительные ресурсы ТС и инфраструктуры ИТС, энергоэффективность и характеристики сети передачи данных. Поиск комплексной модели, которая позволяла бы распределять и прогнозировать параметры и ресурсы системы при различных вычислительных задачах, является основной задачей многих исследователей. Этот вопрос представляет существенную значимость при внедрении и использовании V2X-технологии. Исходя из этих соображений, далее в статье будет проведен аналитический обзор возможностей некоторых самых активно разрабатываемых методов и концепций, которые могут быть применены при решении задач повышения надежности, оптимизации времени доставки данных, устойчивости и ресурсообеспеченности V2X-системы.

Обзор релевантных работ

Проведем обзор научных публикаций отечественных и зарубежных ученых, посвященных задачам оптимизации ИТС. Поиск осуществлялся по базам РИНЦ, IEEE Xplorer, Scopus, Web of Science, а в качестве конкретных статей и результатов интеллектуальной деятельности отбирались наиболее релевантные запросам «V2X системы», «V2X clustering», «V2X edge computing» и «V2X FOG computing» с ретроспективой на глубину до 10 лет. Основная цель исследования состоит в определении концептуальной модели V2X-системы и наиболее значимых показателей качества обслуживания (QoS, аббр. от англ. Quality of Service) с учетом применения комплекса технологических решений для оптимизации V2X-системы, ориентируясь на опыт современных исследований в этой области. На основе детального анализа будут выбраны наиболее малоисследованные, но от этого не менее важные аспекты, оказывающие влияние на управляемость V2X-системы. В данном обзоре будет проведена систематизация результатов по следующим основным методам оптимизации: использование кластерного подхода, граничных и туманных вычислений. В качестве главных характеристик, по которым будет проводиться сравнение, были выбраны следующие направления: цель, ставящаяся исследователем; применяемый автором алгоритм или метод и используемый авторами аппарат исследования. Также отметим, что основной акцент в данном исследовании будет сделан на три элемента, входящие в QoS, предложенного в V2X White Paper [4]: время ожидания и коэффициент простоя (latency), время обработки и коэффициент искажения (throughput), коэффициент потери пакетов с данными (reliability).

Кластерный подход

Высокая нагрузка на V2X-систему влечет за собой большие временные затраты на передачу данных внутри ТС. Рост временных затрат требует поиска решений для оптимизации процессов обработки информации. Одним из самых распространенных и комплексных подходов к решению рассматриваемой проблемы является кластеризация. RSU (аббр. от англ. Road Side Unit, устройство, установленное на дорожной инфраструктуре) или OBU (аббр. от англ. On Board Unit, бортовое устройство) объединяют в группы с общим кэшем с целью минимизации затрат на обслуживание запросов.

В работах [5–7] приведен подробный обзор применения кластерного подхода к решению задач в V2X-системах. Так, в работе [5] кластеризация находит применение в задачах повышения масштабируемости и надежности маршрутизации в сетях, частой проблемы в крупных городских сетях.

Авторы используют модифицированный под свои задачи популярный алгоритм кластеризации с наименьшим идентификатором и наибольшей степенью (LID/HD). В статье исследуются варианты проектирования, сделанные при разработке алгоритмов кластеризации, ориентированных на работу с V2X-сетями. В нем представлена таксономия методов, применяемых для решения проблем выбора главного элемента кластера, принадлежности и управления кластером, а также определены новые направления и последние тенденции в разработке этих алгоритмов. Кроме того, рассматриваются методы проверки эффективности кластеризации и выявляется ключевой недостаток – отсутствие возможности реалистичного моделирования автомобильных каналов. Авторы отмечают важность строгого и стандартизированного режима оценки производительности с использованием реалистичных моделей.

В работе авторов [6] изучены решения проблем высокой мобильности, низкой пропускной способности некоторых дорог и редкого распределения ТС на части дорог. Проведен анализ различных проблем и существующих решений, использующих механизм кластеризации по параметрам (плотность, скорость и географическое расположение ТС) в сетях VANET (аббр. от англ. Vehicular Ad Hoc Network). Основной вклад авторов состоит в подробном описании формулировки проблем, существующих их решениях и направлениях дальнейших исследований. В статье приводится всесторонний анализ существующих предложений в литературе относительно ряда параметров, таких как выбранная топология, дополнительные требования к инфраструктуре, дорожный сценарий, мобильность узлов, обрабатываемые данные и относительное направление, плотность узлов, относительная скорость и режим связи. Анализ, проведенный для различных существующих предложений, позволяет различным пользователям, работающим в этой области, выбрать одно из предложений с учетом его преимуществ перед другими.

Авторы работы [7] применяют маршрутизацию на основе кластеров в качестве эффективного механизма, справляющегося с высокой динамикой, характерной для элементов V2X-систем. В статье предложена новая схема маршрутизации, названная кластеризацией на основе связности. Для выбора главы кластера и собственно его формирования вводится метрика на основе связности каналов. Последняя является функцией плотности, связывающая ТС и дальность передачи на основе возможности подключения. В качестве инструмента решения используется эвристический подход спектральной кластеризации для поиска оптимального количества кластеров. Выбор главы кластера проводится на основе геометрического

подхода, основанного на показателе максимальной собственной центральности рассматриваемого элемента. Приведенные результаты моделирования показывают, что предложенная схема кластеризации на основе связности хорошо работает при выборе оптимального количества кластеров, а также – сильно связанного маршрута. Авторами отмечается, что связность каналов и эвристический подход спектральной кластеризации являются ценными дополнениями к существующим схемам маршрутизации для быстроразвивающихся сетей.

В работе [8] рассматривается решение проблемы ограниченности диапазона сотовой связи для удовлетворения потребностей всех пользователей V2X-системы. Чтобы справиться с этой проблемой, предлагается эффективная схема управления ресурсами на основе кластеров. Далее проводится анализ ее производительности для выявления исключительных потребностей различных типов подключений в сети, а именно: V2V (*аббр. от англ. Vehicle-to-Vehicle*) и V2I (*аббр. от англ. Vehicle-to-Infrastructure*). Из-за высокой мобильности ТС возникает проблема быстрой потери сигнала, обусловленная высокой скоростью ТС и неидеальным сетевым покрытием. Авторы разработали эффективную технику управления ресурсами на основе кластеров для достижения разделения спектра и управления мощностью с учетом масштабных замираний. Предложены эффективные алгоритмы управления и выбора кластеров, которые обеспечивают оптимальное распределение ресурсов. В статье приведены алгоритмы, и их реализация. Моделирование проводилось в среде MATLAB в сочетании с сетевым симулятором NS3.26 (NS-3). Совместное использование обусловлено необходимостью сравнения различных метрик. Экспериментальные результаты показали, что предложенная эффективная схема управления ресурсами достигает хорошей производительности в различных сценариях, в частности, достигая наилучшего индекса приема пакетов, суммарного коэффициента пользователей сотовой связи, а также соотношения в условиях высокой плотности VANET.

Другое приложение кластерного подхода описывается авторами в работе [9]. Благодаря интеграции блокчейна в V2X-систему информация всех уровней детализации, от целых блоков до отдельных транзакций, становится доступной ТС. Основной вклад технологии блокчейн состоит в повышении безопасности и надежности передачи данных в V2X-сети. Кластерный подход применяется в данном случае для решения проблем, связанных с обеспечением совместимости и доступности данных в сети, решение проблем разгрузки задач. В то время как элементы транспортной сети пытаются сбалансировать нагрузку на сеть, ТС выбирают

ближайшие кластеры для выполнения задачи. Это может приводить к перегрузкам и непропорциональному использованию ресурсов автомобильной сети. Авторы проводят анализ теоретико-игрового подхода для балансировки нагрузки на кластеры и сохранения баланса между разгружаемыми ТС. Результаты моделирования, полученные с помощью авторской системы разгрузки, показывают более высокую производительность по сравнению с традиционными методами выбора ближайшего кластера. Отмечается также, что проблема масштабирования сети блокчейн по-прежнему остается сложной проблемой.

Работа [10] посвящена описанию новой схемы распределения ресурсов с поддержкой V2V. Основная идея заключается в том, что V2V-коммуникации на основе технологии сотовой связи между ТС устранивают задержки и позволяют повысить эффективность обмена данными на больших расстояниях. В частности, предлагается новая гибридная архитектура, в которой каждое ТС периодически проверяет необходимость обновления своих пакетов. Проблема оптимального распределения ресурсов решается благодаря выбору оптимального набора ТС-приемников для определения V2V-связей и выделения оптимальных ресурсов. В качестве алгоритма решения поставленных задач используется подход, основанный на выборе максимального взвешенного независимого множества (MWIS-AW). Эта задача является NP-трудной. Авторами предложен аналитический подход к моделированию ожидаемой задержки и коэффициента доставки пакетов с использованием программ SUMO и MATLAB.

Отдельные решения по кластеризации получены в работах [11–13]. Так, в исследовании [11] применен алгоритм кластеризации FOREL с целью минимизации задержки доставки данных. Основная задача исследования была направлена на решение проблемы выбора размера кластера в сети со сверхмалой задержкой. Авторами предложен метод выбора размера цифрового кластера в сети с ультранизкой задержкой с учетом длины соединительных линий. Дополнительно можно отметить, что полученная архитектура не позволяет учесть проблемы, связанные с организацией прокладки кабельных линий, которые не всегда могут быть заданы прямыми линиями.

В [12] предложено использовать спектральную кластеризацию. Объектами изучения являются связи «ТС – инфраструктура» и «ТС – ТС» в сценарии многополосной автомагистрали, где покрытие обеспечивается сетью RSU. Предлагается механизм оптимального выбора ТС, имеющих качественную связь с RSU, что позволяет разгрузить ТС с низким показателем сигнал-шум. Приведены численные результаты моделирования, демонстрирующие

значительное улучшение общей производительности динамической системы. Решение проведено с использованием подхода, основанного на численном анализе с использованием авторского софта.

В работе [13] была рассмотрена модель города, в которой основное внимание уделялось влиянию упреждающего кэширования на некластеризованные и кластеризованные схемы. Авторами было показано, что последние являются более эффективными в случае, если в кластер входит больше RSU. Отмечается, что при этом увеличивается зона покрытия, но растет задержка при передаче информации. В этой связи является важным проверить, позволит ли кластеризация свести к минимуму общую задержку вычислений на граничных устройствах.

Ранняя работа авторов обзора [14] также была посвящена решению задачи минимизации потерь пакетов в сети VANET при взаимодействии ее элементов между собой. Анализ проводился с использованием авторской компьютерной программы [15], написанной на языке Python. Результаты моделирования позволили доказать, что кластеризация RSU в блоки с общим кэшем позволяет значительно снизить потери и повысить эффективность работы динамической системы.

Граничные вычислители

Вычисления, проводимые на границе ТС, или граничные вычисления (VEC, аббр. от англ. Vehicular Edge Computing), стали перспективной парадигмой для предоставления и управления услугами в V2X-системах [16]. Они позволяют обеспечить низкую задержку за счет приближения вычислительных ресурсов к ТС. Однако высокая динамичность автомобильных сетей создает значительные трудности при разработке оптимальной схемы предоставления услуг V2X, обеспечивая при этом безопасность и своевременное предоставление услуг.

Для решения обозначенных проблем в работе [17] предлагается новая система граничных автомобильных вычислений с поддержкой блокчейна (BEVEC), которая использует двухуровневый процесс проверки с правом доступа для обеспечения точности и целостности данных. Для измерения производительности BEVEC разработана новая функция полезности системы, которая также служит основой для механизма поиска баланса. Для оптимизации этой функции предлагается алгоритм глубокого обучения с усилением (DRL), позволяющий своевременно предоставлять информацию в BEVEC. Результаты моделирования демонстрируют эффективность предложенного алгоритма по сравнению с существующими подходами. В среднем применение метода позволяет сократить задержку на 18 %, повысить успешность предоставления

услуг на 38 % и снизить энергопотребление на 65 %.

Управление ресурсами имеет большое значение для повышения производительности V2X-системы. В статье [18] предлагается схема совместной загрузки задач и распределения ресурсов для минимизации общей задержки обработки задач всеми ТС за счет планирования, распределения каналов связи и оптимальный подбор вычислительных ресурсов для OBU и RSU. Главным отличием рассматриваемой работы, как отмечается авторами, является: 1) модель учитывает разнообразие задач, профилируя запросы ТС по нескольким атрибутам, включая размер данных, объем вычислений, допустимую задержку и тип задачи; 2) учитывается классификация ТС, проводится их разделение на 4 набора в зависимости от того, имеют они требования к разгрузке задач или предоставляют услуги по обработке; 3) учитывается гибкость подхода к обработке данных, принимая решение для каждого ТС обрабатывать свои задачи локально, выгружать задачи на RSU через соединения V2I или на другие ТС через соединения V2V. Для решения задачи оптимизации разработан алгоритм, основанный на методах обобщенной декомпозиции Бендерса (GBD) и линейаризации перестроения (RL). Также разработан эвристический алгоритм для получения субоптимального решения с низкой вычислительной сложностью. Проведен анализ сходимости и сложности предложенных алгоритмов, и проведено обширное моделирование в 6 сценариях. Результаты моделирования демонстрируют превосходство предложенной схемы по сравнению с 4 другими известными подходами к решению обозначенных задач.

В работе [19] рассматривается задача совместной загрузки вычислений и распределения ресурсов в V2X-сети. Авторы предлагают иерархическую сеть MEC/C-V2X, которая учитывает динамические изменения в автомобильной сети и разнообразие моделей загрузки данных. Предложена модель совместной загрузки вычислений, которая поддерживает несколько различных вариантов. В основе подхода лежит анализ марковских процессов принятия решений с использованием алгоритмов глубокого обучения (ORAD).

Рост интенсивности вычислений и чувствительных к задержкам бортовых приложений делает довольно сложной задачу обработки данных непосредственно на ТС при сохранении необходимого уровня вычислительных мощностей, а значит, и производительности. Тем не менее, схемы загрузки, в которых все ТС перегружают свои задачи на один и тот же граничный сервер, могут тем самым ограничить производительность системы. В статье [20] предлагается интегрировать балансировку нагрузки с разгрузкой, и исследо-

вать распределение ресурсов для многопользовательской мультисерверной VEC-системы. На первом этапе формулируется совместная задача балансировки нагрузки и разгрузки как смешанная целочисленная задача нелинейного программирования для максимизации полезности системы. В частности, используется протокол IEEE 802.11p для моделирования набора параметров, отвечающих за полезность. Затем задача разделяется на две подпроблемы и разрабатывается алгоритм с низкой вычислительной сложностью для совместного выбора граничного вычислителя RSU и оптимизации разгрузки. Численные результаты, полученные на основе применения алгоритма JSO, приведенные авторами, показывают, что предложенный алгоритм демонстрирует быструю сходимость и показывает превосходную производительность в сравнении с существующими классическими решениями.

Авторы в работе [21] отмечают, что последнее время традиционные транспортные системы постепенно эволюционируют в сторону ИТС. ТС становятся все более умными и подключенными, появляется множество интеллектуальных приложений. Как следствие, появляется нехватка вычислительных мощностей автомобилей, что ведет к возникновению проблем с недостатком вычислительных мощностей для поддержки приложений из-за их требовательности к вычислениям. В связи с этим авторами предложена интеллектуальная схема разгрузки задач на основе глубокого Q-обучения, чтобы справиться с такой быстро меняющейся динамической системой, где программно-определяемая сеть внедряется для сбора информации и централизованного управления V2X-системой. Обширные численные результаты и анализ показывают, что предложенная схема не только обладает хорошей адаптивностью, но и может достичь высокой производительности по сравнению с традиционными схемами разгрузки.

Еще один интересный подход к решению задачи оптимизации функционирования V2X-системы на основе граничных вычислений предложен авторами работы [22]. Показано, что технология цифрового двойника (DT, *аббр. от англ. Digital Twin*) стала одним из способов управления связью между ТС и остальными элементами системы с использованием системы связи шестого поколения (6G). Главные преимущества использования DT включают следующие положения: укрепление взаимодействия человека и машины с помощью анализа поведения водителя, повышение безопасности движения с помощью диагностики неисправностей автомобиля на основе собираемых данных с датчиков, а также анализ пространственно-временных характеристик трафика с помощью сбора статистических данных.

Авторами [23] предлагается модель распределенного машинного обучения, в которой каждый элемент системы может индивидуально обучать локальные модели глубоких нейронных сетей (DNN, *аббр. от англ. Deep Neural Network*) на локальных данных, а затем совместно с другими участниками V2X-системы формировать глобальную модель на центральном сервере, позволяющую осуществлять качественное управление всей системой в целом. Модель приводится на основе анализа приложения по распознаванию изображений, которые позволят фиксировать информацию вокруг движущегося автомобиля и характеризовать текущую ситуацию на дороге по множеству параметров. Реализация построена на основе жадного алгоритма. Численные результаты, приведенные авторами, доказывают, что их подход достигает более высоких результатов по сравнению с базовыми подходами.

Задача эффективного планирования распределения ресурсов в условиях ограниченных возможностей коммуникаций рассматривается в работе [24]. Предполагается, что ТС могут «сотрудничать» между собой для совместных вычислений посредством связи между ними. Единая система связи, кэширование и совместные вычисления позволяют обеспечить минимизацию задержки. Чтобы вывести оптимальную стратегию управления, проводится объемное моделирование с использованием расширенного алгоритма глубокой Q-сети (DQN, *аббр. от англ. Deep Q Network*) с отдельной целевой Q-сетью. Моделирование проводится в программной среде Keras 2.3.1 (на основе TensorFlow) с использованием Python 3.7 на Ubuntu 16.04.6 LTS.

В ранней работе авторов обзора [25] приведен анализ математической модели и ее численное решение для системы взаимодействия граничных устройств в традиционной конфигурации размещения придорожных устройств с использованием одно- и двухканального соединения между OBU и RSU. В качестве среды разработки и численного анализа модели используется программный продукт, созданный на базе игрового движка Godot. Результаты, полученные в данной работе, показывают, что каждая из предложенных моделей может быть эффективно реализована в мобильных узлах и позволит существенно сократить превышающее ожидания время обработки запросов для улучшения организации и алгоритмического обеспечения VANET. К тому же, наряду с этим показано, что разработанный подход позволяет эффективно расходовать электроэнергию при объединении RSU в кластеры с общим кэшем.

Элементы FOG

Понятие туманных вычислений (FOG, *аббр. от англ. Fog Computing*), также называемые перифе-

рийными вычислениями, было введено в 2011 г. из-за необходимости расширения облачных вычислений [26]. Многочисленные устройства ИТС одновременно подключаются к облаку и при этом система испытывает чрезмерную нагрузку. Основная идея FOG состоит в попытке перенести часть вычислительных задач ближе к «земле». Элементы тумана будут собирать необработанные данные (например, от датчиков), и вместо того, чтобы пересылать их на облачные серверы, будут выполнять обработку с использованием своих локальных вычислений [27–29]. Дополнительным преимуществом является то, что собранные данные, скорее всего, потребуются тем же устройствам, которые их сгенерировали, поэтому при локальной, а не удаленной обработке задержка между вводом и ответом минимизируется. В нашей работе под элементами тумана будут рассматриваться в том числе мобильные RSU (mRSU), речь о которых пойдет ниже.

Развертыванию стационарных RSU препятствуют несколько факторов, в том числе высокая стоимость, сложности при адаптации в существующую придорожную инфраструктуру, а также решение вопросов кооперации между государственным сектором, операторами связи и автомобильным бизнесом. Следует отдельно отметить ряд исследований, частично снимающих эти проблемы и направленных на использование ТС в качестве mRSU. Данный подход масштабируем и адаптируем к текущему трафику дорожного движения. Маршруты mRSU можно планировать таким образом, чтобы они пересекали самые сложные участки дорог, а наличие системы контроля маршрута дает в данном случае существенное преимущество. При этом динамическое масштабирование вычислительных мощностей на уровне придорожной сетевой инфраструктуры позволяет рассматривать mRSU в качестве элементов Fog.

Исследование [30] является одной из первых работ, посвященных развертыванию mRSU. Предлагается использовать самоорганизующийся сетевой подход, при котором определенные ТС служат в качестве RSU. Описанное решение основано на разработке локальных управляющих алгоритмов. Данная работа является, по большей части, постановочной, ее результаты показывают, что предлагаемый подход улучшает связность автомобильных сетей на ранних этапах развития V2X-технологии, а также позволяет ускорить ее внедрение, как более экономичного механизма развертывания специализированной придорожной инфраструктуры.

В обзорных работах [31, 32] на базе проведенного анализа существующих решений предложены основные подкатегории динамического развертывания RSU. К ним относятся: 1) специализированное (временное) использование ТС в качестве RSU

(mRSU); 2) припаркованные ТС в качестве RSU (park-mRSU); 3) пассажирский автотранспорт регулярных линий в качестве RSU (bus-mRSU); беспилотные летательные аппараты в качестве RSU (uav-mRSU).

Ограничимся в данном исследовании только наземной инфраструктурой динамического развертывания RSU и рассмотрим некоторые примеры проведенных исследований по указанным подкатегориям.

В исследовании [33] представлена модель связи ТС с RSU, содержащая как стационарные, так и mRSU. Результаты показывают, что даже при введении в схему 5 % mRSU от общего количества стационарных устройств, вероятность установления связи ТС увеличивается вдвое. Нужно учесть, что при отсутствии в системе mRSU вероятность установления связи резко снижается. Данную модель авторы предлагают использовать для увеличения дальности передачи, а также определения оптимальной доли mRSU.

В работе [34] был предложен адаптивный подход, позволяющий каждому mRSU решать, когда активировать свое подключение, в зависимости от состояния соседних mRSU и обычных ТС. Рассмотрена схема с развернутыми mRSU высокой плотности, в которой несколько активных mRSU генерируют множество управляющих сообщений для формирования магистральной сети mRSU.

Для доказательства NP-трудной задачи в статье сформулирован частный случай {0–1} задачи целочисленного линейного программирования. Авторы оценивают производительность предложенного подхода с точки зрения соотношения ТС, охваченных активными mRSU, и управляющих сообщений со служебными данными по сравнению со случаем неадаптивной конфигурации mRSU. По результатам моделирования авторы показали, что с точки зрения подключения, предложенный подход работает так же, как в случае включения всех неадаптивных mRSU.

Следует отметить, что предложенная модель была рассмотрена для простой схемы дороги. Однако в более сложных сценариях необходимо учитывать множество дополнительных факторов, таких как направление движения и фазы светофора, что требует более сложного управления режимами mRSU.

В работе [35] рассмотрено использование специализированных ТС в качестве mRSU для повышения эффективности распространения контента в автомобильных социальных сетях.

В целях минимизации количество запросов к базовой станции предлагается кэшировать данные в стационарных RSU и дополнительно использовать mRSU с кэшированным контентом. Чтобы

решить проблему размещения эша, была поставлена задача оптимизации. Моделируя схему движения mRSU как случай $\{0-1\}$ задачи о ранце (Knapsack Problem), была доказана ее трудноразрешимость и NP-трудность. Далее была выполнена аппроксимация поставленной задачи с помощью стратегии обучения по уменьшению ошибки и решена задача поиска оптимального пути mRSU с использованием метода Монте-Карло. Результаты моделирования показали повышение пропускной способности сети – на 6 % по сравнению с существующими алгоритмами распространения контента.

Несмотря на то, что использование специализированных ТС в качестве mRSU является практическим решением, позволяющим расширить зону покрытия стационарных RSU и обеспечить гибкость в зависимости от дорожной ситуации, следует отметить в качестве основных недостатков дополнительные затраты на создание специализированных ТС, а также трудности с постоянной коррекцией выбора маршрута mRSU для обслуживания заданного количества стандартных ТС.

В работе [36] был предложен самоорганизующийся сетевой подход, аналогичный [30], по задействованию припаркованных в городских районах ТС в качестве RSU (park-mRSU). Такой подход позволяет припаркованным ТС создавать онлайн-карты покрытия на основе мощности принимаемого сигнала и принимать решения, когда припаркованное ТС является park-mRSU. Авторы разработали жадный алгоритм, который ориентируется на максимальный охват сети, образованной припаркованными ТС. Этот алгоритм минимизирует количество ТС, которые необходимо активировать, учитывая препятствия и обеспечивает эффективное покрытие с помощью соседних припаркованных ТС. Результаты этого исследования показывают экономическую эффективность предложенного подхода, способного обеспечить достаточное покрытие, используя лишь небольшую часть ТС, припаркованных в городе. Между тем, в работе есть ряд существенных ограничений. Так, например, обмен картами покрытия осуществлялся только в пределах 1-hop-окрестности. Кроме этого, ввиду особенностей первоначальной настройки в городских районах, где припаркованные ТС существуют в любое время суток, отсутствует механизм мягкой передачи обслуживания и упреждающая замена активных park-mRSU в других условиях.

В работе [37] была предложена системная модель C-V2V-сети на основе park-mRSU и сформулирована задача оптимизации для максимизации энергоэффективности сети с припаркованными автомобилями. Поскольку предлагаемая задача представляла собой NP-трудную задачу смешанно-

целочисленного нелинейного программирования, она была переформулирована в две подзадачи: выбор park-mRSU и совместное распределение ресурсов. Для первой подзадачи представлен механизм обратного аукциона, стимулирующий использование припаркованных автомобилей как park-mRSU. Для второй подзадачи использовалось нелинейное дробное программирование для оптимизации мощности передачи, а также для получения схемы повторного использования канала. Алгоритмы оценивались на основе реальных сценариев с использованием SUMO. Численные результаты показали, что предлагаемый подход может как эффективно выбирать park-mRSU при низких затратах, так и достигать заданных характеристик системы с точки зрения энергоэффективности, использования спектра и покрытия сети по сравнению с другими эталонными алгоритмами.

В работе [38] проведено исследование по оптимальному размещению park-mRSU для C-V2X со случайными требованиями к вычислительным задачам и плотности трафика ТС. Была сформулирована проблема размещения park-mRSU как задача целочисленного линейного программирования для минимизации задержек при разгрузке вычислительных задач. Предложен алгоритм, комбинирующий стохастическое моделирование, искусственную нейронную сеть и метаэвристический алгоритм для определения местоположения на основе реальных данных о трафике ТС. Приведенные в работе результаты позволяют определенному количеству припаркованных ТС выступать в качестве park-mRSU как RSU-шлюз в течение определенного периода времени парковки. Численные результаты показывают, что припаркованные ТС, временно использующиеся как RSU-шлюзы, предоставляют достаточно вычислительных ресурсов и уменьшают общую задержку при разгрузке вычислительных задач. Приведенное сравнение скорости успешной доставки пакетов и общей пропускной способности при различной плотности ТС продемонстрировало лучшие результаты park-mRSU по сравнению со стационарными RSU на перекрестках. Между тем, стоит отметить, что объем приведенного исследования ограничен исследуемой зоной парковки. Кроме этого, модель размещения park-mRSU предусматривает, что определенное количество доступных ТС должны обязательно взаимодействовать в течение определенного периода времени во время парковки. Данные обстоятельства требуют уточнения предложенной модели при ее масштабировании.

Общественные транспортные средства (ОТС), такие как автобусы и такси, могут являться доступными ТС при создании mRSU. С предустановленным коммуникационным и вычислительным

оборудованием их можно использовать для обслуживания других ТС.

В работе [39] предложена автомобильная сеть на базе ОТС, оснащенных как bus-mRSU. Кроме этого, автобусы, такси и автовокзалы образуют магистральную линию LTE D2D для поддержки V2V-связи. В статье предлагается использовать нечеткую маршрутизацию для повышения производительности пересылки сообщений между ТС. Результаты моделирования показывают, что по сравнению с общепринятыми протоколами маршрутизации, в сетях VANET предлагаемое решение может эффективно повысить скорость доставки сообщений и сократить их задержку.

В работе [40] была предложена сеть BUS-VANET, использующая автобусы в качестве bus-mRSU. Сеть имеет двухуровневую архитектуру, где верхний уровень включает bus-mRSU и центр управления движением, а нижний уровень составляют стандартные ТС, оснащенные устройствами OBU. Когда узел нижнего уровня желает передать сообщение, он должен сначала зарегистрироваться на соседнем узле верхнего уровня, чтобы определить путь доставки в соответствии с алгоритмом маршрутизации на основе траектории, заданный узлом верхнего уровня. Результаты моделирования показали, что сеть BUS-VANET с пятью установленными bus-mRSU работает аналогично традиционной VANET с десятью стационарными RSU и при этом имеет наименьшую задержку и самый высокий коэффициент доставки пакетов. Тем не менее, в ситуации с разреженной дорожной сетью предложенный метод не учитывал услуги передачи, предоставляемые существующими стационарными RSU.

В работе [41] показано, как стационарные RSU могут быть заменены автобусами – bus-mRSU, чтобы минимизировать затраты на развертывание V2X-системы и максимизировать зону покрытия между ТС и придорожной инфраструктурой. Компромисс производительности и стоимости использования bus-mRSU решается с помощью математического анализа и проверяется реальными экспериментами. Однако масштаб эксперимента не может соответствовать масштабу моделирования из-за практических ограничений. В целом представленные в работе результаты дают основу для оценки того, выгодно ли дополнять стационарные RSU мобильными устройствами в зависимости от среды развертывания и соотношения цены и качества.

Кроме приведенных работ, следует отметить гибридные подходы развертывания mRSU [42, 43]. Так, в работе [43] предложена гибридная структура развертывания RSU, которая представляет собой комбинацию трех различных подходов: развертывание стационарных RSU, использование bus-

mRSU на ОТС и использование специализированных mRSU. Исследуется стратегия наилучшего развертывания RSU, чтобы их пространственно-временной охват был максимальным при ограниченном бюджете. Сформулирована оптимизационная задача и показана ее NP-трудность. Предложен новый полиномиальный алгоритм аппроксимации времени выполнения задачи и показано, что коэффициент производительности (отношение между качеством результата предлагаемого алгоритма и качеством наилучшего возможного решения) составляет как минимум половину наилучшего возможного решения. В работе представлены результаты моделирования предлагаемого подхода в различных условиях.

Концепция mRSU затрагивалась в работах авторов данного обзора [44, 45]. Здесь мобильные RSU выполняли роль RSU, динамически меняющих свое положение. В обоих исследованиях ставилась задача минимизации потерь данных при функционировании V2X-системы. Численный анализ системы без mRSU и после их внедрения показал, что использование mRSU значительно снижает нагрузку на сеть в целом. При этом численно доказано, что возможен полный отказ от стационарных RSU при выполнении ряда дополнительных ограничений. Подход к визуализации с использованием нагретой карты позволяет визуализировать результат более наглядно.

Поиск научных публикаций по указанным выше ключевым запросам показал критически малое количество отечественных исследований по сравнению с зарубежными.

Систематизация результатов

Осуществим систематизацию проведенных обзоров (таблица 1) путем их ранжирования с помощью следующего набора критериев:

- K₁ – год публикации, позволяющий оценить тенденции в предметной области;
- K₂ – подход к решению задачи;
- K₃ – основная цель, поставленная авторами (задача исследования);
- K₄ – основной используемый метод (алгоритм);
- K₅ – система моделирования.

Если информация по критерию отсутствует, будем ставить «---».

Отметим, что большая часть анализируемых решений имеет теоретическое обоснование или доведено до состояния работающего прототипа, при этом достаточно мало решений внедрено и реально используется на практике. Это, вероятно, дополнительно подтверждает мысль о том, что научное сообщество стремится создать рабочую модель, внедрение которой существенно упростит регулирование работы V2X-системы.

ТАБЛИЦА 1. Результаты систематизации обзоров научных публикаций

TABLE 1. Results of Systematizing Reviewing Scientific Publications

Название, ссылка	К_1	К_2	К_3	К_4	К_5
Comparative Survey of VANET Clustering Techniques [5]	2017	Cluster	улучшение масштабируемости и надежности маршрутизации в сети	Несколько методов и алгоритмов решения задачи	несколько различных сред моделирования
Clustering in vehicular ad hoc networks: taxonomy, challenges and solutions [6]	2014	Cluster	проблемы высокой мобильности и редкого распределения ТС	несколько методов и алгоритмов решения задачи	несколько различных сред моделирования
A Connectivity-Based Clustering Scheme for Intelligent Vehicles [7]	2021	Cluster	повышение надежности, стабильности и масштабируемости сети	эвристический подход спектральной кластеризации	SUMO 0.25.0, MATLAB R2015b
An Efficient Cluster Based Resource Management Scheme and its Performance Analysis for V2X Networks [8]	2020	Cluster	схема управления ресурсами на основе кластеров и анализ ее производительности для V2X-сетей	математический анализ	MATLAB сетевой симулятор NS3.26 (NS-3)
Efficient Mining Cluster Selection for Blockchain-Based Cellular V2X Communications [9]	2020	Cluster	минимизация задержки	математический анализ, блокчейн-технология	авторский софт
A novel low-latency V2V resource allocation scheme based on cellular V2X communications [10]	2018	Cluster	построение оптимальной схемы распределения ресурсов	жадный алгоритм	SUMO 0.25.0, MATLAB R2015b
An Efficient Method for choosing Digital Cluster Size in Ultralow Latency Networks [11]	2021	Cluster	минимизация задержки доставки данных	алгоритм кластеризации FOREL	Mathcad program
Vehicle clustering for improving enhanced LTE-V2X network performance [12]	2017	Cluster	разгрузка ТС с низким показателем сигнал-шум	спектральная кластеризация	Vienna LTE-A Downlink System Level Simulator
Proactive Caching for Vehicular Ad hoc Networks Using the City Model [13]	2019	Cluster	минимизация потерь данных	математический анализ	---
Numerical Analysis of the Mathematical Model of a Cluster V2X-System [14]	2023	Cluster	минимизация потерь данных	математический анализ	Python 3.7, Godot Engine
A Blockchain-Enabled Vehicular Edge Computing Framework for Secure Performance-oriented V2X Service Delivery [17]	2024	Edge	улучшения производительности BEVEC с точки зрения энергопотребления, задержки и успешности предоставления услуг	алгоритм DRL, названный 3DPER	BEVEC: Blockchain-Enabled Vehicular Edge Computing
Joint Task Offloading and Resource Allocation for Vehicular Edge Computing Based on V2I and V2V Modes [18]	2023	Edge	разгрузка и распределение ресурсов для минимизации общей задержки обработки задач	алгоритм, основанный на GBD и RL	MATLAB simulator
Joint computation offloading and resource allocation based on deep reinforcement learning in C-V2X edge computing [19]	2023	Edge	задача совместной оптимизации разгрузки вычислений и распределения ресурсов в сети	математический анализ, марковские процессы, алгоритм ORAD	Python 3.7 with the PyTorch framework to implement the DNN networks with the Adam optimizer
Joint Load Balancing and Offloading in Vehicular Edge Computing and Networks [20]	2019	Edge	интеграция балансировки нагрузки с разгрузкой, и исследование распределения ресурсов для многопользовательской мультисерверной VEC-системы	алгоритм JSCO	Rayleigh fading model, MathLab
Intelligent Task Offloading in Vehicular Edge Computing Networks [21]	2020	Edge	оптимальная разгрузка задач с минимизацией задержек	схема разгрузки задач на основе глубокого Q-обучения	авторский софт
Task-Efficiency Oriented V2X Communications: Digital Twin Meets Mobile Edge Computing [22]	2023	Edge	укрепление взаимодействия человека и машины, повышение безопасности движения, анализ пространственно-временных характеристик трафика	DT-технология	симулятор движения на базе SUMO

Название, ссылка	K_1	K_2	K_3	K_4	K_5
Federated Learning in Vehicular Edge Computing: A Selective Model Aggregation Approach [23]	2020	Edge	повышение уровня управляемости V2X-системы в целом	анализ локальных моделей DNN, принцип объединенного обучения, оригинальный алгоритм	MATLAB simulator
Collaborative Data Scheduling for Vehicular Edge Computing via Deep Reinforcement Learning [24]	2020	Edge	минимизация задержки	расширенный алгоритм DQN с отдельной целевой Q-сетью	Keras 2.3.1 (на основе TensorFlow), Python 3.7
Cluster-Based Vehicle-to-Everything Model with a Shared Cache [25]	2023	Edge	сокращение времени ожидания обработки запросов	математический анализ, численное моделирование	Python 3.7, Godot Engine
How mobile RSUs can enhance communications in VANETs? [33]	2018	Fog (mRSU)	максимизация сетевого покрытия	математический анализ	численный анализ
Adaptive configuration of mobile roadside units for the cost-effective vehicular communication infrastructure [34]	2019	Fog (mRSU)	максимизация сетевого покрытия	решение задачи {0-1} ILP	SUMO (Veins), OMNet++
Social-aware mobile road side unit for content distribution in vehicular social networks [35]	2019	Fog (mRSU)	повышение скорости доставки пакетов	решения задачи {0-1} Knapsack problem	SUMO, Mininet
Parked cars are excellent roadside units [36]	2017	Fog (park-mRSU)	максимизация сетевого покрытия	самоорганизующаяся сеть, Greedy-алгоритм	SUMO, Специализированное ПО
Energy-efficient resource allocation for parked-cars-based cellular-V2V heterogeneous networks [37]	2022	Fog (park-mRSU)	энергоэффективность, максимизация сетевого подключения	решение задачи оптимизации для максимизации энергоэффективности сети	SUMO, MATLAB, OpenStreetMap
Optimal exploitation of on-street parked vehicles as roadside gateways for social IoV—a case of Kigali City [38]	2020	Fog (park-mRSU)	минимизация задержки	решение задачи ILP	SUMO, NS3, OpenStreetMap
Routing in taxi and public transport based heterogeneous vehicular networks [39]	2016	Fog (bus-mRSU)	повышение скорости доставки пакетов, минимизация задержки	алгоритм нечеткой маршрутизации	The Opportunistic Network Environment simulator (ONE)
Bus-VANET: A bus vehicular network integrated with traffic infrastructure [40]	2015	Fog (bus-mRSU)	минимизация потерь пакетов, минимизация задержки	математический анализ	SUMO, NS3
Performance-cost tradeoff of using mobile roadside units for V2X communication [41]	2019	Fog (bus-mRSU)	максимизация сетевого покрытия	математический анализ	SUMO, NS3
A new comprehensive RSU installation strategy for cost-efficient VANET deployment [42]	2016	Fog (hybrid RSU)	экономическая эффективность, минимизация задержки	полиномиальный алгоритм аппроксимации времени выполнения задачи	SUMO, Open Street Map, Visual studio 2015
Hybrid RSU management in cybertwin-IoV for temporal and spatial service coverage [43]	2022	Fog hybrid RSU	экономическая эффективность	решение задачи максимизации полезности с ограничениями покрытия	MATLAB
Performance Evaluation of V2X Model with a Mobile Road Side Units [44]	2023	Fog mRSU	минимизация потерь данных	математический анализ	Python 3.7, Godot Engine
Numerical Analysis of roadside Units Deployment Models in V2X Communication System [45]	2024	Fog mRSU	минимизация потерь данных	математический анализ	Python 3.7, Godot Engine

Исходя из результатов сравнительного анализа обзоров (см. таблицу 1), можно сделать следующие выводы по каждому из критериев.

Во-первых (по критерию К_1), публикационная активность имеет характерный стабильно высокий уровень интереса со стороны научного сообщества. Отсутствие комплексно решенной задачи дает возможность смело предположить, что в будущем интерес к моделям V2X-систем будет только расти, поскольку необходимость автоматизации управления системой дорожного движения не теряет своей актуальности.

Во-вторых (по критерию К_2), рассмотренные три наиболее популярных подхода к решению задач оптимизации V2X-систем остаются актуальными на протяжении последних десяти лет, поэтому можно считать, что каждый из них будет в дальнейшем развиваться. При этом будущее, на наш взгляд, за туманными вычислениями, по той причине, что эта концепция является самой новой и перспективной, с учетом появления новых технических разработок в сфере ИТС.

В-третьих (по критерию К_3), несмотря на то, что класс решаемых задач оптимизации V2X-систем достаточно широк, основной интерес представляют задачи минимизации потерь при передаче данных, уменьшении задержек, построении энергоэффективной системы и повышении надежности и стабильности системы в целом. При этом почти во всех рассмотренных научных публикациях отмечается необходимость создания именно комплексной модели управления V2X-системой.

В-четвертых (по критерию К_4), в большинстве публикаций используются классические подходы к решению оптимизационных задач, затрагивающие такие разделы математики, как математический анализ, теория вероятностей и экстремальные задачи, а также некоторые элементы теории алгоритмов, эвристический, жадный или алгоритмы глубокого обучения. Можно дополнительно отметить, что метод зачастую выбирается на основе содержания той задачи, которую необходимо решить, то есть каждый подход имеет свои преимущества и недостатки.

В-пятых (по критерию К_5), средств для моделирования процессов, возникающих при работе с V2X-системами, достаточно много. Какого-либо существенного преимущества одной программной среды перед другой в процессе подготовки обзора не было выявлено. Стоит отметить, что наиболее популярной программой для моделирования можно считать программу MATLAB в кооперации с программой визуализации SUMO. Программные средства, созданные самими исследователями, реализуются в основном на языке программирования Python. При этом все подходы к проведению моделирования имеют право на существование.

Результаты анализа

На основании приведенного анализа публикаций, их систематизации, а также авторского опыта предлагается концептуальная модель организации V2X-системы, основанная на следующих принципах.

Принцип 1. RSUs и mRSUs будут выступать в роли туманных узлов и обладать вычислительными возможностями граничных серверов, позволяющими обслуживать задачи OBUs, находящиеся в их зоне покрытия. Элементы OBU, в свою очередь, будут пониматься как туманные узлы второго типа, обслуживаемыми элементами системы, обладающие высокой мобильностью и значительно меньшими вычислительными способностями. Вычислительные задачи, превышающие вычислительные возможности граничных серверов, переносятся для решения в облако. Таким образом рассматривается трехэлементная архитектура V2X-системы: OBU-RSU/mRSU-CLOUD, – представленная на рисунке 1. Это идея позволяет построить трехуровневую систему, предложенную в качестве гипотезы в [45].



Рис. 1. Трехуровневая схема V2X системы

Fig. 1. Three-Level V2X System Scheme

Принцип 2. В основе построения комплексной V2X-системы должны лежать, по классификации [4], следующие оптимизируемые параметры: покрытие (coverage), задержка (latency), надежность (reliability), пропускная способность (throughput), дальность связи (communication range), скорость (velocity) и мульти-операторская работа (multi-operator's operation).

В таблице 2 приведено число публикаций, посвященных анализу каждого из оптимизируемых параметров. В нашем обзоре параметры понимаются как задачи исследования (критерий K_3).

ТАБЛИЦА 2. Анализ публикаций по параметрам оптимизации

TABLE 2. Analysis of Publications on Optimization Parameters

Оптимизационные параметры (задачи исследования)	Cluster	Edge	FOG
покрытие	2	1	3
задержка	2	5	4
надежность	4	3	4
пропускная способность	4	4	3
дальность связи	2	–	1
скорость	1	1	2
мультиоператорская работа	1	3	2

По результатам анализа таблицы можно сделать вывод, что поиск программно-оптимизационных решений должен вестись по трем основным параметрам обозначенного списка: задержка, надежность (в смысле потерь данных и энергозатрат) и пропускная способность. По остальным параметрам исследования проводятся реже в силу особой специфики задач, а также возможности пе-

рехода на более современное оборудование, которое позволяет частично решать проблему за счет совершенствования элементной базы.

Заключение

В работе проведен обзор научных публикаций, посвященных оптимизации V2X-систем. Произведен сравнительный анализ обзоров (и их результатов), который позволил сделать систематизированные выводы касательно:

- актуальности и перспективности исследований в данной области;
- преимуществ и недостатков реализации той или иной модели и метода ее решения.

Исходя из результатов сравнительного анализа, были сделаны обобщенные выводы, которые послужили отправной точкой к реализации концептуальной модели V2X-системы, основанной на указанных принципах. Результаты исследования могут быть использованы при проектировании и развертывании V2X-систем.

Продолжением исследования должна стать последовательная реализация комплексной модели, основанной на вышеизложенных принципах.

Список источников

1. Mueck M., Karls I. Networking Vehicles to Everything: Evolving Automotive Solutions. Walter de Gruyter, 2018. 233 p.
2. Chen S, Hu J., Zhao L., Zhao R., Fang J., Shi Y., Xu H. Cellular Vehicle-to-Everything (C-V2X). Wireless Networks. Springer, 2023. 416 p.
3. Wang J., Shao Y., Ge Y., Yu R. A survey of vehicle to everything (V2X) testing // Sensors. 2019. Vol. 19. Iss. 2. P. 334. DOI:10.3390/s19020334
4. V2X White Paper. Next Generation Mobile Networks Ltd.: San Jose, 2018.
5. Cooper C., Franklin D., Ros M., Safaei F., Abolhasan M. A Comparative Survey of VANET Clustering Techniques // IEEE Communications Surveys and Tutorials. 2017. Vol. 19. Iss. 1. PP. 657–681. DOI:10.1109/COMST.2016.2611524
6. Bali R.S., Kumar N., Rodrigues J.J. Clustering in vehicular ad hoc networks: taxonomy, challenges and solutions // Vehicular Communications. 2014. Vol. 1. Iss. 3. PP. 134–152. DOI:10.1016/j.vehcom.2014.05.004
7. Khan Z., Koubaa A., Fang S., Lee M.Y., Muhammad K. A Connectivity-Based Clustering Scheme for Intelligent Vehicles // Applied Sciences. 2021. Vol. 11. Iss. 5. P. 2413. DOI:10.3390/app11052413
8. Abbas F., Liu G. Fan P., Khan Z. An efficient cluster-based resource management scheme and its performance analysis for V2X networks // IEEE Access. 2020. Vol. 8. PP. 87071–87082. DOI:10.1109/ACCESS.2020.2992591
9. Jameel F., Javed M.A., Zeadally S., Jantti R. Efficient Mining Cluster Selection for Blockchain-Based Cellular V2X Communications // IEEE Transactions on Intelligent Transportation Systems. 2021. Vol. 22. Iss. 7. PP. 4064–4072. DOI:10.1109/TITS.2020.3006176
10. Abbas F., Fan P., Khan Z. A novel low-latency V2V resource allocation scheme based on cellular V2X communications // IEEE Transactions on Intelligent Transportation Systems. 2019. Vol. 20. Iss. 6. PP. 2185–2197. DOI:10.1109/TITS.2018.2865173
11. Paramonov A., Khayyat M., Chistova N., Muthanna A., Elgendy I.A., Koucheryavy A., et al. An Efficient Method for choosing Digital Cluster Size in Ultralow Latency Networks // Wireless Communications and Mobile Computing. 2021. Vol. 2021. P. 9188658. DOI:10.1155/2021/9188658
12. Luoto P., Bennis M., Pirinen P., Samarakoon S., Horneman K., Latvaaho M. Vehicle clustering for improving enhanced LTE-V2X network performance // Proceedings of the European Conference on Networks and Communications (EuCNC, Oulu, Finland, 12–15 June 2017). IEEE, 2017. DOI:10.1109/EuCNC.2017.7980735
13. AlNagar Y., Hosny S., El-Sherif A.A. Proactive Caching for Vehicular Ad hoc Networks Using The City Model // Proceedings of the Wireless Communications and Networking Conference Workshop (WCNCW, Marrakech, Morocco, 15–18 April 2019). IEEE, 2019. DOI:10.1109/WCNCW.2019.8902590
14. Плотников П.В., Владыко А.Г. Численный анализ математической модели кластерной V2X-системы // Труды учебных заведений связи. 2023. Т. 9. № 1. С. 14–23. DOI:10.31854/1813-324X-2023-9-1-14-23. EDN:JDPDSD
15. Плотников П.В., Тамбовцев Г.И., Владыко А.Г. Программный модуль моделирования взаимодействия граничных устройств в сети VANET с одно- и двухканальным подключением. Свидетельство о регистрации программы для ЭВМ № RU 2023681939 от 06.10.2023. Оpubл. 19.10.2023. EDN:EYFCRR
16. Liu L., Chen C., Pei Q., Maharjan S., Zhang Y. Vehicular edge computing and networking: A survey // Mobile Networks and Applications. 2021. Vol. 26. PP. 1145–1168. DOI:10.1007/s11036-020-01624-1

17. Fardad M., Muntean G.M., Tal I. A Blockchain-Enabled Vehicular Edge Computing Framework for Secure Performance-oriented V2X Service Delivery // *IEEE Transactions on Vehicular Technology*. 2024. DOI:10.1109/TVT.2024.3394150
18. Fan W., Su Y., Liu J., Li S., Huang W., Wu F., Liu Y. Joint Task Offloading and Resource Allocation for Vehicular Edge Computing Based on V2I and V2V Modes // *IEEE Transactions on Intelligent Transportation Systems*. 2023. Vol. 24. Iss. 4. PP. 4277–4292. DOI:10.1109/TITS.2022.3230430
19. Hou, P., Jiang, X., Lu, Z. et al. Joint computation offloading and resource allocation based on deep reinforcement learning in C-V2X edge computing // *Applied Intelligence*. 2023. Vol. 53. PP. 22446–22466. DOI:10.1007/s10489-023-04637-x
20. Dai Y., Xu D., Maharjan S., Zhang Y., Joint Load Balancing and Offloading in Vehicular Edge Computing and Networks // *IEEE Internet of Things Journal*. 2019. Vol. 6. Iss. 3. PP. 4377–4387. DOI:10.1109/JIOT.2018.2876298
21. Guo H., Liu J., Ren J., Zhang Y. Intelligent Task Offloading in Vehicular Edge Computing Networks // *IEEE Wireless Communications*. 2020. Vol. 27. Iss. 4. PP. 126–132. DOI:10.1109/MWC.001.1900489
22. Cai G., Fan B., Dong Y., Li T., Wu Y., Zhang Y. Task-Efficiency Oriented V2X Communications: Digital Twin Meets Mobile Edge Computing // *IEEE Wireless Communications*. 2024. Vol. 31. Iss. 2. PP. 149–155. DOI:10.1109/MWC.012.2200465
23. Ye D., Yu R., Pan M., Han Z. Federated Learning in Vehicular Edge Computing: A Selective Model Aggregation Approach // *IEEE Access*. 2020. Vol. 8. PP. 23920–23935. DOI:10.1109/ACCESS.2020.2968399
24. Luo Q., Li C., Luan T.H., Shi W. Collaborative Data Scheduling for Vehicular Edge Computing via Deep Reinforcement Learning // *IEEE Internet of Things Journal*. 2020. Vol. 7. Iss. 10. PP. 9637–9650. DOI:10.1109/JIOT.2020.2983660
25. Vladyko A., Tambovtsev G., Podgornaya E., Chelloug S.A., Alkanhel R., Plotnikov P. Cluster-Based Vehicle-to-Everything Model with a Shared Cache // *Mathematics*. 2023. Vol. 11. Iss. 13. P. 3017. DOI:10.3390/math11133017
26. Bonomi F. Connected vehicles, the internet of things, and fog computing // *Proceedings of the Eighth ACM International Workshop on Vehicular Inter-NETworking (VANET 2011, 23 September 2011, Las Vegas, USA)*. 2011.
27. Khattak H.A., Islam S.U., Din I.U., Guizani M. Integrating fog computing with VANETs: A consumer perspective // *IEEE Communications Standards Magazine*. 2019. Vol. 3. Iss. 1. PP. 19–25. DOI:10.1109/MCOMSTD.2019.1800050
28. Sarrigiannis I., Contreras L.M., Ramantas K., Antonopoulos A., Verikoukis C. Fog-Enabled Scalable C-V2X Architecture for Distributed 5G and Beyond Applications // *IEEE Network*. 2020. Vol. 34. Iss. 5. PP. 120–126. DOI:10.1109/MNET.111.2000476
29. Alvi A.N., Javed M.A., Hasanat M.H.A., Khan M.B., et al. Intelligent task offloading in fog computing based vehicular networks // *Applied Sciences*. 2022. Vol. 12. Iss. 9. P. 4521. DOI:10.3390/app12094521
30. Tonguz O.K., Viriyasitavat W. Cars as roadside units: A self-organizing network solution // *IEEE Communications Magazine*. 2013. Vol. 51. Iss. 12. PP. 112–120. DOI:10.1109/MCOM.2013.6685766
31. Karunathilake T., Forster A. A survey on mobile road side units in VANETs // *Vehicles*. 2022. Vol. 4. Iss. 2. PP. 482–500. DOI:10.3390/vehicles4020029
32. Guerna A., Bitam S., Calafate C.T. Roadside unit deployment in internet of vehicles systems: A survey // *Sensors*. 2022. Vol. 22. Iss. 9. P. 3190. DOI:10.3390/s22093190
33. Ercan S., Ayaida M., Messai N. How mobile RSUs can enhance communications in VANETs? // *Proceedings of the 6th International Conference on Wireless Networks and Mobile Communications (WINCOM, Marrakesh, Morocco, 16–19 October 2018)*. IEEE, 2018. DOI:10.1109/WINCOM.2018.8629641
34. Lee J., Ahn S. Adaptive configuration of mobile roadside units for the cost-effective vehicular communication infrastructure // *Wireless Communications and Mobile Computing*. 2019. Vol. 2019. P. 6594084. DOI:10.1155/2019/6594084
35. Bitagsir S.A., Kashipazha S., Dadlani A., Khonsari A. Social-aware Mobile Road Side Unit for Content Distribution in Vehicular Social Networks // *Proceedings of the Symposium on Computers and Communications (ISCC, Barcelona, Spain, 29 June 2019 – 03 July 2019)*. IEEE, 2019. DOI:10.1109/ISCC47284.2019.8969669
36. Reis A.B., Sargento S., Tonguz O.K. Parked cars are excellent roadside units // *IEEE Transactions on Intelligent Transportation Systems*. 2017. Vol. 18. Iss. 9. PP. 2490–2502. DOI:10.1109/TITS.2017.2655498
37. Qin P., Fu Y., Feng X., Zhao X., Wang S., Zhou Z. Energy-efficient resource allocation for parked-cars-based cellular-V2V heterogeneous networks // *IEEE Internet of Things Journal*. 2022. Vol. 9. Iss. 4. P. 3046–3061. DOI:10.1109/JIOT.2021.3094903
38. Evariste T., Kasakula W., Rwigema J., Datta R. Optimal exploitation of on-street parked vehicles as roadside gateways for social IoV – a case of Kigali City // *Journal of Open Innovation: Technology, Market, and Complexity*. 2020. Vol. 6. Iss. 3. P. 73. DOI:10.3390/joitmc6030073
39. Li G., Ma M., Liu C., Shu Y. Routing in taxi and public transport based heterogeneous vehicular networks // *Proceedings of the IEEE Region 10 Conference (TENCON, Singapore, Singapore, 22–25 November 2016)*. IEEE, 2019. PP. 1863–1866. DOI:10.1109/TENCON.2016.7848344
40. Jiang X., Du D.H.C. Bus-VANET: A bus vehicular network integrated with traffic infrastructure // *IEEE Intelligent Transportation Systems Magazine*. 2015. Vol. 7. Iss. 2. P. 47–57. DOI:10.1109/MITS.2015.2408137
41. Heo J., Kang B., Yang J.M., Paek J., Bahk S. Performance-cost tradeoff of using mobile roadside units for V2X communication // *IEEE Transactions on Vehicular Technology*. 2019. Vol. 68. Iss. 9. PP. 9049–9059. DOI:10.1109/TVT.2019.2925849
42. Kim D., Velasco Y., Wang W., Uma R.N., Hussain R., Lee S. A new comprehensive RSU installation strategy for cost-efficient VANET deployment // *IEEE Transactions on Vehicular Technology*. 2016. Vol. 66. Iss. 5. PP. 4200–4211. DOI:10.1109/TVT.2016.2598253
43. Ni Y., Zhao C., Cai L. Hybrid RSU management in cybertwin-IoV for temporal and spatial service coverage // *IEEE Transactions on Vehicular Technology*. 2022. Vol. 71. Iss. 5. P. 4596–4606. DOI:10.1109/TVT.2021.3138749
44. Plotnikov P.V., Tambovtsev G.I., Vladyko A.G. Performance Evaluation of V2X Model with a Mobile Road Side Units // *Proceedings of the Intelligent Technologies and Electronic Devices in Vehicle and Road Transport Complex (TIRVED, Moscow, Russian Federation, 15–17 November 2023)*. IEEE, 2023. DOI:10.1109/TIRVED58506.2023.10332617

45. Plotnikov P.V., Tambovtsev G.I., Vladyko A.G. Numerical Analysis of roadside Units Deployment Models in V2X Communication System // Proceedings of the Systems of Signals Generating and Processing in the Field of on Board Communications (Moscow, Russian Federation, 12–14 March 2024). IEEE, 2024. DOI:10.1109/IEEECONF60226.2024.10496720

References

1. Mueck M., Karls I. *Networking Vehicles to Everything: Evolving Automotive Solutions*. Walter de Gruyter; 2018. 233 p.
2. Chen S, Hu J, Zhao L, Zhao R, Fang J, Shi Y, Xu H. *Cellular Vehicle-to-Everything (C-V2X)*. *Wireless Networks*. Springer; 2023. 416 p.
3. Wang J, Shao Y, Ge Y, Yu R. A survey of vehicle to everything (V2X) testing. *Sensors*. 2019;19(2):334. DOI:10.3390/s19020334
4. *V2X White Paper*. Next Generation Mobile Networks Ltd.: San Jose; 2018.
5. Cooper C., Franklin D., Ros M., Safaei F., Abolhasan M. A Comparative Survey of VANET Clustering Techniques. *IEEE Communications Surveys and Tutorials*. 2017;19(1):657–681. DOI:10.1109/COMST.2016.2611524
6. Bali R.S., Kumar N., Rodrigues J.J. Clustering in vehicular ad hoc networks: taxonomy, challenges and solutions. *Vehicular Communications*. 2014;1(3):134–152. DOI:10.1016/j.vehcom.2014.05.004
7. Khan Z., Koubaa A., Fang S., Lee M.Y., Muhammad K. A Connectivity-Based Clustering Scheme for Intelligent Vehicles. *Applied Sciences*. 2021;11(5):2413. DOI:10.3390/app11052413
8. Abbas F., Liu G. Fan P., Khan Z. An efficient cluster based resource management scheme and its performance analysis for V2X networks. *IEEE Access*. 2020;8:87071–87082. DOI:10.1109/ACCESS.2020.2992591
9. Jameel F., Javed M.A., Zeadally S., Jantti R. Efficient Mining Cluster Selection for Blockchain-Based Cellular V2X Communications. *IEEE Transactions on Intelligent Transportation Systems*. 2021;22(7):4064–4072. DOI:10.1109/TITS.2020.3006176
10. Abbas F., Fan P., Khan Z. A novel low-latency V2V resource allocation scheme based on cellular V2X communications. *IEEE Transactions on Intelligent Transportation Systems*. 2019;20(6):2185–2197. DOI:10.1109/TITS.2018.2865173
11. Paramonov A., Khayyat M., Chistova N., Muthanna A., Elgendy I.A., Koucheryavy A., et al. An Efficient Method for choosing Digital Cluster Size in Ultralow Latency Networks. *Wireless Communications and Mobile Computing*. 2021;2021:9188658. DOI:10.1155/2021/9188658
12. Luoto P., Bennis M., Pirinen P., Samarakoon S., Horneman K., Latvaaho M. Vehicle clustering for improving enhanced LTE-V2X network performance. *Proceedings of the European Conference on Networks and Communications, EuCNC, 12–15 June 2017, Oulu, Finland*. IEEE; 2017. DOI:10.1109/EuCNC.2017.7980735
13. AlNagar Y., Hosny S., El-Sherif A.A. Proactive Caching for Vehicular Ad hoc Networks Using The City Model. *Proceedings of the Wireless Communications and Networking Conference Workshop, WCNCW, 15–18 April 2019, Marrakech, Morocco*. IEEE; 2019. DOI:10.1109/WCNCW.2019.8902590
14. Plotnikov P., Vladyko A. Numerical Analysis of the Mathematical Model of a Cluster V2X-System. *Proceedings of Telecommunication Universities*. 2023;9(1):14–23. (in Russ.) DOI:10.31854/1813-324X-2023-9-1-14-23. EDN:JDPDSD
15. Plotnikov P.V., Tambovtsev G.I., Vladyko A.G. *Software Module for Modeling the interaction of Edge Devices in VANET with one- and two-channel connectivity*. Patent RF, no. 2023681939, 06.10. 2023. (in Russ.)
16. Liu L., Chen C., Pei Q., Maharjan S., Zhang Y. Vehicular edge computing and networking: A survey. *Mobile Networks and Applications*. 2021;26:1145–1168. DOI:10.1007/s11036-020-01624-1
17. Fardad M., Muntean G.M., Tal I. A Blockchain-Enabled Vehicular Edge Computing Framework for Secure Performance-oriented V2X Service Delivery. *IEEE Transactions on Vehicular Technology*. 2024. DOI:10.1109/TVT.2024.3394150
18. Fan W., Su Y., Liu J., Li S., Huang W., Wu F., Liu Y. Joint Task Offloading and Resource Allocation for Vehicular Edge Computing Based on V2I and V2V Modes. *IEEE Transactions on Intelligent Transportation Systems*. 2023;24(4):4277–4292. DOI:10.1109/TITS.2022.3230430
19. Hou, P., Jiang, X., Lu, Z. et al. Joint computation offloading and resource allocation based on deep reinforcement learning in C-V2X edge computing. *Applied Intelligence*. 2023;53:22446–22466. DOI:10.1007/s10489-023-04637-x
20. Dai Y., Xu D., Maharjan S., Zhang Y., Joint Load Balancing and Offloading in Vehicular Edge Computing and Networks. *IEEE Internet of Things Journal*. 2019;6(3):4377–4387. DOI:10.1109/JIOT.2018.2876298
21. Guo H., Liu J., Ren J., Zhang Y. Intelligent Task Offloading in Vehicular Edge Computing Networks. *IEEE Wireless Communications*. 2020;27(4):126–132. DOI:10.1109/MWC.001.1900489
22. Cai G., Fan B., Dong Y., Li T., Wu Y., Zhang Y. Task-Efficiency Oriented V2X Communications: Digital Twin Meets Mobile Edge Computing. *IEEE Wireless Communications*. 2024;31(2):149–155. DOI:10.1109/MWC.012.2200465
23. Ye D., Yu R., Pan M., Han Z. Federated Learning in Vehicular Edge Computing: A Selective Model Aggregation Approach. *IEEE Access*. 2020;8:23920–23935. DOI:10.1109/ACCESS.2020.2968399
24. Luo Q., Li C., Luan T.H., Shi W. Collaborative Data Scheduling for Vehicular Edge Computing via Deep Reinforcement Learning. *IEEE Internet of Things Journal*. 2020;7(10):9637–9650. DOI:10.1109/JIOT.2020.2983660
25. Vladyko A., Tambovtsev G., Podgornaya E., Chelloug S.A., Alkanhel R., Plotnikov P. Cluster-Based Vehicle-to-Everything Model with a Shared Cache. *Mathematics*. 2023;11(13):3017. DOI:10.3390/math11133017
26. Bonomi F. Connected vehicles, the internet of things, and fog computing. *Proceedings of the Eighth ACM International Workshop on Vehicular Ad Hoc Inter-Networking, VANET 2011, Las Vegas, USA, 23 September 2011*. 2011.
27. Khattak H.A., Islam S.U., Din I.U., Guizani M. Integrating fog computing with VANETs: A consumer perspective. *IEEE Communications Standards Magazine*. 2019;3(1):19–25. DOI:10.1109/MCOMSTD.2019.1800050
28. Sarrigiannis I., Contreras L.M., Ramantas K., Antonopoulos A., Verikoukis C. Fog-Enabled Scalable C-V2X Architecture for Distributed 5G and Beyond Applications. *IEEE Network*. 2020;34(5):120–126. DOI:10.1109/MNET.111.2000476
29. Alvi A.N., Javed M.A., Hasanat M.H.A., Khan M.B., et al. Intelligent task offloading in fog computing based vehicular networks. *Applied Sciences*. 2022;12(9):4521. DOI:10.3390/app12094521

30. Tonguz O.K., Viriyasitavat W. Cars as roadside units: A self-organizing network solution. *IEEE Communications Magazine*. 2013;51(12):112–120. DOI:10.1109/MCOM.2013.6685766
31. Karunathilake T., Forster A. A survey on mobile road side units in VANETs. *Vehicles*. 2022;4(2):482–500. DOI:10.3390/vehicles4020029
32. Guerna A., Bitam S., Calafate C.T. Roadside unit deployment in internet of vehicles systems: A survey. *Sensors*. 2022;22(9):3190. DOI:10.3390/s22093190
33. Ercan S., Ayaida M., Messai N. How mobile RSUs can enhance communications in VANETs? // Proceedings of the 6th International Conference on Wireless Networks and Mobile Communications, WINCOM, 16–19 October 2018, Marrakesh, Morocco. IEEE; 2018. DOI:10.1109/WINCOM.2018.8629641
34. Lee J., Ahn S. Adaptive configuration of mobile roadside units for the cost-effective vehicular communication infrastructure. *Wireless Communications and Mobile Computing*. 2019;2019:6594084. DOI:10.1155/2019/6594084
35. Bitaghsir S.A., Kashipazha S., Dadlani A., Khonsari A. Social-aware mobile road side unit for content distribution in vehicular social networks. *Proceedings of the Symposium on Computers and Communications, ISCC, 29 June 2019 – 03 July 2019, Barcelona, Spain*. IEEE; 2019. DOI:10.1109/ISCC47284.2019.8969669
36. Reis A.B., Sargento S., Tonguz O.K. Parked cars are excellent roadside units. *IEEE Transactions on Intelligent Transportation Systems*. 2017;18(9):2490–2502. DOI:10.1109/TITS.2017.2655498
37. Qin P., Fu Y., Feng X., Zhao X., Wang S., Zhou Z. Energy-efficient resource allocation for parked-cars-based cellular-V2V heterogeneous networks. *IEEE Internet of Things Journal*. 2022;9(4):3046–3061. DOI:10.1109/JIOT.2021.3094903
38. Evariste T., Kasakula W., Rwigema J., Datta R. Optimal exploitation of on-street parked vehicles as roadside gateways for social IoV – a case of Kigali City. *Journal of Open Innovation: Technology, Market, and Complexity*. 2020;6(3):73. DOI:10.3390/joitmc6030073
39. Li G., Ma M., Liu C., Shu Y. Routing in taxi and public transport based heterogeneous vehicular networks. *Proceedings of the IEEE Region 10 Conference, TENCN, 22–25 November 2016, Singapore, Singapore*. IEEE; 2019. p.1863–1866. DOI:10.1109/TENCN.2016.7848344
40. Jiang X., Du D.H.C. Bus-VANET: A bus vehicular network integrated with traffic infrastructure. *IEEE Intelligent Transportation Systems Magazine*. 2015;7(2):47–57. DOI:10.1109/MITS.2015.2408137
41. Heo J., Kang B., Yang J.M., Paek J., Bahk S. Performance-cost tradeoff of using mobile roadside units for V2X communication. *IEEE Transactions on Vehicular Technology*. 2019;68(9):9049–9059. DOI:10.1109/TVT.2019.2925849
42. Kim D., Velasco Y., Wang W., Uma R.N., Hussain R., Lee S. A new comprehensive RSU installation strategy for cost-efficient VANET deployment. *IEEE Transactions on Vehicular Technology*. 2016;66(5):4200–4211. DOI:10.1109/TVT.2016.2598253
43. Ni Y., Zhao C., Cai L. Hybrid RSU management in cybertwin-IoV for temporal and spatial service coverage. *IEEE Transactions on Vehicular Technology*. 2022;71(5):4596–4606. DOI:10.1109/TVT.2021.3138749
44. Plotnikov P.V., Tambovtsev G.I., Vladyko A.G. Performance Evaluation of V2X Model with a Mobile Road Side Units. *Proceedings of the Intelligent Technologies and Electronic Devices in Vehicle and Road Transport Complex, TIRVED, 15–17 November 2023, Moscow, Russian Federation*. IEEE; 2023. DOI:10.1109/TIRVED58506.2023.10332617
45. Plotnikov P.V., Tambovtsev G.I., Vladyko A.G. Numerical Analysis of roadside Units Deployment Models in V2X Communication System. *Proceedings of the Systems of Signals Generating and Processing in the Field of on Board Communication, 12–14 March 2024, Moscow, Russian Federation*. IEEE; 2024. DOI:10.1109/IEEECONF60226.2024.10496720

Статья поступила в редакцию 13.05.2024; одобрена после рецензирования 21.06.2024; принята к публикации 24.06.2024.

The article was submitted 13.05.2024; approved after reviewing 21.06.2024; accepted for publication 24.06.2024.

Информация об авторах:

ПЛОТНИКОВ
Павел Владимирович

кандидат физико-математических наук, доцент, доцент кафедры высшей математики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
 <https://orcid.org/0000-0001-8869-6142>

ВЛАДЫКО
Андрей Геннадьевич

кандидат технических наук, доцент, декан факультета фундаментальной подготовки Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
 <https://orcid.org/0000-0002-8852-5607>

Владыко А.Г. является заместителем главного редактора журнала «Труды учебных заведений связи» с 2023 г., но не имеет никакого отношения к решению опубликовать эту статью. Статья прошла принятую в журнале процедуру рецензирования. Об иных конфликтах интересов авторы не заявляли.

Vladyko A.G. has been a Deputy editor-in-chief of the journal "Proceedings of Telecommunication Universities" since 2023, but has nothing to do with the decision to publish this article. The article has passed the review procedure accepted in the journal. The authors has not declared any other conflicts of interest.

ЭЛЕКТРОНИКА, ФОТОНИКА, ПРИБОРОСТРОЕНИЕ И СВЯЗЬ

2.2.6 – Оптические
и оптико–электронные приборы
и комплексы

2.2.13 – Радиотехника, в том числе системы
и устройства телевидения

2.2.14 – Антенны, СВЧ–устройства
и их технологии

2.2.15 – Системы, сети и устройства
телекоммуникаций

2.2.16 – Радиолокация и радионавигация

Научная статья

УДК 621.391

<https://doi.org/10.31854/1813-324X-2024-10-3-24-34>

Динамические туманные вычисления и бессерверная архитектура: на пути к зеленым ИКТ

✉ Артем Николаевич Волков, artem.nv@sut.ru

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича,
Санкт-Петербург, 193232, Российская Федерация

Аннотация

Актуальность. В условиях роста парка оборудования центров обработки данных, развития сетей ИМТ-2020 и появлением услуг Телеприсутствия сетей ИМТ-2030 особо актуальным направлением современных исследований является поиск нетривиальных, нестандартных подходов и решений в области обеспечения вычислительными и сетевыми ресурсами. Данная статья освещает актуальные вопросы инфраструктурного направления сетей ИМТ-2030 – динамических туманных вычислений. Рассматривается вклад данной технологии для повышения эффективности используемых ресурсов, приводятся актуальные сценарии сетей ИМТ-2030. В частности, исследуется задача поиска группы устройств в туманных вычислениях для последующей миграции типовых контейнеров платформы FaaS.

Постановка задачи: исследование вопросов совместного использования бессерверной архитектуры и динамических туманных вычислений для эффективного распределения нагрузки услуг Телеприсутствия. **Цель работы:** исследование и разработка эффективного метода распределения группы микросервисов в динамических туманных вычислениях.

Используемые методы: исследуемые алгоритмы относятся к типу метаэвристических алгоритмов для решения задач многокритериальной оптимизации. Для апробации метода был разработан сегмент лабораторной сети, который послужил генератором реальных данных работы тестируемых платформ в условиях роста нагрузки. На базе серии экспериментов были собраны данные для последующего моделирования предложенного метода, который, в свою очередь, был реализован на языке программирования Python.

Анализ **результатов** показал эффективность предложенного метода в рамках поставленной задачи, что, в конечном итоге, позволяет значительно быстрее принимать решение о миграции.

Новизна: разработаны модель и метод для бессерверной архитектуры с миграцией групп микросервисов на группы устройств туманных вычислений в условиях их подвижности, и использован метаэвристический алгоритм стаи серых волков с целью определения группы устройств для последующей миграции типовых микросервисов.

Практическая значимость: разработанная модель и метод могут быть использованы при реализации туманных вычислений в условиях подвижности устройств, в том числе с целью достижения требований перспективных услуг Телеприсутствия.

Ключевые слова: ИМТ-2030, туманные вычисления, услуги Телеприсутствия, бессерверная архитектура, метаэвристические алгоритмы

Источник финансирования: статья подготовлена в рамках мегагранта Минобрнауки по соглашению № 075-15-2022-1137.

Ссылка для цитирования: Волков А.Н. Динамические туманные вычисления и бессерверная архитектура: на пути к зеленым ИКТ. 2024. Т. 10. № 3. С. 24–34. DOI:10.31854/1813-324X-2024-10-3-24-34. EDN:QOELMJ

Original research

<https://doi.org/10.31854/1813-324X-2024-10-3-24-34>

Dynamic Fog Computing Towards Green ICT

 Artem N. Volkov, artem.nv@sut.ru

The Bonch-Bruевич Saint Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Annotation

Relevance: In the context of the growing fleet of data center equipment, the development of IMT-2020 networks and the imminent emergence of Telepresence services of IMT-2030 networks, a particularly relevant area of modern research is the search for non-trivial, non-standard approaches and solutions in the field of provision of computing and network resources. This article covers current issues in the infrastructure direction of IMT-2030 networks - dynamic fog computing. The contribution of this technology to improve the efficiency of used resources is considered, and current scenarios for IMT-2030 networks are presented. In particular, we study the problem of searching for a group of devices in the computing fog for subsequent migration of typical FaaS platform containers.

Problem statement: Research on the joint use of serverless architecture and dynamic fog computing for efficient load distribution of telepresence services.

Goal of the work: Research and development of an effective method for distributing a group of microservices in dynamic fog computing.

Methods: the algorithms under study belong to the type of metaheuristic algorithms for solving multicriteria optimization problems. To test the method, a laboratory network segment was developed, which served as a generator of real data on the operation of the tested platforms under conditions of increasing load. Based on a series of experiments, data was collected that formed the basis for subsequent modeling of the proposed method, which in turn was implemented in the Python programming language.

Result: Analysis of the results showed the effectiveness of the proposed method within the framework of the task, which ultimately makes it possible to make a decision on migration many times faster.

Novelty: A model and method for serverless architecture have been developed for migrating groups of microservices to groups of fog computing devices, under conditions of their mobility, and a meta-heuristic algorithm of a pack of gray wolves has been used to determine a group of devices for subsequent migration of typical microservices.

Practical significance: The developed model and method can be used in the implementation of fog Computing, in conditions of device mobility, including in order to achieve the requirements of promising Telepresence services.

Keywords: IMT-2030, fog computing, telepresence services, serverless architecture, metaheuristic algorithms

Funding: The article was prepared within the framework of a megagrant from the Ministry of Education and Science under agreement No. 075-15-2022-1137.

For citation: Volkov A.N. Dynamic Fog Computing Towards Green ICT. *Proceedings of Telecommunication Universities*. 2024;10(3):24–34. (in Russ.) DOI:10.31854/1813-324X-2024-10-3-24-34. EDN:QOELMJ

Введение

Общее стремление к цифровизации процессов в государстве, бизнесе и обществе одновременно приносит как положительные аспекты – повышение эффективности и прозрачности систем, так и новые вызовы и трудноразрешимые задачи. Принятие и внедрение концепции Интернета Вещей (ИВ), масштабы которой 10 лет назад были недооценены, и последующие базирующиеся на ней технологические направления привели к фундаментальным изменениям не только в области

конкретных технологий и решений, но и во взглядах на услуги и саму сеть. Так, развитие платформ ИВ, позволяющих обрабатывать гигабайты данных и получать новые знания с использованием инструментов искусственного интеллекта (ИИ), привело к бурному развитию центров обработки данных (ЦОДы). Последующее развитие ИВ породило различные концепции услуг, например таких, как: Тактильный Интернет, Интернет Навыков и другие. Приведенные примеры относятся к сверхнадежным сетям с ультрамалыми задержками

(URLLC, аббр. от англ. Ultra-Reliable Low Latency Communications), которые являются одним из фундаментальных направлений сетей ИМТ-2020. Стоит отметить, что принятая в конце 2023 г. концепция сетей ИМТ-2030 естественным образом стала преемницей ИМТ-2020, в тоже время увеличив требования и представив такие сценарии, как TIRO (аббр. от англ. Tactile Internet for Remote Operations) и HTC (аббр. от англ. Holographic Type Communications). Сети ИМТ-2030 определяют следующие «технологические измерения»:

– Massive Communication (пер. с англ. – массовые коммуникации), что, в свою очередь, является расширением massive Machine Type Communication (mMTC);

– Immersive Communication (пер. с англ. – иммерсивные коммуникации), является расширенным enhanced Mobile Broadband (eMBB); при этом важно отметить, что новый сценарий включает в себя и поднаправления mMTC и URLLC;

– Hyper Reliable & Low-Latency Communication (HURLLC, пер. с англ. – гипернадёжные сети связи с ультрамалой задержкой), представляют развитие направления URLLC-сетей ИМТ-2020;

– Artificial Intelligence in Communication (AI in Communication, пер. с англ. – искусственный интеллект в связи) или автономные сети связи; на сегодня можно обнаружить достаточно большой пласт разработанных Рекомендаций МСЭ-Т (Международный союз электросвязи, сектор стандартизации телекоммуникаций) в 13 ИК (Исследовательской комиссии), где определены фундаментальные решения для последующей имплементации технологий ИИ в сети связи;

– Ubiquitous Connectivity (пер. с англ. – повсеместная связь): данное направление, в первую очередь, раскрывает концепцию МСЭ сетей 2030 STIN (от англ. Space-Terrestrial Integrated Network – космически-наземная интегрированная сеть) и является предложением по решению ряда целей устойчивого развития ООН, в том числе для сокращения цифрового разрыва с удалёнными районами и поселениями;

– Integrated Sensing and Communication (пер. с англ. – интегрированное зондирование и связь): формирует целый пласт задач в области позиционирования в сети ИМТ-2030 и тесно связано с другими сценариями ее применения.

В результате бурного развития ИВ и других сценариев сетей ИМТ-2020 несколько лет назад был сформирован тренд на декомпозицию систем вычислений. Граничные вычисления позволили, благодаря своей архитектуре, приблизить реализацию ряда услуг, а также снизить нагрузку на ядро сети. В то же время автономные сети призваны разрешить вопросы интеллектуального распределения ресурсов как сетевых, так и вычислитель-

ных, которые мягко интегрированы в системы управления сетью. В итоге глобальный тренд на абстрагирование программного обеспечения сетевых и вычислительных сущностей от аппаратной части сформировал технические возможности реализации программного слайсинга ресурсов. Пройдя вышеприведенные этапы развития сети и вычислительных систем, стала более ясна цель – максимальная автономизация инфраструктуры с рациональным использованием вычислительных и сетевых ресурсов на базе алгоритмов машинного интеллекта.

Если обратиться к отчетам статистического агентства Straits Research [1], можно заметить продолжающийся рост объема рынка оборудования для ЦОДов. Ожидается, что к 2031 г. он достигнет 164,36 млрд долларов США, а среднегодовой темп роста (рисунок 1) составит 13,2% (CAGR, аббр. от англ. Compound Annual Growth Rate – совокупный среднегодовой темп роста) в течение прогнозируемого периода (2023–2031 гг.).



Рис. 1. Рост рынка оборудования ЦОД [1]

Fig. 1. Data Center Equipment Market Growing [1]

С учетом планируемых услуг Телеприсутствия сетей ИМТ-2030 цифры роста могут быть изменены в большую сторону, и факт объема строящихся ЦОДов заставляет задуматься об эффективности используемого сетевого и вычислительного оборудования, а также увеличении потребления энергоресурсов для обеспечения работы данного парка оборудования.

В работе [2] приводится проблема создания зеленых инфокоммуникационных технологий (Green ICT). Исследуются как организационные, так и информационно-технологические способы перехода к Green ICT, то есть на рациональное энергопотребление. К примеру, приводится сравнительный анализ потребности энергии для судна-контейнеровоза «Emma-Maersk», одного из крупных ЦОДов европейской части России, где сравнительно наглядно становится понятно, насколько ЦОДы потребляют электроресурсов. Существует немало работ в области Green ICT [3–6], а также – немало решений в данной области,

которые внедряются различными компаниями по всему миру. Стоит также отметить то, что данная повестка активно исследуется и прорабатывается на уровне международных рекомендаций МСЭ-Т Исследовательской комиссией № 5. В частности, можно найти серию Рекомендаций МСЭ-Т L.1300-L.1399: Энергоэффективность, умная энергетика и экологически чистые центры обработки данных, а также немало технических отчетов и спецификаций. МСЭ-Т дает следующее определение: «Зеленый» или устойчивый ЦОД – это хранилище для управления и распространения данных, в котором механические, осветительные, электрические и компьютерные системы спроектированы с учетом максимальной энергоэффективности и минимального воздействия на окружающую среду. В работе [7] дано следующее определение Green ICT как совокупности способов, призванных уменьшать вредное воздействие на человека и окружающую среду, эффективно использовать ресурсы, которые предоставляет природа и одновременно повышать производительность систем в расчете на единицу потребляемых физических ресурсов. Существует также принцип Р. Ландауэра, который позволяет установить связь между объемом данных и энергозатратами, при этом независимо от физики и технологии вычислительного процесса в случае потери одного бита данных в ходе вычисления как минимум выделяется энергия E (Дж). Как бы это «парадоксально» не звучало, принцип Ландауэра означает, что компьютер потребляет тем меньше энергии, чем меньше вычислительных операций он выполняет. Если же рассматривать принципы обработки данных на базе ЦОД, то необходимо учесть добавочные затраты энергоносителей, которые необходимы для постоянной работы систем охлаждения и других вспомогательных систем, а также систем питания сетей связи, которые обеспечивают доступ к ЦОД.

Таким образом, с точки зрения принципа Ландауэра, а также учитывая вышеприведенные исследования в области трендов рынка и развития технологий услуг Телеприсутствия и сетей ИМТ-2030, в настоящее время существует потребность в поиске более эффективных методов построения инфраструктуры. В частности, ожидается, что декомпозиция ЦОДов в меньшие центры, а также внедрение алгоритмов ИИ и более инновационных материалов, а также использование возобновляемых источников энергии позволит снизить общий эффект на окружающую среду. При этом декомпозиция вычислительной архитектуры и систем «эпохи» до туманных вычислений (Fog), в том числе динамических, позволит исключить некоторые составляющие в общей формуле потребления энергии на удельный размер вычислительной задачи. Здесь использование устройств пользовате-

ля и устройств ИВ не требует дополнительных систем охлаждения, резервирования и построения технологичных зданий с надстроенными инженерными системами для его функционирования. В таком случае концепция Fog не только позволяет обеспечить требования к качеству обслуживания для ряда услуг при условии микросервисных архитектур, но и снизить общую суммарную потребность в энергоресурсах. Де-факто Fog являются инструментом бережливого производства в области инфокоммуникационных технологий и систем связи.

Динамические туманные вычисления и бессерверная архитектура услуг

Бессерверная архитектура (serverless) и контейнеры могут быть интегрированы для создания высокомасштабируемых и эффективных платформ высоконагруженных услуг. Контейнеры могут использоваться для упаковки и развертывания функций serverless, что позволяет разработчикам услуг использовать преимущества обеих технологий. К преимуществам совместного использования технологий можно отнести следующие:

- упрощенное развертывание (контейнеры упрощают развертывание функций serverless, поскольку они уже содержат все зависимости программного обеспечения в виде библиотек и фреймворков);
- портативность (контейнер позволяет быстро переносить функции serverless между различными облачными платформами и локальными средами);
- безопасность (контейнеры обеспечивают изоляцию и безопасность между serverless-функциями, что в итоге снижает риск уязвимостей).

Для анализа работы сети Fog необходимо использовать модель, которая позволит описать функционирование сети в условиях изменяющейся архитектуры ввиду мобильности Fog-устройств как рамках кластера, так и в рамках *туманностей* (Nebula) [8]. При этом данные кластера и/или туманности обладают характеристикой гетерогенности как самих Fog-устройств, так и собственно структур. Таким образом, с учетом вышеприведенных допущений, в качестве математической модели может быть использована модель точечного процесса, учитывая гетерогенность структур и Fog-устройств. При этом, в данных условиях процессы Неймана – Скотта, относящиеся к точечным процессам с кластеризацией (то есть с объединениями устройств), будут предпочтительнее для построения модели. Так как процессы без кластеризации применяются для моделирования однородных систем, где объекты образуют одно единственное поле, размещенное на плоскости или в пространстве (такая модель может быть применима в частных случаях при использовании

однородных вычислительных ферм). Более подробные исследования в области применения точечных процессов для распределенных Fog представлены в следующей статье [9]. Стоит отметить, что Fog обладают отчасти противоречивыми характеристиками. Например, устройства динамических Fog могут образовывать mesh-сеть, при этом обладающую характеристикой самоорганизации с возможностью горизонтального масштабирования, что больше напоминает самоорганизующиеся сенсорные сети. В то же время, Fog являются вычислительным кластером, на базе которого могут быть развернуты платформы, услуги и др. Соответственно, для разрешения задач может быть перенят опыт исследований и разработок в вышеуказанных областях знаний. Так, в работах [10, 11] приводятся исследования применения аппарата точечных процессов, в частности процессов Томаса для формирования математических моделей в сверхплотных сенсорных сетях ИВ, что говорит об актуальности использования данной математической базы для перспективных сетей и услуг.

В данной работе необходимо решить задачу поиска группы устройств в вычислительной туманности, которая может быть представлена в виде группы или одного кластера Fog. При этом делается допущение о том, что все устройства, находясь в условиях мобильности относительно базовой станции или сетевого координатора, стремятся сохранять единый вектор перемещения при минимально возможных отклонениях между собой. На практике такой сценарий может быть обнаружен в быстрых поездах типа Сапсан, самолетах и других похожих условиях (общественный транспорт, проспекты и т. п.).

Таким образом, опираясь на сценарий, модель сети Fog при поиске группы Fog-устройств для дальнейшей живой миграции 4-х типовых контейнеров платформы FaaS может быть представлена в виде рисунка 2. Каждое из Fog-устройств – набор параметров, характеризующих устройство с точки зрения элемента вычислительного кластера: CPU (количество и частота ядер процессора), GPU (производительность графического процессора), Network (тип интерфейса и тип технологии связи, в том числе возможная скорость подключения), и многие другие. В текущей модели, для развертывания FaaS-unit, с 4-мя типовыми контейнерами ($MS_i, \forall i \in N$) и оценки предлагается использовать временные характеристики реализации задачи. Вводя типизацию контейнеров MS_i , возможно перейти к оценке характеристик самого Fog-устройства, а также собственно контейнера в пространстве времени, а именно: времени реализации задачи типовым контейнером T_c (мс) и задержки передачи соответствующего объема информации T_r (мс), который является конечным. Типовой

контейнер решает одну задачу: например, сортировка данных методом пузырька, где определен соответствующий формат и объем принимаемых данных, а также формат и объем передаваемых результатов.

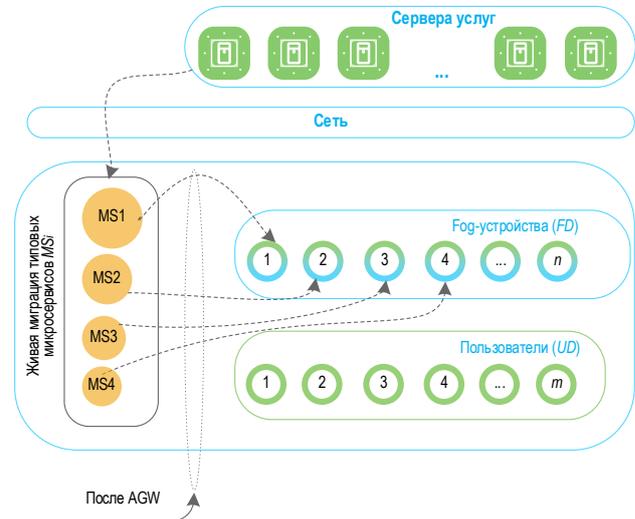


Рис. 2. Модель сети туманных вычислений при поиске группы Fog-устройств

Fig. 2. Fog Computing Network Model for Group of Fog-Devices Searching

Таким образом, необходимо определить параметры, описывающие каждое из исследуемых Fog-устройств. При этом некоторые параметры могут оцениваться на уровне сравнения с предельными значениями: например, количество выделенной логической ОЗУ, необходимой для работы готовящегося к миграции микросервиса или группы микросервисов. В рамках данной задачи были определены параметры, описывающие Fog-узел с точки зрения затраченного времени реализации типовой задачи.

В общем виде целевая функция оценки устройства может быть представлена следующим образом:

$$F = \sum_{i=1}^m k_i P_i, \quad (1)$$

где $0 \leq k_i \leq 1$ – коэффициенты, при этом $\sum k_i = 1$; P_i – параметры оценки, при m – количество параметров для $\forall i > 0, i \in N$, а основная задача сформулирована в виде выражения:

$$\{F_1, F_2, F_3, F_4\} = \arg \min_{T_r, T_c, S} \{F\}, \quad (2)$$

где $\{F_1, F_2, F_3, F_4\}$ – ряд решений $F(T_r, T_c, S)$ в порядке неубывания их значений, то есть: $F_1 \leq F_2 \leq F_3 \leq F_4$. T_c – время выполнения типовой задачи в типовом контейнере MS_i . Параметр T_r характеризует связь узла с основным шлюзом-брокером в соответствующей зоне Fog, через который проходят все транзакции между устройствами и, соот-

ветственно, контейнерами; может быть представлен как задержка при передаче типового запроса с соответствующим объемом данных до шлюза-брокера. Параметр S описывает степень стабильности кластера Fog, в частности рассматривается стабильность соответствующего устройства в кластере Fog. При этом вероятность того, что расстояние между элементом кластера Fog и шлюзом-брокером превысит величину R , может быть оценено как [9]:

$$p(d > R) = 1 - \text{Dis}(R, \delta), \quad (3)$$

где $\text{Dis}(R, \delta)$ – функция распределения вероятности расстояния между устройством и координатором. В зависимости от условий, она может быть описана Гамма-распределением или его частными формами, например, распределением Пирсона или распределением Райса. R – расстояние между устройством и координатором. При этом вероятность того, что расстояние между координатором и хотя бы одним из элементов кластера превышает величину R определяется как [9]:

$$p(> R) = 1 - \prod_{i=1}^k \text{Dis}(R, \delta_i), \quad (4)$$

где k – число устройств кластера Fog; δ_i – параметр распределения вероятности расстояния.

Таким образом, в работе [9] было сформулировано предложение о максимальной стабильности Fog-кластера, где под стабильностью понимается стремление сохранить структуру, то есть связи между координатором и элементами кластера:

$$\min_R \left\{ 1 - \prod_{i=1}^k \text{Dis}(R, \delta_i) \right\}. \quad (5)$$

Стабильность кластера Fog может быть представлена как оценка, описанная в виде функции минимизации вероятности изменения географического состояния устройства относительно так называемого центра масс кластера или шлюза-брокера в кластере Fog, через который проходят все транзакции. Данная задача может быть решена с использованием точечных процессов Неймана – Скотта [9].

Соответственно, стабильность самого устройства относительно его отношения к шлюзу-брокеру будет представляться в следующем виде:

$$\min_R \{1 - \text{Dis}(R, \delta)\}, \quad (6)$$

а используемый параметр оценки стабильности S в основной целевой-функции может быть представлен следующим образом:

$$S = \max \left\{ \min_R \{1 - \text{Dis}(R, \delta)\} \right\}. \quad (7)$$

В данной работе предлагается рассмотреть частный случай, как ранее было упомянуто, в качестве исследуемых параметров взять оценку Fog-узла с точки зрения T_c и T_r , а также параметра оценки стабильности устройства в кластере, где $0 < S \leq 1$.

Таким образом, целевая функция, исследуемая в данной работе, может быть представлена в следующем виде:

$$F = \sum_{i=1}^m k_i P_i = k_1 T_r + k_2 T_c + k_3 S. \quad (8)$$

Данный метод может быть использован при выполнении условия типизации контейнеров для развертывания serverless. В общем случае, метод может быть сложно реализуем с точки зрения необходимости предварительного тестирования среднего времени выполнения функции соответствующим нетиповым контейнером общей услуги.

Для решения поставленной задачи был исследован класс метаэвристических алгоритмов, которые позволяют определить глобальный экстремум фитнес-функции. Существует немало метаэвристических алгоритмов. Рассмотрим основные: алгоритм стаи серых волков (GWO, аббр. от англ. Grew Wolf Optimizer), алгоритм оптимизации роя частиц (PSO, аббр. от англ. Particle Swarm Optimization), генетический алгоритм (GA, аббр. от англ. Genetic Algorithm) и алгоритм роя сальп (SSA, аббр. от англ. Salp Swarm Algorithm). Каждый из этих алгоритмов имеет свои уникальные особенности и преимущества. К их сходству можно отнести следующие критерии: все они являются популяционными (то есть, они работающими с популяцией кандидатных решений) и используют итеративный процесс поиска.

В целом GWO, PSO, GA и SSA являются мощными и эффективными алгоритмами, которые полезно использовать для решения широкого спектра оптимизационных задач. Выбор алгоритма зависит от конкретной задачи и требований к производительности. Так, например, генетический алгоритм является более ресурсозатратным, что также влечет за собой скорость/время сходимости.

В результате анализа особенностей данных алгоритмов, в частности при рассмотрении требований к скорости сходимости, простоте (в том числе при настройке параметров), предлагается использовать алгоритм GWO (метаэвристический алгоритм, который был вдохновлен социальным поведением серых волков). Серые волки – это социальные животные, которые живут в стае, возглавляемой альфа-самцом. Метаэвристический алгоритм GWO имитирует социальное поведение серых волков, чтобы решить оптимизационные задачи – поиск экстремума фитнес-функции. Алгоритм

инициализирует популяцию волков (возможных решений) и оценивает каждого волка в популяции $X_\alpha, X_\beta, X_\delta$. Затем алгоритм итеративно обновляет

положения волков на основе их текущих позиций и позиций других волков в стае.

ТАБЛИЦА 1. Сравнительный анализ

TABLE 1. Comparing Analysis

	Метаэвристические алгоритмы			
	GWO	PSO	GA	SSA
Биологическая модель-источник	социальное поведение волков	поведении стаи птиц	процесс эволюции	поведение роя сальп (морские животные)
Структура популяции	волки	частицы	хромосомы	сальпы
Принцип обновления	волки обновляют свои положения на основе позиций альфа-, бета- и дельта-волков	частицы обновляют свои положения на основе своих собственных лучших положений и лучшего положения в популяции	хромосомы обновляются с помощью операций кроссовера и мутации	сальпы обновляют свои положения на основе положения передней и задней сальпы
Топологии	волки расположены в иерархической структуре	частицы обычно расположены в топологии кольца	хромосомы не имеют определенной топологии	сальпы расположены в одномерной топологии

Таким образом, на каждой итерации, в том числе финальной, алгоритм будет выдавать 4 результата, которые по возрастающей будут отражать соответствующие устройства, пригодные для последующего размещения типовых микросервисов услуг.

В GWO позиция каждого волка рассчитывается на основе следующих выражений (9–11):

$$D_\alpha = |C_1 X_\alpha - X(i)|, D_\beta = |C_2 X_\beta - X(i)|, \quad (9)$$

$$D_\delta = |C_3 X_\delta - X(i)|, \quad (10)$$

$$X_1 = X_\alpha - A_1(D_\alpha), X_2 = X_\beta - A_2(D_\beta), X_3 = X_\delta - A_3(D_\delta), \quad (11)$$

$$X(x+1) = \frac{X_1 + X_2 + X_3}{3}, \quad (11)$$

где $[X_\alpha, X_\beta, X_\delta, X_\omega]$: альфа-волк (X_α) – лучшее решение в популяции; бета-волк (X_β) – второе лучшее решение в популяции; дельта-волк (X_δ) – третье лучшее решение в популяции; омега-волки (X_ω) – остальные волки в популяции; X_i – позиция решения на соответствующей итерации i ; $D_\alpha, D_\beta, D_\delta$ – вспомогательные векторы для расчета соответственно значений X_1, X_2, X_3 .

На каждой итерации алгоритма обновляются коэффициенты A и C , согласно следующим выражениям (12–14):

$$A = 2a \cdot r_1 - a, \quad (12)$$

$$C = 2r_2, \quad (13)$$

$$a = 2 - \left(i \cdot \frac{2}{I}\right). \quad (14)$$

где a – параметр, линейно уменьшающийся от 2 до 0 на каждой итерации согласно выражению (14); r_1, r_2 – равномерно распределенные случайные числа от 0 до 1; I – количество итераций.

Следственно параметрами, которые могут повлиять на эффективность алгоритма GWO, являются количество волков, количество итераций, а также параметры a и C . При этом, величина C на каждой итерации обеспечивает диверсификацию алгоритма GWO. Схематично работа алгоритма представлена на рисунке 3.

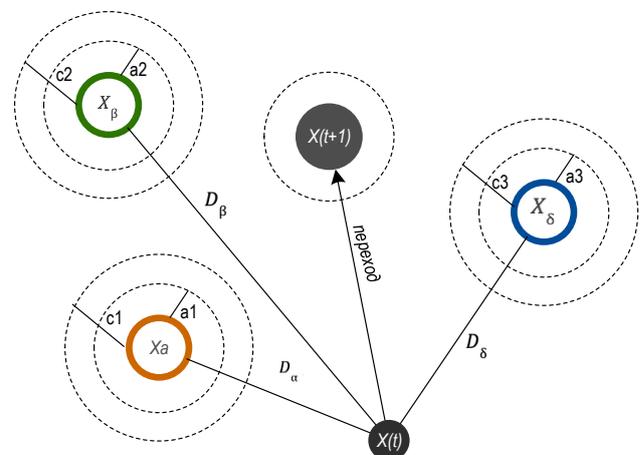


Рис. 3. Схема работы алгоритма

Fig. 3. Algorithm Scheme

Алгоритм GWO представлен в виде псевдокода:

```

0:BEGIN
1: Инициализация популяции GWO –  $X_i (i = 1, 2, \dots, n)$ ;
2: Инициализация GWO-параметров:  $a, A$  и  $C$ ;
3: Расчет фитнес-функции  $F_x$  для каждого агента;
4: /* комментарий:
5:  $X_\alpha$  – лучший агент
6:  $X_\beta$  – второй лучший агент
7:  $X_\delta$  – третий лучший агент
8:  $X_\omega$  – остальные агенты
9: */
10: Нахождение 3-х лучших  $X_\alpha, X_\beta, X_\delta$ ;
11: While достижение критерия do
12: for каждого агента do
13: Обновление позиции согласно с формулой (11);
14: end for
15: обновить  $a, A$  и  $C$ ;
16: расчет  $F_x$  фитнес-функции для каждого агента;
17: обновление  $X_\alpha, X_\beta, X_\delta$ ;
18: end while
19: вернуть значение  $X_\omega$ , лучшее значение  $F(X_\omega)$ , а также значение на последней итерации алгоритма [ $X_\beta, X_\delta, X_\omega$ ];
20:END.
    
```

GWO – это мощный и эффективный алгоритм, который можно использовать для решения широкого спектра оптимизационных задач, в том числе для поиска группы значений экстремумов функции, в том числе фитнес-функции, описывающей каждое из Fog-устройств в туманности.

Результаты моделирования

Для моделирования было проведено предварительное натурное исследование существующих платформ: Kata, Firecracker, Wasm, Docker. Тестирование проводилось на базе серверного оборудования лаборатории Meganetlab 6G кафедры сетей связи и передачи данных СПбГУТ. Для исследования были выбраны два метода распределения поступающей нагрузки:

Метод 1. Каждый новый запрос, входящий на агент (брокер/шлюз), направлялся на типовой микросервис/контейнер, который обслуживал запросы в порядке очереди FIFO.

Метод 2. Каждый новый запрос, входящий на агент, обслуживался вновь созданным клоном типowego микросервиса, после чего данный клон уничтожался. Таким образом, система гибко масштабировалась под рост нагрузки.

Для этого рассматривался пример работы типowego микросервиса, который был представлен в виде контейнера и решал типовую задачу – расчет числа π . На рисунке 4а в виде пузырьковой диаграммы отражены результаты тестирования первого метода на реальном стенде, где были развернуты платформы и реализованы типовые контейнеры. На рисунке 4б в виде пузырьковой диаграммы отражены результаты тестирования второго метода на реальном стенде, где при поступлении новой задачи происходил принудительный старт

нового контейнера в кластере, и задача выполнялась параллельно.

На рисунке 4 размер пузырька является средним временем решения типовой задачи, вычисленным на базе пяти повторных экспериментов. При этом ось абсцисс представлена в логарифмическом масштабе на обоих рисунках. Представленные графики позволяют визуально оценить возможности существующих решений контейнеризации для сегментов Fog, учитывая различные подходы к распределению вычислений в микросервисной архитектуре. Согласно рисунку 4б, Docker при росте нагрузки и сравнительно равным (в меньшей степени изменяющимся) временем старта нового контейнера для каждой задачи уменьшает время реализации типовой задачи. При этом Docker находится на втором месте после Wasm, относительно времени старта типowego контейнера.

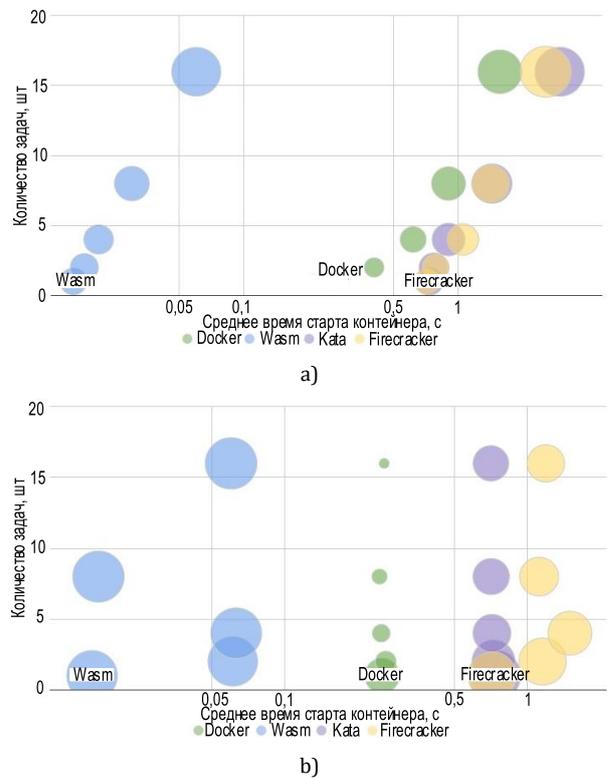


Рис. 4. Диаграммы: по методу 1 (а); по методу 2 (б)
 Fig. 4. Diagram for method 1 (a) and method 2 (b)

Для дальнейшего моделирования были взяты за основу данные, которые измерялись на стенде при работе Docker-контейнеров ввиду эффективности их работы при возрастающих нагрузках и большом количестве типовых микросервисов, что может быть свойственно Fog. Полученные в ходе эксперимента результаты легли в основу набора данных T_r и T_c , которые были составлены для 100 Fog-устройств, при этом структура этих данных была согласована с целевой функцией, представленной в выражении (8). Для визуализации ре-

зультата параметр устойчивости узла был установлен в виде константы $S = \text{const} = 1$, а коэффициенты k_1, k_2 и k_3 – равными 0,33. Итог моделирования Fog-устройств представлен на рисунке 6, где ось абсцисс – это значение $k_1 T_r$, ось ординат – представляет значение $k_2 T_c$, а ось аппликат, соответственно, – значение целевой функции F . Далее на поле данных смоделированных Fog-устройств был применен алгоритм GWO, разработанный также на языке программирования Python. Результат поиска группы устройств с помощью данного алгоритма представлен на рисунке 7.

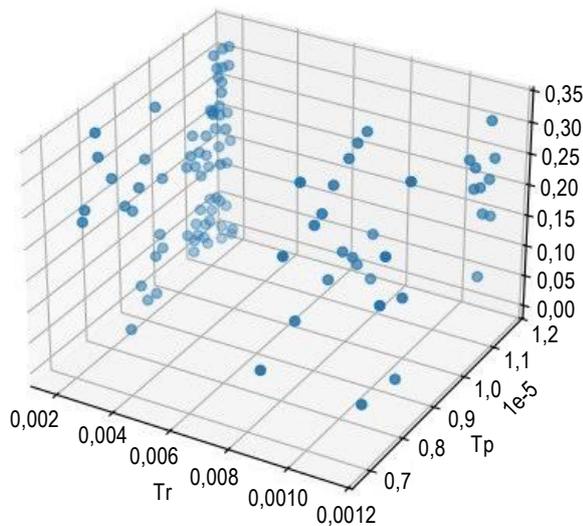


Рис. 6. Результаты моделирования Fog-устройств

Fig. 6. Results of Fog-Devices Modeling

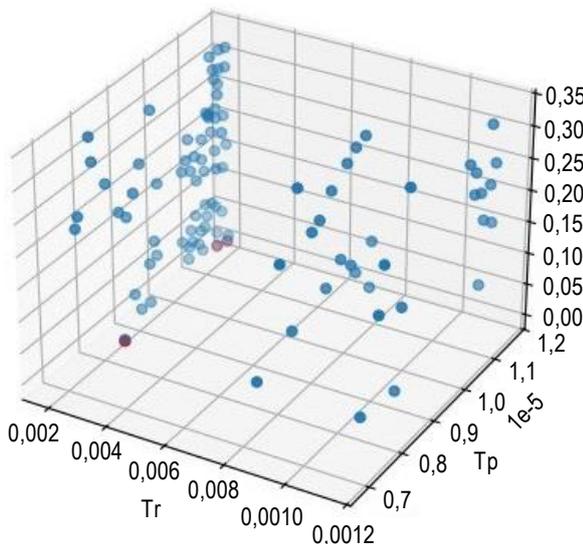


Рис. 7. Результат работы алгоритма GWO

Fig. 7. Result of GWO Algorithm Working

В ходе поиска были найдены основные три устройства, выделенные фиолетовым цветом (см. рисунок 7), а четвертое является первым устройством во множестве данных ω .

Оценка эффективности метода

Для оценки эффективности предложенного метода предлагается сравнить алгоритм GWO с алгоритмом PSO, который также является одним из эффективных с точки зрения скорости схождения и затрат вычислительных ресурсов. Ниже представлено описание данного алгоритма.

Каждая отдельная частица i состоит из трех векторов: ее положение в D -мерном пространстве поиска $\bar{x}_i = (x_{i1}, x_{i2}, \dots, x_{iD})$, лучшая найденная позиция $\bar{p}_i = (p_{i1}, p_{i2}, \dots, p_{iD})$, направленная скорость движения $\bar{v}_i = (v_{i1}, v_{i2}, \dots, v_{iD})$. При запуске алгоритма частицы равномерно, случайным образом инициализируются по всему пространству поиска, при этом скорость частиц также инициализируется случайным образом. Сформированные частицы перемещаются по пространству поиска с помощью довольно простого набора уравнений обновления векторов частицы. Алгоритм обновляет весь рой на каждом временном шаге, обновляя скорость и положение всякой частицы в каждом измерении по следующим правилам:

$$v_{id} = v_{id} + c\varepsilon_1(p_{id} - x_{id}) + c\varepsilon_2(p_{gd} - x_{id}), \quad (15)$$

$$x_{id} = x_{id} + v_{id}, \quad (16)$$

где c – константа со значением 2; 0, 1 и 2 – независимые случайные числа, уникально генерируемые при каждом обновлении для всякого отдельного измерения от $d = 1$, до D ; p_{gd} – положение, найденное любой соседней частицей.

Процесс обновления кратко описан в алгоритме PSO, представленном в виде псевдокода:

1. **for** каждого шага t **do**;
2. **for** каждой частицы i в рое **do**
3. обновить позицию xt , используя выражения (15) и (16)
4. рассчитать фитнес-функцию для xt $f(xt)$
5. обновить p_i, p_g
6. **end for**;
7. **end for**.

Стоит отметить, что в алгоритме скорость частиц фиксируется на максимальном значении v_{max} . Без фиксации алгоритм склонен не сойтись, когда расчет значений (15) и (16) приводил бы к быстрому увеличению скорости и, следовательно, положения частиц, приближались бы к бесконечности. Параметр v_{max} не позволяет системе войти в данное состояние, ограничивая скорость всех частиц.

Для оценки эффективности алгоритмов была проведена серия экспериментов, где отслеживалось время схождения алгоритмов, то есть время поиска устройств для последующей миграции группы типовых контейнеров. Функция счета времени была реализована в разработанном программном коде самой модели на языке Python. Результаты сравнения представлены на рисунке 8.

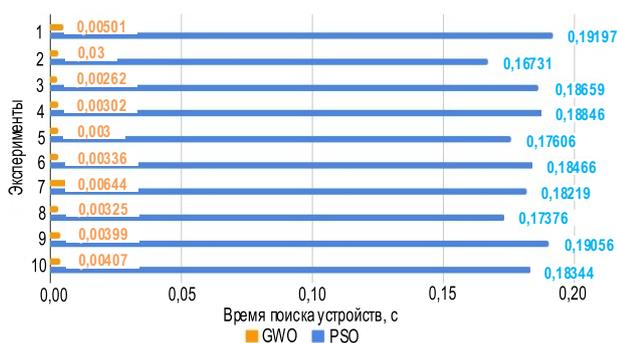


Рис. 8. Сравнение алгоритмов PSO и GWO

Fig. 8. PSO and GWO Algorithms Comparing

Среднее время в течение 10-ти экспериментов по алгоритму PSO составило 0,18249 с, в то время, как по алгоритму GWO – 0,00377 с, что меньше примерно в 48 раз. Также стоит учесть, что PSO в результате работы выдавал значение глобального экстремума целевой функции, то есть находил одно устройство, наиболее подходящее для миграции контейнера, в отличие от GWO, который позволял найти группу устройств ($\alpha, \beta, \delta, \omega$), соответственно. Стоит отметить, что данное сравнение алгоритмов актуально в рамках исследуемой задачи. Как ранее было приведено в теоретической части, метаэвристические алгоритмы обладают своими особенностями ввиду собственной «проекции» с биологического мира, примерами кото-

рого они были вдохновлены. Соответственно, PSO может быть также достаточно эффективным решением в рамках других условий задачи.

Выводы

Исследования и разработки в области распределенных вычислений занимают немалую часть работ в современных и перспективных сетях и услугах. Одной из ожидаемых инфраструктурных технологий являются Fog, в частности, динамические. Данная технология позволит снизить нагрузку на ядро сети, замыкая пользовательский трафик, а также – приблизиться к достижению цели снижения энергозатрат вычислительной инфраструктуры в условиях бурного роста ЦОДов. В качестве практических исследований, в статье приводится разработанная модель и метод поиска группы Fog-устройств для последующей миграции типовых контейнеров одной из платформ FaaS. В качестве математической базы предлагается для решения сложной оптимизационной задачи использовать метаэвристические алгоритмы. В работе приводится практическое сравнение работы двух распространенных алгоритмов: GWO и PSO. В результате моделирования на основе экспериментальных данных эффективное решение поставленной задачи было достигнуто на основе алгоритма GWO.

Список источников

1. Market Overview // Straits research. URL: <https://straitresearch.com/report/data-center-equipment-market> (дата обращения 31.05.2024)
2. Колбанёв М.О., Палкин И.И., Пойманова Е.Д., Татарникова Т.М. Пути создания зеленых информационных технологий // Гидрометеорология и экология. 2021. № 62. С. 127–138. DOI:10.33933/2074-2762-2021-62-127-138. EDN:OEJEMQ
3. Manner J. Black software – the energy unsustainability of software systems in the 21st century // Oxford Open Energy. 2023. Vol. 2. DOI:10.1093/ooenergy/oia011
4. Alloghani M.A. Architecting Green Artificial Intelligence Products: Recommendations for Sustainable AI Software Development and Evaluation // Artificial Intelligence and Sustainability. Signals and Communication. Cham: Springer, 2024. PP. 65–86. DOI:10.1007/978-3-031-45214-7_4
5. Schwartz R., Dodge J., Smith N.A., Etzioni O. Green AI // Communications of the ACM. 2020. Vol. 63. Iss. 12. PP. 54–63. DOI:10.1145/3381831
6. Li Y., Zhu Z., Guan Y., Kang Y. Research on the structural features and influence mechanism of the green ICT transnational cooperation network // Economic Analysis and Policy. 2022. Vol. 75. PP. 734–749. DOI:10.1016/j.eap.2022.07.003
7. Кричевский Г.Е. Экология и «Зеленые технологии». Как сдержать превращение биосферы в техносферу? // НБИКС – Наука. Технологии. 2019. Т. 3. № 8. С. 22–26.
8. Волков А.Н. Туманность в перспективных сетях связи для услуг телеприсутствия // Электросвязь. 2024. № 4. С. 50–56.
9. Волков А.Н. Стабильность кластера в динамических туманных вычислениях // Электросвязь. 2024. № 6. С. 8–16.
10. Марочкина А.В. Моделирование и кластеризация трехмерной сети интернета вещей с применением метода оценки фрактальной размерности // Электросвязь. 2023. № 6. С. 60–66. DOI:10.34832/ELSV.2023.43.6.008. EDN:ZBNQKI
11. Марочкина А.В. Выбор головных узлов кластеров в трехмерных сетях Интернета вещей высокой плотности // Электросвязь. 2023. № 7. С. 26–32. DOI:10.34832/ELSV.2023.44.7.004. EDN:MKMNQZ

References

1. Straits research. Market Overview. URL: <https://straitresearch.com/report/data-center-equipment-market> (дата обращения 31.05.2024)
2. Kolbanev M.O., Palkin I.I., Poymanova E.D., Tatarnikova T.M. The Challenges of the Digital Economy. *Hydrometeorology and Ecology*. 2021;62:127–138. (in Russ.) DOI:10.33933/2074-2762-2021-62-127-138. EDN:OEJEMQ

3. Manner J. Black software – the energy unsustainability of software systems in the 21st century. *Oxford Open Energy*. 2023;2. DOI:10.1093/ooenergy/oiac011
4. Alloghani M.A. Architecting Green Artificial Intelligence Products: Recommendations for Sustainable AI Software Development and Evaluation. In: *Artificial Intelligence and Sustainability. Signals and Communication*. Cham: Springer; 2024. p.65–86. DOI:10.1007/978-3-031-45214-7_4
5. Schwartz R., Dodge J., Smith N.A., Etzioni O. Green AI. *Communications of the ACM*. 2020;63(12):54–63. DOI:10.1145/3381831
6. Li Y., Zhu Z., Guan Y., Kang Y. Research on the structural features and influence mechanism of the green ICT transnational cooperation network. *Economic Analysis and Policy*. 2022;75:734–749. DOI:10.1016/j.eap.2022.07.003
7. Krichevsky G.E. Ecology and Green Technologies. How to contain the transformation of the biosphere into the technosphere? *NBIKS – Nauka. Tekhnologii*. 2019;3(8):22–26. (in Russ.)
8. Volkov A.N. Nebula in promising communication networks for telepresence services. *Electrosvyaz*. 2024;4:50–56. (in Russ.)
9. Volkov A.N. Cluster stability in dynamic fog computing. *Elektrosvyaz*. 2024;6:8–16. (in Russ.)
10. Marochkina A.V. Modeling and clustering of a three-dimensional Internet of things network using the fractal dimension estimation method. *Elektrosvyaz*. 2023;6:60–66. (in Russ.) DOI:10.34832/ELSV.2023.43.6.008. EDN:ZBNQKI
11. Marochkina, A.V. Selection of cluster head nodes in high-density three-dimensional Internet of Things networks. *Electrosvyaz*. 2023;7:26–32. (in Russ.) DOI:10.34832/ELSV.2023.44.7.004. EDN:MKMNQZ

Статья поступила в редакцию 02.06.2024; одобрена после рецензирования 25.06.2024; принята к публикации 28.06.2024.

The article was submitted 02.06.2024; approved after reviewing 25.06.2024; accepted for publication 28.06.2024.

Информация об авторе:

ВОЛКОВ
Артем Николаевич

кандидат технических наук, доцент кафедры сетей связи и передачи данных
Санкт-Петербургского государственного университета телекоммуникаций им.
проф. М.А. Бонч-Бруевича
 <https://orcid.org/0009-0002-4296-1822>

Автор сообщает об отсутствии конфликтов интересов.

The author declares no conflicts of interests.

Научная статья

УДК 654.19:621.396.9

<https://doi.org/10.31854/1813-324X-2024-10-3-35-44>

Интерференция между поднесущими частотами в системе DRM

Юрий Алексеевич Ковалгин, kovalgin@sut.ru

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация

Аннотация

Актуальность. В России и в мире идет процесс постепенного перехода к цифровому радиовещанию (ЦРВ), обеспечивающему более высокое качество воспроизведения звуковых программ, значительную экономию радиочастотного ресурса, высокую помехозащищенность, существенный энергетический выигрыш по сравнению с аналоговыми системами радиовещания, возможность построения одночастотных сетей. Свойственной системам ЦРВ пороговый эффект требует учета влияния уровня интерференции между поднесущими (ИМП) OFDM-сигнала (OFDM, аббр. от англ. Orthogonal Frequency-Division Multiplexing) на изменение помехозащищенности систем ЦРВ в целом. Последнее обусловлено в том числе рассогласованием частот генераторов передающего и приемного трактов систем ЦРВ. Однако в рекомендациях Международного союза электросвязи (МСЭ-R, ITU-R) и доступных публикациях отсутствуют требования, предъявляемые к стабильности частот генераторов. Работа восполняет данный пробел.

Цель работы. Повышение помехозащищенности системы цифрового радиовещания DRM.

Методы. На основе анализа данных, имеющихся в публикациях, развит метод расчета уровня интерференции между поднесущими частотами в ситуации, когда при приеме OFDM-сигнала нет потери ортогональности поднесущих частот, а в радиоканале присутствует только белый шум (AWGN, аббр. от англ. Additive White Gaussian Noise).

Результаты. Исследовано и оценено влияние нормализованного частотного сдвига генераторов приемного и передающего трактов системы DRM на ухудшение отношения сигнал/шум при модуляции поднесущих частот QPSK для разных уровней помехозащищенности (PL0-PL3). Показано, что величина интерференции между поднесущими частотами OFDM-сигнала зависит от условий приема, вида модуляции, скорости кода, требуемого минимального значения напряженности электромагнитного поля сигнала передатчика и требуемого минимального отношения сигнал/шум в точке приема, от собственных шумов приемника и величины атмосферного шума. Достоверность полученных результатов подтверждена экспериментальными данными других исследователей.

Новизна. Полученные результаты являются новыми для системы DRM, при работе в режиме устойчивости E в случае стационарного приема и модуляции поднесущих частот QAM-4 прием OFDM-сигнала системы DRM становится невозможным уже при рассогласовании частот генераторов приемного и передающего трактов более чем на (2,07... 2, 32) Гц.

Практическая значимость. Знание уровня интерференции между поднесущими частотами OFDM-сигнала при расстройке частот генераторов передающего и приемного трактов систем ЦРВ необходимо для разработки национальных нормативных документов, регламентирующих эксплуатационные характеристики оборудования систем ЦРВ.

Ключевые слова: цифровое радиовещание, DRM, интерференция между поднесущими частотами OFDM-сигнала

Ссылка для цитирования: Ковалгин Ю.А. Интерференция между поднесущими частотами в системе DRM // Труды учебных заведений связи. 2024. Т. 10. № 3. С. 35–44. DOI:10.31854/1813-324X-2024-10-3-35-44. EDN:MDQDUX

Original research

<https://doi.org/10.31854/1813-324X-2024-10-3-35-44>

Interference Between Subcarrier Frequencies in DRM System

 Yuriy A. Kowalgin, kowalgin@sut.ru

The Bonch-Bruевич Saint Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Annotation

Relevance. In Russia and worldwide, there is a gradual transition to digital radio broadcasting. This transition offers higher quality sound reproduction, significant radio frequency resource savings, high interference resistance, substantial energy savings compared to analog broadcasting systems, and the ability to build single-frequency networks. The cliff effect inherent in DRM-systems necessitates considering the influence of the interference level between subcarriers (ICI, Intercarrier Interference) of the OFDM-signal (Orthogonal Frequency-Division Multiplexing) on the overall interference resistance of DRM-systems. This is partly due to the mismatch of generators in the transmitting and receiving paths of DRM-systems. However, the recommendations of the International Telecommunication Union (ITU-R) and available publications lack requirements for the stability of generators in the transmitting and receiving paths of digital radio broadcasting systems, which significantly affect their interference resistance. This work addresses this gap.

Goal. Improve the interference resistance of the DRM-system.

Methods. Based on the analysis and development of data available in publications, a method for calculating the interference level between subcarrier frequencies is proposed for situations where there is no loss of orthogonality of subcarrier frequencies during OFDM signal reception, and only white noise (AWGN - Additive White Gaussian Noise) is present in the radio channel.

Results. The impact of normalized frequency shift of generators in the DRM-system's transceiver path on the degradation of the signal-to-noise ratio when modulating subcarrier frequencies with QPSK for different levels of interference resistance (PL0-PL3) has been studied and evaluated. It is shown that the interference level between subcarrier frequencies of the OFDM signal depends on reception conditions, modulation type, code rate, required minimum signal strength of the transmitter's electromagnetic field, and the required minimum signal-to-noise ratio at the reception point, receiver's own noise, and atmospheric noise level. The validity of the obtained results is confirmed by experimental data from other researchers.

Novelty. The obtained results are new for the DRM-system. In mode stability under stationary reception and QAM-4 subcarrier frequency modulation, DRM-system OFDM signal reception becomes impossible when the frequency mismatch of the transceiver path generators exceeds (2.07...2.32) Hz.

Practical significance. Knowledge of the ICI level of the OFDM-signal when the frequency of the generators in the transmitting and receiving clocks of DRM-systems is detuned is necessary for developing national regulatory documents that govern the operational characteristics of DRM system equipment.

Keywords: digital broadcasting, DRM, interference between subcarrier frequencies of OFDM-signal

For citation: Kowalgin Yu.A. Interference Between Subcarrier Frequencies in DRM System. *Proceedings of Telecommunication Universities*. 2024;10(3):35–44. (in Russ.) DOI:10.31854/1813-324X-2024-10-3-35-44. EDN:MDQDUX

Введение

Технология OFDM (аббр. от англ. Orthogonal Frequency-Division Multiplexing, ортогональное мультиплексирование с частотным разделением) широко используется в телевизионном вещании (DVB, ISDB), радиовещании (DAB, DRM, РАВИС, ИВОС HD

Radio, CDR), мобильной связи (3GPP, Mobile WiMAX). При передаче OFDM-сигнал претерпевает целый ряд изменений, что при определенных условиях приводит к появлению межсимвольной интерференции (МСИ) и к интерференции между поднесущими частотами (ИМП) [1–5].

ИМП при передаче OFDM-сигнала возникает, когда приемник из-за наличия временного рассогласования с передатчиком не точно оценивает начало полезной (информационной) части OFDM-символа при старте прямого дискретного преобразования Фурье (ДПФ); иначе говоря, достоверно не знает, с какого дискретизированного отсчета начинается полезная часть OFDM-символа, а также, если имеет место смещение несущей частоты радиоканала.

При когерентном приеме должны быть синхронизированы также и фазы поднесущих частот OFDM-символов. Когерентный приемник должен «знать» амплитуды и фазы всех поднесущих частот при демодуляции.

До процесса демодуляции поднесущих частот OFDM-приемник должен: найти границы полезной части OFDM-символов; определить наиболее оптимальные моменты для временной синхронизации; оценить и скорректировать сдвиг несущей частоты принятого сигнала; осуществлять непрерывное слежение с целью минимизации текущих значений ИМП при изменении условий приема, характеристик приемопередающего оборудования и радиоканала.

МСИ – результат влияния предыдущего OFDM-символа на текущий. ИМП – результат потери ортогональности или сдвига по частоте в текущем OFDM-символе.

Системы синхронизации в цифровом радиовещании (ЦРВ) решают две задачи: захват и слежение. Захват обеспечивается, как правило, оценкой временного и частотного рассогласования; слежение предполагает наличие непрерывного процесса, в течение которого грубая оценка уточняется и минимизируется для получения требуемого результата. Работа посвящена исследованию и оценке влияния ИМП при передаче OFDM-сигнала системы DRM при сдвиге частот генераторов передающего и приемного трактов на изменение его помехозащищенности в ситуации, когда нет потери ортогональности поднесущих частот.

Основная часть

Напомним, что OFDM-сигнал на передающей стороне после обратного ДПФ до его переноса в полосу частот радиоканала может быть записан в виде [6–8]:

$$X(n) = \frac{1}{N} \sum_{k=0}^{N-1} X(k) \cdot e^{\frac{j2\pi nk}{N}}, \quad n = 0, 1, \dots, N - 1,$$

$$n = \frac{t}{T},$$

где n – дискретное время; t – текущее непрерывное время; T – интервал (период) дискретизации; N – число точек обратного ДПФ; k – индекс (номер) модулированной поднесущей частоты; $X(k)$ – комплексная огибающая модулированной k -й поднесущей.

Пусть при радиоприеме межсимвольные искажения отсутствуют, то есть точка старта прямого ДПФ выбрана в безопасном временном интервале (рисунок 1), где: CP – аббр. от англ. Cyclic Prefix, защитный интервал; светлая область – полезная (информационная) часть OFDM-символа; темная область – безопасная часть защитного интервала для старта прямого ДПФ. Тогда после выполнения процедуры прямого ДПФ OFDM-сигнал примет вид [6, 7]:

$$Y(k) = \sum_{n=0}^{N-1} X(n) \cdot e^{-\frac{j2\pi nk}{N}}, \quad k = 0, 1, \dots, N - 1,$$

где $Y(k)$ – модулированная поднесущая частота с индексом k .

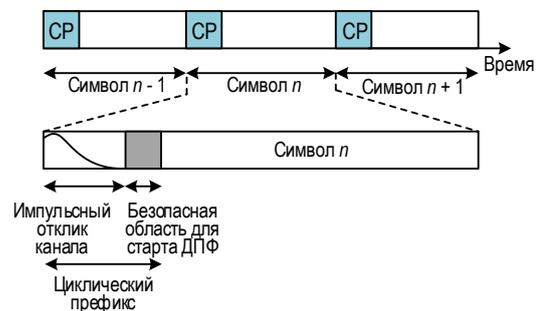


Рис. 1. Расположение окна прямого ДПФ относительно OFDM-символа

Fig. 1. Position of the Direct Discrete Fourier Transform Window with Respect to OFDM-Symbol

Предположим, что имеет место только рассогласование частот генераторов, искажения, обусловленные влиянием радиоканала, отсутствуют, в радиоканале присутствует только белый шум (AWGN, аббр. от англ. Additive White Gaussian Noise). Тогда после выполнения ряда преобразований [6] предшествующее выражение примет вид [7]:

$$Y(k) = \frac{1}{N} \sum_{n=0}^{N_U-1} X(k) \cdot e^{\frac{j2\pi nk\varepsilon}{N}} + \frac{1}{N} \sum_{l=0, l \neq k}^{N-1} X(l) \cdot e^{j2\pi n(l-k+\varepsilon)/N} + \sum_{n=0}^{N_U-1} W(n) \cdot e^{-j2\pi nk/N}, \quad \varepsilon = \frac{\Delta f_1}{\Delta f}.$$

Величина ε (рисунок 2) представляет собой нормализованный сдвиг поднесущей частоты передатчика при приеме, Δf_1 – сдвиг частоты генераторов, Δf – расстояние между поднесущими частотами OFDM-символа, равное $1/T_U$, где T_U – длительность полезной (информационной) части OFDM-символа. Заметим, что при целом значении ε ИМП не возникает, но имеет место сдвиг фазы поднесущих частот, дробное значение ε сопровождается при приеме появлением ИМП.

Первое слагаемое в (1) представляет собой оценку принятой поднесущей частоты с индексом k , амплитуда и фаза которой изменилась вследствие смещения частоты при приеме, и может быть представлено в виде [8–10]:

$$X(k) = \frac{\sin(\pi\varepsilon)}{N \cdot \sin(\pi\varepsilon/N)} X(k). \quad (2)$$

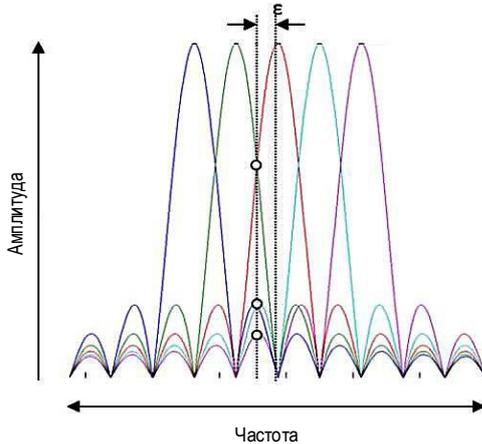


Рис. 2. К появлению ИМП при сдвиге частот генераторов передающего и приемного трактов системы ЦРВ

Fig. 2. On the Appearance of Interference Between Subcarrier Frequencies in Case of a Frequency Shift the DRM-system Transmitting and Receiving Generator Channels

Второе слагаемое в (1) характеризует величину ИМП для частоты с индексом k , обусловленной влиянием остальных поднесущих частот OFDM-символа и определяется как:

$$\hat{I}(k) = e^{j2\pi\varepsilon(N-1)/N} \times \sum_{l=0, l \neq k}^{N_U-1} \frac{\sin(\pi(l-k+\varepsilon))}{N \cdot \sin(\pi(l-k+\varepsilon)/N)} X(l) \times e^{\frac{j\pi(l-k)(N-1)}{N}}, \quad (3)$$

где N_U – число поднесущих частот в OFDM-символе.

Третье слагаемое в (1) – это AWGN. Видно, что в выражении (3) величина ИМП при передаче OFDM-символа зависит от длины выборки N дискретизированного OFDM-сигнала.

В [11] приводится и другое выражение для оценки величины ИМП для поднесущей с индексом k при сдвиге несущей частоты приемника:

$$X(k) = \frac{\sin(\pi\varepsilon)}{\pi\varepsilon} X(k)$$

и

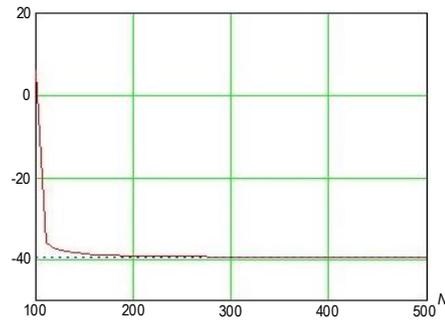
$$\hat{I}(k) = \sum_{l=0, l \neq k}^{N_U-1} \frac{\sin(\pi(l-k+\varepsilon))}{\pi(l-k+\varepsilon)} X(k). \quad (4)$$

Для всех поднесущих частот OFDM-символа суммарная величина полезного сигнала и ИМП может быть найдена как:

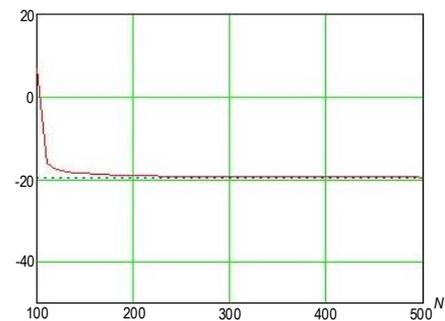
$$\hat{I}_\Sigma = \sum_{k=0}^{N_U-1} \frac{\sin(\pi\varepsilon)}{\pi\varepsilon} X(k) \quad (5)$$

$$\hat{I}_\Sigma = \sum_K \sum_{l=0, l \neq k}^{N_U-1} \frac{\sin(\pi(l-k+\varepsilon))}{N \cdot \sin(\frac{\pi(\varepsilon+l-k)}{N})} X(k).$$

Результаты вычисления величин ИМП по формулам (3) – сплошная кривая, и (4) – пунктирная линия, представленные на рисунке 3, дают практически одинаковые результаты при $N \geq 2k$; здесь и далее величина ИМП дана в дБ.



а)



б)

Рис. 3. Оценка уровня ИМП в системе DRM для поднесущей частоты с индексом $k = 106$: а) $\varepsilon = 0,001$; б) $\varepsilon = 0,01$

Fig. 3. Estimation of the Level of Interference Between Subcarrier Frequencies ($k = 106$): а) $\varepsilon = 0,001$; б) $\varepsilon = 0,01$

Для большей наглядности на рисунке 4 приведены результаты вычислений величины ИМП OFDM-сигнала для случая, когда число поднесущих частот равно $N_U = 213$, расстояние между ними по частоте $\Delta f = 444,44$ Гц.

Из рисунка видно, что:

- уровень ИМП для поднесущих, расположенных в центре полосы частот OFDM-сигнала, существенно выше, чем на краях, ибо на них влияют поднесущие с обеих сторон спектра;

- для 213 поднесущих частот, что имеет место в системе DRM при работе в режиме устойчивости E, при числе отсчетов дискретизированного OFDM-сигнала ≥ 426 , различие результатов оценки ИМП по формулам (3) и (4) не превышает 0,1 дБ для поднесущих частот, расположенных в центре полосы частот OFDM-сигнала (рисунок 5).

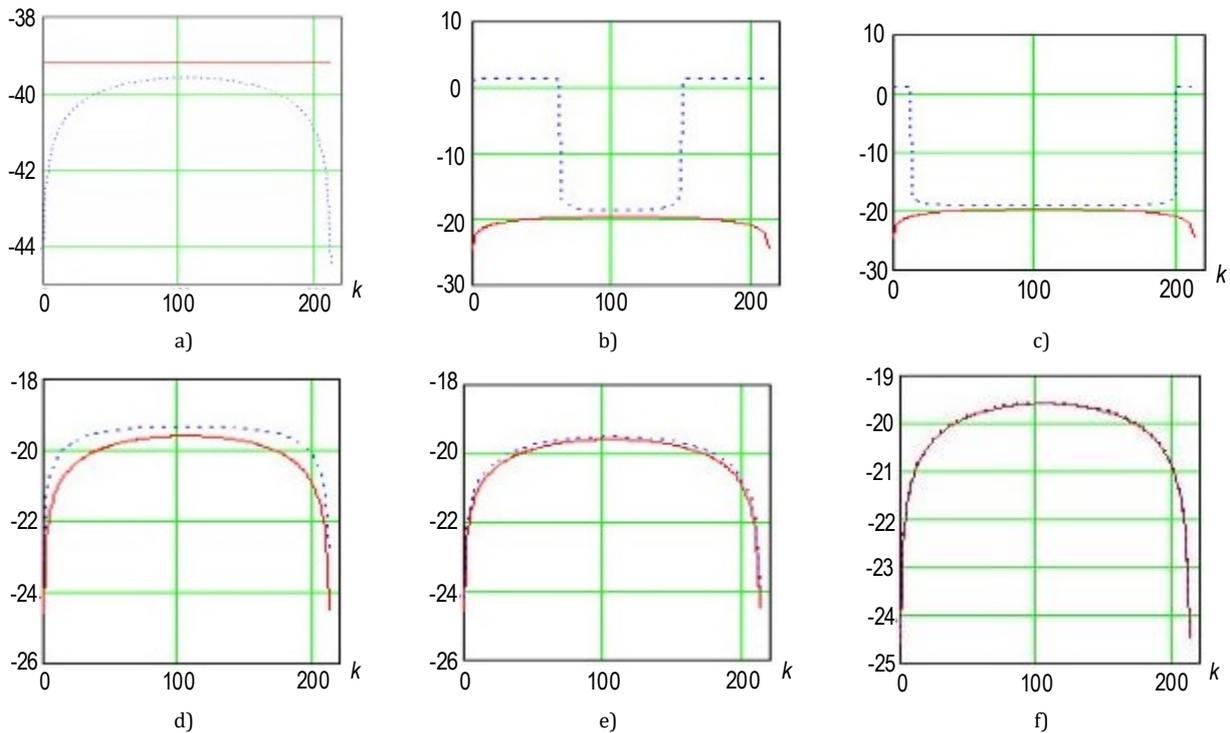


Рис. 4. Результаты вычислений уровня ИМП по выражениям (3) – пунктирные кривые и (4) – сплошные кривые: а) $\epsilon = 0,0001, N = 213$; б) $\epsilon = 0,01, N = 150$; в) $\epsilon = 0,02, N = 200$; д) $\epsilon = 0,01, N = 250$; е) $\epsilon = 0,01, N = 426$; ф) $\epsilon = 0,01, N \geq 750$
 Fig. 4. Calculation of the Level of Interference Between Subcarrier Frequencies, Using Equations (3) – dotted lines and (4) – solid lines: а) $\epsilon = 0,0001, N = 213$; б) $\epsilon = 0,01, N = 150$; в) $\epsilon = 0,02, N = 200$; д) $\epsilon = 0,01, N = 250$; е) $\epsilon = 0,01, N = 426$; ф) $\epsilon = 0,01, N \geq 750$

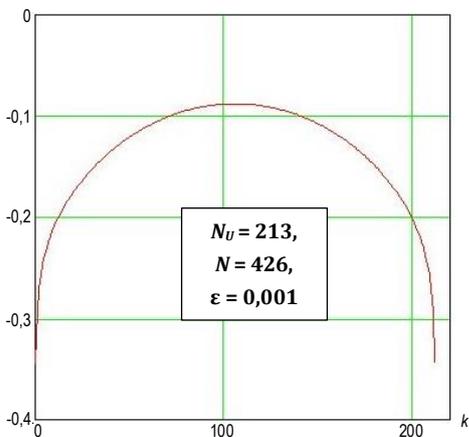


Рис. 5. Различия в результатах вычислений уровня ИМП OFDM-сигнала системы DRM по выражениям (3) и (4)
 Fig. 5. Difference in Calculation Results of the Level of Interference Between Subcarrier Frequencies of OFDM-Signal DRM System, from Equations (3) and (4)

Оценим, используя полученные выражения, влияние частотного сдвига генераторов передающего и приемного трактов на величину ИМП и на изменение помехозащищенности OFDM-сигнала для системы ЦРВ DRM при работе в режиме устойчивости E и модуляции QPSK (аббр. от англ. Quadrature Phase Shift Keying, квадратурная фазовая модуляция). Система DRM в этом режиме работы имеет 213 активных ортогональных поднесущих частот, расстояние

между ними равно 444,44 Гц, полная длительность OFDM-символа – 2,5 мс, длительность его полезной (информационной) части – 2,25 мс, полоса частот радиоканала – 96 кГц. При модуляции QPSK амплитуда поднесущих частот остается неизменной; в расчетах она принята равной $X(k) = 1$. Результаты выполненных вычислений представлены на рис. 6, 7 и 8.

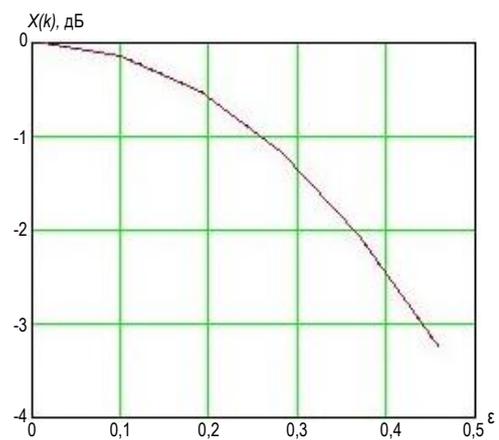


Рис. 6. Изменение амплитуды поднесущих частот от величины нормализованного частотного сдвига ϵ генераторов передающего и приемного трактов для системы DRM (режим устойчивости E)
 Fig. 6. Change of the Amplitude of Subcarrier Frequencies versus Normalized Frequency Shift ϵ of the DRM System Transmitting and Receiving Generator Channels (Stability Regime E)

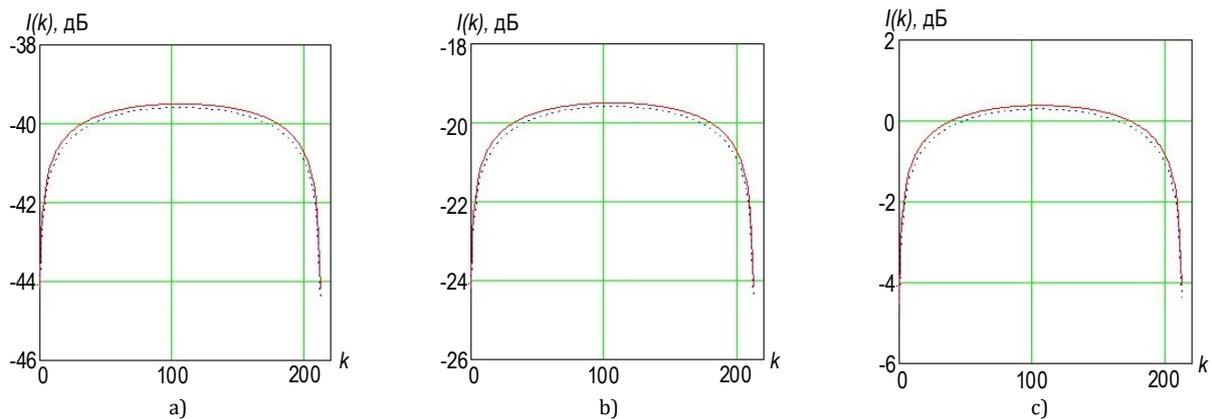


Рис. 7. Уровни ИМП при наличии частотного сдвига генераторов, передающего и приемного трактов для системы DRM при работе в режиме устойчивости E , $X(k) = 1$, модуляция QPSK: а) $\varepsilon = 0,001$; б) $\varepsilon = 0,01$; в) $\varepsilon = 0,1$ (пунктирные кривые – расчет по формуле (3), сплошные линии – расчет по формуле (4))

Fig. 7. Levels of the Interference Between Subcarrier Frequencies in Case of Having a Frequency Shift Between the DRM System Transmitting and Receiving Generator Channels in the Stability Regime E , $X(k) = 1$, QPSK Modulation: а) $\varepsilon = 0,001$; б) $\varepsilon = 0,01$; в) $\varepsilon = 0,1$ (Dotted Lines – Calculations by Equation (3), Solid Lines – Calculations by Equation (4))

Анализ полученных результатов позволяет сформулировать следующие предварительные выводы.

Во-первых, формулы (3) и (4) дают практически совпадающие результаты уже при $N \geq 2k$. В этом случае различие в оценке величины ИМП для любых значений индексов поднесущих частот k не превышает 0,1 дБ.

Во-вторых, уровень ИМП зависит от величины нормализованного частотного сдвига ε и от индекса поднесущей частоты k : он меньше для крайних поднесущих частот и больше для поднесущих частот, расположенных в центре полосы частот радиоканала. При всех значениях частотного сдвига различие в уровне ИМП для крайних и центральных поднесущих частот OFDM-сигнала составляет $\approx 4,7$ дБ (рисунок 8а).

В-третьих, увеличение нормализованного сдвига по частоте в интервале $\varepsilon = 0,0001 \dots 0,1$ изменяет уровень ИМП для поднесущих частот, расположенных в центре полосы частот OFDM-сигнала, от $-40,5$ до $0,5$ дБ. В-четвертых, величина ИМП для поднесущих, расположенных в центре полосы частот радиоканала, практически не зависит от их числа в OFDM-символе, в то время как суммарное значение ИМП в целом для OFDM-сигнала растет с увеличением числа поднесущих частот. Для системы DRM (режим устойчивости E) при каждом значении сдвига частоты суммарное значение оказывается выше уровня ИМП для поднесущей частоты с индексом $k = 106$ примерно на $20 \cdot \lg 213 = 46,5$ дБ (рисунок 8б).

Величина ИМП зависит от условий приема, вида модуляции, скорости кода, требуемого минимального значения напряженности электромагнитного поля (E_{\min}) сигнала передатчика и требуемого минимального отношения сигнал/шум (SNR_{\min}) в точке приема, от собственных шумов приемника и величины атмосферного шума.

Перечисленные выше источники шума имеют разную природу возникновения и при оценке могут считаться статистически независимыми. Эти параметры влияют на вероятность появления битовой ошибки, величина которой для условий комфортного приема не должна превышать 10^{-4} [13–16]. Напомним, что изменение отношения сигнал/шум от порогового значения на величину $\Delta = 1$ дБ делает прием сигнала системы DRM практически невозможным [13].

Оценим влияние ИМП на прием DRM-сигнала в режиме устойчивости E , используя экспериментальные данные (таблица 1), полученные для условий стационарного приема при модуляции поднесущих частот QAM-4 [17].

ТАБЛИЦА 1. Значения требуемого минимального медианного значения напряженности поля $E_{\text{тр},\min}$ сигнала передатчика и требуемого минимального значения отношения сигнал/шум $SNR_{\text{тр},\min}$ для разных значений скорости кода в режиме стационарного приема на штыревую антенну в помещении на расстоянии 12 км от телебашни в Санкт-Петербурге, для системы DRM при работе в режиме устойчивости E (несущая частота DRM-передатчика 95,7 МГц)

TABLE 1. Values of the required minimum median voltage field $E_{\text{тр},\min}$ of the transmitter signal and the required minimum signal-to-noise ratio $SNR_{\text{тр},\min}$ for different encoding rates, for stationary receiving on a pin antenna inside a building at a distance of 12 km from the St.-Petersburg's transmitting tower, for a DRM system operating in the stability regime E (main frequency of DRM-transmitter is 95,7 MHz)

Скорость кода	Медианный уровень напряженности поля сигнала передатчика, дБ (мкВ/м)	Требуемое минимальное значение SNR, дБ
0,250 (PL0)	16,997	2,27
0,333 (PL1)	17,437	2,71
0,400 (PL2)	17,657	2,93
0,500 (PL3)	18,817	4,09

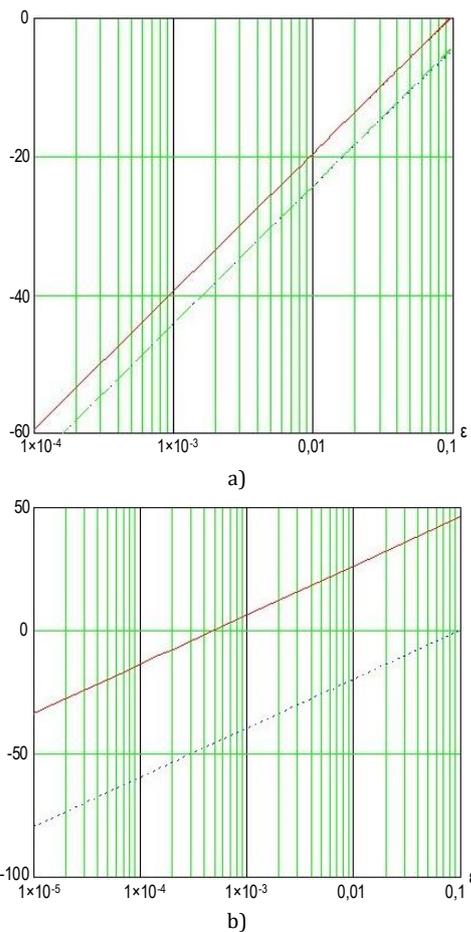


Рис. 8. Уровни ИМП от величины нормализованного частотного сдвига ϵ генераторов передающего и приемного трактов: а) верхняя кривая для поднесущей частоты с индексом $k = 106$, нижние две (совпавшие) кривые для крайних поднесущих частот с индексами $k = 0$ и $k = 212$, соответственно, $X(k) = 1$, модуляции QPSK, $N = 426$; б) нижняя кривая получена для поднесущей частоты с индексом $k = 106$, верхняя кривая – суммарные значения ИМП для всех поднесущих частот OFDM-сигнала, $X(k) = 1$, модуляция QPSK

Fig. 8. Levels of the Interference Between Subcarrier Frequencies versus Normalized Frequency Shift ϵ of the Transmitting and Receiving Generator Channels: a) Upper Curve Corresponds to Subcarrier Frequency Index $k = 106$, Lower Two Curves are for Boundary Subcarrier Frequencies with Indices $k = 0$ and $k = 212$, Respectively; $X(k) = 1$, QPSK Modulation, $N = 426$; b) Lower Curve is Obtained for Subcarrier Frequency Index $k = 106$, Upper Curve – Summarized Values of ICI for all Subcarrier Frequencies of OFDM-Signal, $X(k) = 1$, QPSK modulation

Предположим, что в точке приема медианные уровни напряженности поля сигнала передатчика и требуемые минимальные значения отношения сигнал/шум соответствуют значениям, приведенным в таблице. При появлении частотного сдвига генераторов приемопередающего тракта возникла ИМП, ее уровень можно определить с помощью выражения:

$$U_{\text{ИМП}} = 20 \lg \sqrt{\left(\frac{E_{\text{тр.мин}}}{10^{(SNR_{\text{тр.мин}} - \Delta)/20}}\right)^2 - \left(\frac{E_{\text{тр.мин}}}{10^{SNR_{\text{тр.мин}}/20}}\right)^2}, \quad (6)$$

где $U_{\text{ИМП}}$ – величина ИМП при наличии частотного сдвига генераторов приемопередающего тракта;

$E_{\text{тр.мин}}$ и $SNR_{\text{тр.мин}}$ – требуемые для выбранного условия приема, вида модуляции и скорости кода минимальные значения напряженности электромагнитного поля сигнала передатчика и отношения сигнал/шум в точке приема; Δ – изменение (ухудшение) отношения сигнал/шум из-за появления ИМП в OFDM-сигнале при приеме.

Рассчитанные по формуле (6) с использованием данных таблицы 1 уровни ИМП позволяют, используя выражение (5), определить допустимую величину нормализованного частотного сдвига поднесущих частот. Результаты данных вычислений представлены на рисунке 9а.

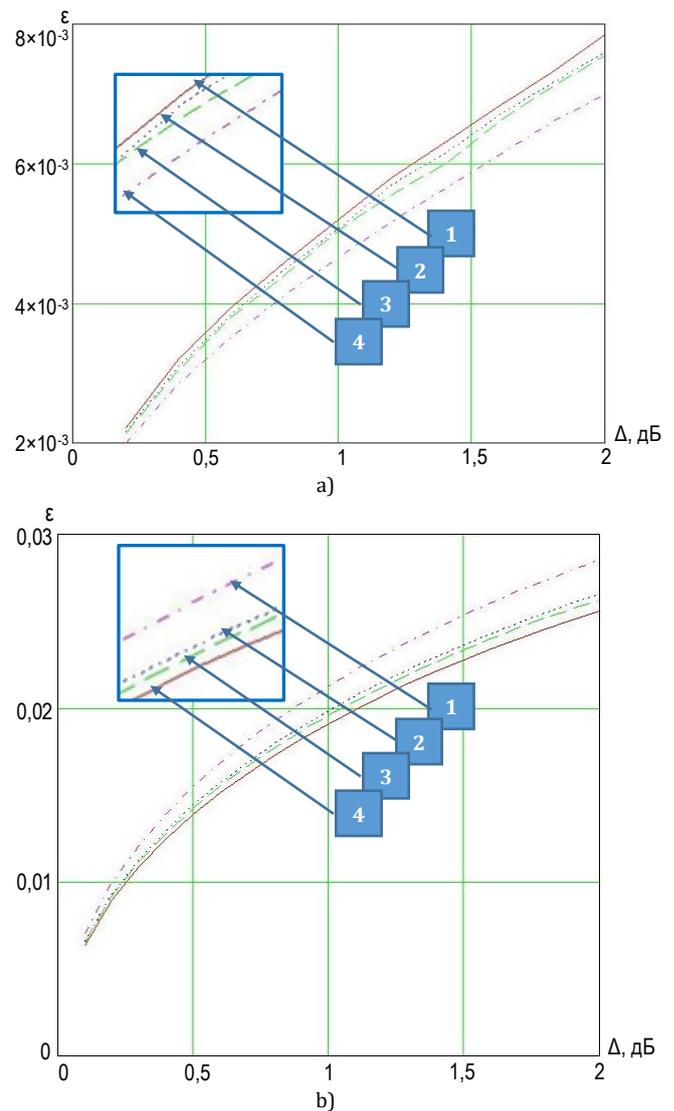


Рис. 9. Изменение нормализованного частотного сдвига ϵ генераторов приемопередающего тракта системы DRM (режим устойчивости E, модуляция поднесущих частот QAM-4) от изменения SNR, вызванного появлением ИМП

Fig. 9. Change of the Normalized Frequency Shift ϵ of the Transmitting and Receiving Generator Channel of a DRM System (Stability Regime E, QAM-4 Modulation) Versus SNR Change Due to Appearance of the Interference Between Carrying Frequencies

Здесь кривая 1 – $E_{\text{тр.мин}} = 16,997$ дБ (мкВ/м), $\text{SNR} = 2,27$ дБ; кривая 2 – $E_{\text{тр.мин}} = 17,437$ дБ (мкВ/м), $\text{SNR} = 2,71$ дБ; кривая 3 – $E_{\text{тр.мин}} = 17,657$ дБ (мкВ/м), $\text{SNR} = 2,93$ дБ; кривая 4 – $E_{\text{тр.мин}} = 18,817$ дБ (мкВ/м), $\text{SNR} = 4,09$ дБ (расчет по формуле 3).

Для системы DRM при работе в режиме устойчивости E и модуляции QAM-4 величина порога, при котором прием становится невозможным, составляет $\Delta = 1$ дБ [13]. Для данного значения величина нормализованного частотного сдвига (рисунок 9а) не должна превышать: $\varepsilon = 0,00521$ ($\Delta f_1 = 2,32$ Гц) – кривая 1; $\varepsilon = 0,00508$ ($\Delta f_1 = 2,26$ Гц) – кривая 2; $\varepsilon = 0,00505$ ($\Delta f_1 = 2,24$ Гц) – кривая 3; $\varepsilon = 0,00466$ ($\Delta f_1 = 2,07$ Гц) – кривая 4.

Заметим, что в публикации [7] приводится другое выражение для оценки уровня ИМП при OFDM-передаче (7) и (8), где $u^2_{\text{ИМП}=0}$ – мощность шума при отсутствии сдвига несущей частоты; $u^2_{\text{ИМП}\neq 0}$ – мощность сигнала ИМП при наличии частотного сдвига несущей частоты при приеме.

Результаты оценки уровня ИМП по формулам (7) и (8) приведены на рисунке 9б. Здесь кривая 1 – $E_{\text{тр.мин}} = 18,817$ дБ (мкВ/м), $\text{SNR} = 4,09$; кривая 2 – $E_{\text{тр.мин}} = 16,657$ дБ (мкВ/м), $\text{SNR} = 2,93$ дБ; кривая 3 – $E_{\text{тр.мин}} = 17,437$ дБ (мкВ/м), $\text{SNR} = 2,71$ дБ; кривая 4 – $E_{\text{тр.мин}} = 16,997$ дБ (мкВ/м), $\text{SNR} = 2,27$ дБ (расчет по формуле 8). По данным публикации [7], для системы DRM при работе в режиме устойчивости E и модуляции QAM-4 величина нормализованного частотного сдвига (см. рисунок 9б) при $\Delta = 1$ дБ не

должна превышать следующих значений: $\varepsilon < 0,019$ ($\Delta f_1 < 8,44$ Гц) – кривая 1; $\varepsilon < 0,02$ ($\Delta f_1 < 8,89$ Гц) – кривая 2; $\varepsilon < 0,02$ ($\Delta f_1 < 8,89$ Гц) – кривая 3; $\varepsilon < 0,021$ ($\Delta f_1 < 9,3$ Гц) – кривая 4.

Сравнение полученных результатов показало, что расчет по формулам, предложенным в данной работе, дает существенно более жесткие требования к рассогласованию частот генераторов приемопередающего тракта для системы DRM (режим устойчивости E , модуляция QAM-4, условие стационарного приема F_x , $\Delta = 1$ дБ): (2,07... 2,32 Гц) $\ll \ll$ (8,44 ... 9,3 Гц). Заметим, что расчет по формулам (7) и (8) не учитывает такие факторы как: условие приема и требуемые для уверенного приема минимальные значения напряженности электромагнитного поля сигнала передатчика, а также SNR и с этой точки зрения является более приближенным.

В качестве дополнения на рисунке 10 приведены результаты вычислений допустимого частотного сдвига ε , приведенные в [11]. Смещение частоты при приеме приводит к ухудшению отношения сигнал/шум и, как следствие, разрушает сигнальное созвездие.

Видно, что при модуляции QPSK (QAM-4) прием цифрового сигнала становится невозможным уже при $\varepsilon = 0,5\%$, что дает для системы DRM значение $\Delta f_1 = 2,22$ Гц, которое хорошо согласуется с полученными в работе данными (2,07... 2,32) Гц и подтверждает их достоверность.

$$\varepsilon < \frac{\sqrt{3}}{\pi} \cdot \sqrt{\frac{1}{\gamma_{\text{ИМП}=0}} \cdot \left(1 - \frac{1}{\Delta\gamma}\right)}, \quad (7)$$

$$\gamma_{\text{ИМП}=0} = u^2_{\text{ИМП}=0} \left(10^{[E_{\text{тр.мин}}/(SNR_{\text{тр.мин}}/20)]}\right)^2, \quad \Delta\gamma = u^2_{\text{ИМП}\neq 0} = \left(\frac{10^{E_{\text{тр.мин}}/(SNR_{\text{тр.мин}}/20)}}{10^{E_{\text{тр.мин}}/[E_{\text{тр.мин}}/(SNR_{\text{тр.мин}}-\Delta)/20]}}\right)^2$$

или

$$\varepsilon < \frac{\sqrt{3}}{\pi} \cdot \sqrt{\left(\frac{1}{10^{E_{\text{тр.мин}}/(SNR_{\text{тр.мин}}/20)}}\right)^2 \cdot \left(1 - \left(\frac{10^{E_{\text{тр.мин}}/(SNR_{\text{тр.мин}}/20)}}{10^{E_{\text{тр.мин}}/[E_{\text{тр.мин}}/(SNR_{\text{тр.мин}}-\Delta)/20]}}\right)^2\right)}. \quad (8)$$

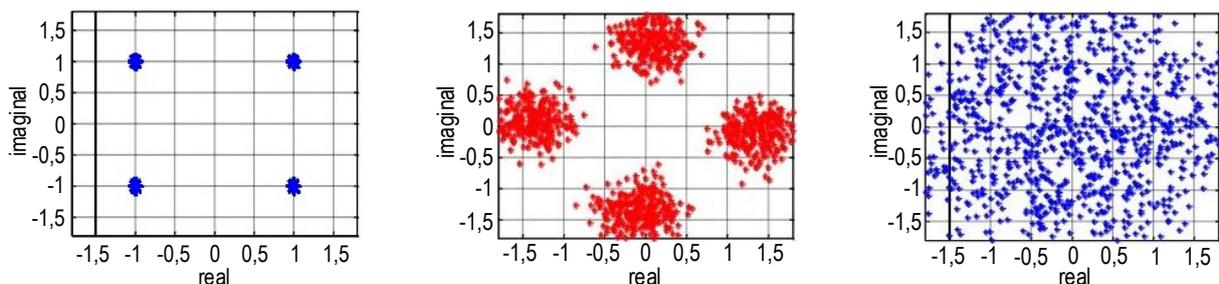


Рис. 10. Влияние нормализованного сдвига частоты на вид сигнальных созвездий при модуляции поднесущих частот QPSK: а) $\varepsilon = 0\%$ ($\Delta f_1 = 0$ Гц); б) $\varepsilon = 0,3\%$ ($\Delta f_1 = 1,33$ Гц); в) $\varepsilon = 0,5\%$ ($\Delta f_1 = 2,22$ Гц)

Fig. 10. Influence of the Normalized Frequency Shift on Signal-Map Distribution on QPSK Modulation:
 a) $\varepsilon = 0\%$ ($\Delta f_i = 0$ Hz); b) $\varepsilon = 0,3\%$ ($\Delta f_i = 1,33$ Hz); c) $\varepsilon = 0,5\%$ ($\Delta f_i = 2,22$ Hz)

Заключение

1) Сдвиг частот генераторов передающего и приемного трактов системы DRM приводит к появлению ИМП. Ее величина зависит от множества факторов: от числа поднесущих частот в OFDM-символе, вида модуляции, скорости кода, условий приема, уровня атмосферного шума, собственных шумов приемопередающего тракта.

2) Для системы DRM при работе в режиме устойчивости E в случае стационарного приема F_x и модуляции поднесущих частот QAM-4 прием OFDM-

сигнала становится невозможным уже при рассогласовании частот генераторов приемопередающего трактов более, чем на (2,07... 2,32) Гц.

3) Полученные результаты наглядно подтверждают необходимость жесткой частотной синхронизации приемопередающего оборудования системы ЦРВ DRM, что может быть реализовано программным путем.

Список источников

1. Бакулин М.Г., Крейнделин В.Б., Шлома А.М., Шумов А.П. Технология OFDM: учебное пособие для вузов. М.: Горячая линия – Телеком, 2016. 352 с. EDN:YPURRV
2. Cho Y.S., Kim J., Yang W.Y., Kang C.G. MIMO-OFDM Wireless Communications with Matlab. Singapore: John Wiley & Sons, 2010. 544 p.
3. Fazel K., Kaiser S. Multi-Carrier and Spread Spectrum Systems: from OFDM and MC-CDMA to LTE and WiMAX. John Wiley & Sons, 2008. 384 p.
4. Kung T.L. Synchronization and Coding in Wireless Communications Systems. Dissertation Submitted to the Faculty of the Graduate School of the University of Minnesota. 2013. p. 156.
5. Younis S.B.T. Synchronization Algorithms and Architectures for Wireless OFDM Systems. PhD Thesis. Newcastle University, 2012. 197 p. URL: <http://hdl.handle.net/10443/1417> (Accessed 20.04.2024)
6. Батырев А.И. Оценка влияния сдвига несущей частоты на качество принимаемого сигнала // Омский научный вестник. 2015. № 3(143). С. 259–262. EDN:VCNUSF
7. Speth M., Fechtel S.A., Fock G., Meyr H. Optimum Receiver Design for Wireless Broad-Band Systems Using OFDM. Part I // IEEE Transactions on Communications. 1999. Vol. 47. Iss. 11. PP. 1668–1677. DOI:10.1109/26.803501
8. Morelli M., Kuo C.C.J., Pun M.O. Synchronization Techniques for Orthogonal Frequency Division Multiple Access (OFDMA): A Tutorial Review // Proceedings of the IEEE. 2007. Vol. 95. Iss. 7. PP. 1394–1427. DOI:10.1109/JPROC.2007.897979
9. Sun Z., Peng T., Wan W. A novel sampling synchronization scheme for OFDM-based system with unified reference clock // Journal on Wireless Communications and Networking. 2012. Vol. 2012. P. 368. DOI:10.1186/1687-1499-2012-368
10. Zhao Y., Häggman S.-G. Inter-carrier Interference Self-Cancellation Scheme for OFDM Mobile Communication Systems // IEEE Transactions on Communications. 2001. Vol. 49. Iss. 7. PP. 1185–1191. DOI:10.1109/26.935159
11. Raboh M.S.A., Al Bassiouni A.A.M., Zakaria H.M., El Bahy M.M. Performance Analysis of OFDM Systems Subjected to Carrier Frequency Offset in Fading Communication Channels // International Journal of Engineering Research & Technology. 2015. Vol. 4. Iss. 7. URL: <https://www.ijert.org/research/performance-analysis-of-ofdm-systems-subjected-to-carrier-frequency-offset-in-fading-communication-channels-IJERTV4IS070404.pdf> (Accessed 20.04.2024)
12. Жерносеков Р.А., Першин В.Т. Синхронизация системы мультиплексирования с ортогональным разделением частот // Доклады БГУИР. 2017. № 4(106). С. 5–11. EDN:ZDINJL
13. Ковалгин Ю.А. Цифровое радиовещание: системы и технологии. М.: Горячая линия – Телеком, 2021. 580 с.
14. ETSI ES 201 980 v4.1.2 (2017-04). Digital Radio Mondiale (DRM); System.
15. Specification // ETSI. 196 p. URL: <http://www.etsi.org/standards-search> (Accessed 20.04.2024)
16. Рекомендация ITU-R BS.1660-8 (10/2015). Техническая основа для планирования наземного цифрового звукового радиовещания в полосе ОВЧ.
17. Planning Parameters for DRM Mode E ('DRM+') concerning the use in VHF bands I, II and III V 3.0. 2011. URL: https://drm-radio-kl.eu/berichte_vortraege/drmplus-hdradio/Planning-parameters-for-DRMplus-V30.pdf
18. Ковалгин Ю.А. Частотное планирование сетей цифрового радиовещания. СПб.: СПбГУТ, 2021. 194 с. (Accessed 20.04.2024)

References

1. Bakulin M.G., Kreindelin V.B., Shloma A.M., Shumov A.P. *OFDM Technology*. Moscow: Goryachaya liniya – Telekom Publ.; 2016. 352 p. (in Russ.) EDN:YPURRV
2. Cho Y.S., Kim J., Yang W.Y., Kang C.G. *MIMO-OFDM Wireless Communications with Matlab*. Singapore: John Wiley & Sons; 2010. 544 p.
3. Fazel K., Kaiser S. *Multi-Carrier and Spread Spectrum Systems: from OFDM and MC-CDMA to LTE and WiMAX*. John Wiley & Sons; 2008. 384 p.
4. Kung T.L. *Synchronization and Coding in Wireless Communications Systems*. Dissertation Submitted to the Faculty of the Graduate School of the University of Minnesota. 2013. p. 156.

5. Younis S.B.T. *Synchronization Algorithms and Architectures for Wireless OFDM Systems*. PhD Thesis. Newcastle University; 2012. 197 p. URL: <http://hdl.handle.net/10443/1417> [Accessed 20.04.2024]
6. Batyrev A.I. The influence of carrier frequency offset on quality of received OFDM signal. *Omsk Scientific Bulletin*. 2015;3(143):259–262. (in Russ.) EDN:VCNUSF
7. Speth M., Fechtel S. A., Fock G., Meyr H. Optimum Receiver Design for Wireless Broad-Band Systems Using OFDM. Part I. *IEEE Transactions on Communications*. 1999;47(11):1668–1677. DOI:10.1109/26.803501
8. Morelli M., Kuo C.C.J., Pun M.O. Synchronization Techniques for Orthogonal Frequency Division Multiple Access (OFDMA): A Tutorial Review. *Proceedings of the IEEE*. 2007;95(7):1394–1427. DOI:10.1109/JPROC.2007.897979
9. Sun Z., Peng T., Wan W. A novel sampling synchronization scheme for OFDM-based system with unified reference clock. *Journal on Wireless Communications and Networking*. 2012;2012:368. DOI:10.1186/1687-1499-2012-368
10. Zhao Y., Häggman S.-G. Inter-carrier Interference Self-Cancellation Scheme for OFDM Mobile Communication Systems. *IEEE Transactions on Communications*. 2001;49(7):1185–1191. DOI:10.1109/26.935159
11. Raboh M.S.A., Al Bassiouni A.A.M., Zakaria H.M., El Bahy M.M. Performance Analysis of OFDM Systems Subjected to Carrier Frequency Offset in Fading Communication Channels. *International Journal of Engineering Research & Technology*. 2015;4(7). URL: <https://www.ijert.org/research/performance-analysis-of-ofdm-systems-subjected-to-carrier-frequency-offset-in-fading-communication-channels-IJERTV4IS070404.pdf> [Accessed 20.04.2024]
12. Zhernosekov R.A., Pershin V.T. The synchronization of the orthogonal frequency division multiplexing system. *Doklady BGUIR*. 2017;4(106):5–11. (in Russ.) EDN:ZDINJL
13. Kovalgin Y.A. *Digital broadcasting: systems and technologies*. Moscow: Goryachaya liniya – Telekom Publ.; 2021, 580 p. (in Russ.)
14. ETSI ES 201 980 v.4.1.2. *Digital Radio Mondiale (DRM); System*. April 2017.
15. ETSI. Specification. 196 p. URL: <http://www.etsi.org/standards-search> [Accessed 20.04.2024]
16. Rec. ITU-R BS.1660-8. *Technical basis for on-ground digital audio broadcasting planning in the UHF range*. October 2015.
17. *Planning Parameters for DRM Mode E ('DRM+') concerning the use in VHF bands I, II and III V 3.0*. 2011. URL: https://drm-radio-kl.eu/berichte_vortraege/drmplus-hdradio/Planning-parameters-for-DRMplus-V30.pdf [Accessed 20.04.2024]
18. Kovalgin Y.A. *Frequency planning of digital broadcasting networks*. St.-Petersburg: The Bonch-Bruevich Saint Petersburg State University of Telecommunications Publ.; 2021. 194 p. (in Russ.)

Статья поступила в редакцию 22.04.2024; одобрена после рецензирования 25.05.2024; принята к публикации 09.06.2024.

The article was submitted 22.04.2024; approved after reviewing 25.05.2024; accepted for publication 09.06.2024.

Информация об авторе:

**КОВАЛГИН
Юрий Алексеевич**

доктор технических наук, профессор, профессор кафедры телевидения и метрологии Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича

 <https://orcid.org/0000-0002-6753-8062>

Ковалгин Ю.А. является членом редакционного совета журнала «Труды учебных заведений связи» с 2016 г., но не имеет никакого отношения к решению опубликовать эту статью. Статья прошла принятую в журнале процедуру рецензирования. Об иных конфликтах интересов автор не заявлял.

Kovalgin Yu.A. has been a member of the editorial board of the journal "Proceedings of Telecommunication Universities" since 2016, but has nothing to do with the decision to publish this article. The article has passed the review procedure accepted in the journal. The author has not declared any other conflicts of interest.

Научная статья

УДК 512.624.5

<https://doi.org/10.31854/1813-324X-2024-10-3-45-58>

Кодовое разделение на основе двойного расширения спектра сигнала

✉ Дмитрий Сергеевич Кукунин, kukunin.ds@sut.ru

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация

Аннотация

Актуальность: работа затрагивает проблемы широкополосной модуляции применительно к задачам множественного доступа. Обозначены преимущества кодового уплотнения в процессе расширения спектра сигнала, которое, как показано в работе, является перспективным методом параллельной передачи данных. **Целью** настоящей работы является, во-первых, повышение эффективности применения адресных последовательностей для идентификации отправителя и получателя информации; во-вторых, организация параллельного процесса передачи данных от одного узла ко многим, обеспечивающая анонимность получателя; и, в-третьих, сохранение низкого пик-фактора сигнала. В **задачи** работы входит выбор адресных кодовых конструкций, которые на двух этапах расширения спектра сигнала должны решить вопросы идентификации отправителей и получателей информации в сети на физическом уровне. Требуется построить модель системы, которая обеспечит параллельную передачу данных от одного узла ко многим. Важным требованием в такой сети множественного доступа должна стать возможность использования модуляции с наименьшим пик-фактором сигнала. **Методы:** в данной работе предлагается двухэтапная широкополосная модуляция методом прямого расширения спектра, где каждый узел-отправитель сначала формирует эквивалентный код Голда как сумму последовательностей максимальной длины, адресованных узлам-получателям, а затем использует идентифицирующую его самого адресную последовательность из набора ортогональных сигналов. В работе предложены методы обработки расширяющих спектр последовательностей на основе двойственного базиса поля Галуа, позволяющие достаточно эффективно выделять информацию, предназначенную для каждого получателя.

Результаты: предложена модель системы параллельной передачи данных с множественным доступом на основе двухэтапного расширения спектра. Идентификация отправителей и получателей информации осуществляется механизмами формирования адресных сигнально-кодовых конструкций на физическом уровне. Возможен вариант реализации модели с анонимными получателями, когда любой из узлов-получателей не обладает информацией о данных, адресованных другим узлам. Также данная модель не противоречит использованию наиболее помехоустойчивого типа модуляции BPSK (или QPSK в режиме передачи одного разряда), который призван обеспечить предельно низкий пик-фактор сигнала. **Новизна.** Предложен принципиально новый метод адресации на физическом уровне для сети с параллельной передачей информации, который повышает эффективность использования частотного диапазона. **Теоретическая и практическая значимость.** Полученные в работе результаты, в перспективе, могут быть использованы при построении различных высоко помехоустойчивых сетей с множественным доступом, где важным требованием является, прежде всего, предельно низкий пик-фактор сигнала источников данных. К таким сетям можно отнести, в частности, сети, образованные роями БПЛА.

Ключевые слова: кодовое разделение, последовательность максимальной длины, последовательность Голда, поле Галуа, двойственный базис

Источник финансирования: статья подготовлена в рамках прикладных научных исследований СПбГУТ, регистрационный номер 1023031600087-9-2.2.4;2.2.5;2.2.6;1.2.1;2.2.3 в ЕГИСУ НИОКТР.

Ссылка для цитирования: Кукунин Д.С. Кодовое разделение на основе двойного расширения спектра сигнала // Труды учебных заведений связи. 2024. Т. 10. № 3. С. 45–58. DOI:10.31854/1813-324X-2024-10-3-45-58. EDN:KQSXL

Original research

<https://doi.org/10.31854/1813-324X-2024-10-3-16-23>

Code Division Based on Double Spread Spectrum Signal

 **Dmitriy S. Kukunin**, kukunin.ds@sut.ru

The Bonch-Bruевич Saint Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Annotation

Relevance: The work addresses the problems of broadband modulation in relation to multiple access problems. The advantages of code multiplexing in the process of expanding the signal spectrum are indicated, which, as shown in the work, is a promising method of parallel data transmission. **Purpose:** The purpose of this work is, firstly, to increase the efficiency of using address sequences to identify the sender and recipient of information; secondly, to organize a parallel data transmission process from one node to many, ensuring the anonymity of the recipient and, thirdly, maintaining a low peak signal factor. **Statement of the problem:** The objectives of the work include the selection of address code structures, which, at two stages of expanding the signal spectrum, should solve the issues of identifying senders and recipients of information in the network at the physical level. It is required to build a system model that will ensure parallel data transfer from one node to many. An important requirement in such a multiple access network should be the ability to use modulation with the lowest signal crest factor. **Methods:** This work proposes two-stage wideband modulation using the direct spread spectrum method, where each sending node first generates an equivalent Gold code as the sum of sequences of maximum length addressed to recipient nodes, and then uses an address sequence identifying itself from set of orthogonal signals. The paper proposes methods for processing spectrum-expanding sequences based on the dual basis of the Galois field, which make it possible to quite effectively isolate information intended for each recipient. **Results:** A model of a parallel data transmission system with multiple access based on two-stage spectrum expansion is proposed. Identification of senders and recipients of information is carried out by mechanisms for the formation of address signal-code structures at the physical level. It is possible to implement a model with anonymous recipients, when any of the recipient nodes does not have information about the data addressed to other nodes. Also, this model does not contradict the use of the most noise-resistant type of modulation BPSK (or QPSK in single-bit transmission mode), which is designed to provide an extremely low signal crest factor. **Novelty:** A fundamentally new method of addressing at the physical level for a network with parallel information transmission is proposed, which increases the efficiency of using the frequency range. **Theoretical and practical significance:** The results obtained in the work, in the future, can be used in the construction of various highly noise-resistant networks with multiple access, where an important requirement is, first of all, an extremely low crest factor of the data source signal. Such networks include, in particular, networks formed by swarms of UAVs.

Keywords: code division, maximum length sequence, Gold sequence, Galois field, dual basis

Funding: the article was prepared within the framework of applied scientific research of St. Petersburg State University, registration number 1023031600087-9-2.2.4;2.2.5;2.2.6;1.2.1;2.2.3 in the USISU of R&D.

For citation: Kukunin D.S. Code Division Based on Double Spread Spectrum Signal. *Proceedings of Telecommunication Universities*. 2024;10(3):45–58. (in Russ.) DOI:10.31854/1813-324X-2024-10-3-45-58. EDN:KQSXLX

Введение

Основной целью процедуры кодового уплотнения на практике является организация множественного доступа по принципу кодового разделения каналов (CDMA, аббр. от англ. Code Division Multiple Access) [1, 2], который призван обеспечить

обмен данными между абонентами сети, исключив недостатки временного (TDMA, аббр. от англ. Time Division Multiple Access) и частотного (FDMA, аббр. от англ. Frequency Division Multiple Access) множественного доступа.

Технология FDMA, наиболее востребованная на сегодняшний день в вариации ортогонального частотного разделения (OFDM, аббр. от англ. Orthogonal Frequency-Division Multiplexing) [3–6], предполагает использование в качестве абонентских ресурсов полосы частот, временной интервал при этом будет общим ресурсом для всех каналов. TDMA, в свою очередь, разделяет абонентов по времени так, что каждый из временных интервалов выделяется для передачи блока информации, адресованного определенному абоненту. Таким образом, в случае использования TDMA общим ресурсом является полоса частот, а время, как самый ценный ресурс, становится разделяемым.

Качественное преимущество CDMA заключается в том, что и частотный, и временной диапазоны становятся для системы передачи данных общими ресурсами.

Основным инструментом множественного доступа в технологии CDMA являются специальные адресные кодовые последовательности, которые обеспечивают решение двух основных задач [7]:

- увеличение базы сигнала путем расширения его частотного спектра методом прямой последовательности (DSSS, аббр. от англ. Direct Sequence Spread Spectrum) [8–12];

- кодовое уплотнение в спектре сигналов, используемых для информационного обмена между множеством абонентов.

Известно, что сигнал с большой базой, то есть широкополосный, обладает лучшей энергетической эффективностью по сравнению с узкополосным сигналом [13, 14]. Немаловажную роль играет также скрытность сигнала, передаваемого в широком спектре частот.

Кодовое разделение каналов CDMA в классическом варианте использует адресные кодовые последовательности, которые в силу своей формы не оказывают влияния друг на друга, или оно сведено к минимуму. Такие кодовые последовательности могут быть объединены в общий сложный сигнал на передаче и разделены соответствующим

образом на приеме. При этом каждая адресная последовательность однозначно идентифицирует отправителя информации, что требует в дальнейшем поддержки некоторого протокола идентификации получателя, которому данная последовательность была адресована. Это неизбежно приводит к усложнению архитектуры подобной системы организации множественного доступа вне зависимости, используется ли базовая станция или все абоненты сети работают автономно. Добавим к этому проблему использования в CDMA сложных многоуровневых сигналов, которые так или иначе будут иметь высокое значение пик-фактора.

Целью настоящей работы является, во-первых, повышение эффективности применения адресных последовательностей для идентификации отправителя и получателя информации; во-вторых, организация параллельного процесса передачи данных от одного узла ко многим, обеспечивающая анонимность получателя; и, в-третьих, сохранение низкого пик-фактора сигнала с учетом использования модуляции BPSK или QPSK для передачи одного разряда.

Организация множественного доступа с кодовым уплотнением

В идеале, в качестве адресных последовательностей для кодового уплотнения с последующим разделением следует использовать полностью ортогональные сигналы $A_i(t)$ и $A_j(t)$ периода T , для которых выполняется условие ортонормированности [15]:

$$\frac{1}{T} \int A_i(t)A_j(t) dt = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases} \quad (1)$$

Выполнение условия (1) позволяет реализовать простейшую систему с кодовым уплотнением (рисунок 1), где $A_i(t)$ и $A_j(t)$ действительно не оказывают влияния друг на друга и, следовательно, могут быть использованы в общем частотном и временном диапазонах [7].

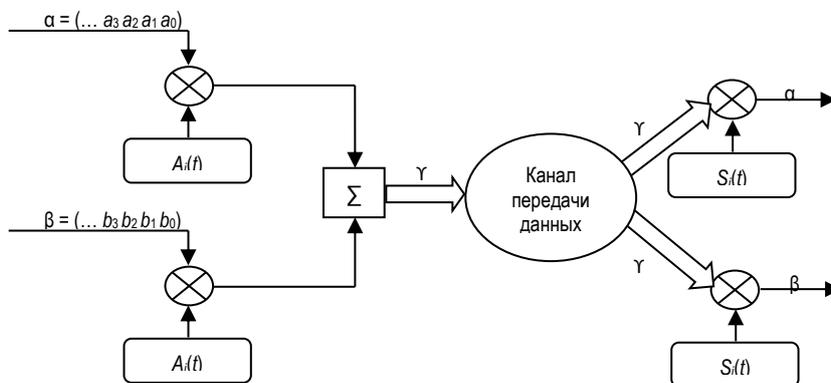


Рис. 1. Схема системы с кодовым уплотнением на основе адресных последовательностей $A_i(t)$ и $A_j(t)$

Fig. 1. The Scheme of Code Division System Based on Address Sequences $A_i(t)$ and $A_j(t)$

Система, построенная на основе схемы, содержит две адресные последовательности: $A_i(t)$ и $A_j(t)$, которые требуется привести к биполярному виду в том случае, если они были двоичными и состояли из символов «0» и «1». Это не будет противоречить дальнейшему применению фазовой модуляции (BPSK или QPSK в режиме передачи одного разряда), которая обеспечит наилучшую помехоустойчивость и низкий пик-фактор сигналов.

Для такого преобразования целесообразно использовать следующее правило [15]:

$$b_i = \begin{cases} +1, & d_i = 0; \\ -1, & d_i = 1; \end{cases} \quad i = 0 \dots (R - 1), \quad (2)$$

где d_i – двоичный символ исходной последовательности длины R ; b_i – соответствующий ему символ, который принимает значение «+1» или «-1». Таким образом, логический ноль кодируется символом «+1», а единица – символом «-1».

Правило (2) не является жестким. Возможен и обратный вариант преобразования, который в последствии должен учитываться на приемной стороне.

Расширение спектра информационных сигналов α и β на схеме (см. рисунок 1) реализуется путем последовательного умножения каждого их элемента на функции $A_i(t)$ и $A_j(t)$, соответственно, что фактически предполагает замену каждого информационного символа «0» на прямую, а символа «1» на инверсную адресную последовательность. Полученный в итоге широкополосный биполярный многоуровневый сигнал на приеме будет представлять собой линейную сумму соответствующих элементов $A_i(t)$ и $A_j(t)$.

Обработку суммарного сигнала на приеме следует рассматривать как независимое вычисление его нормированного скалярного произведения со всеми адресными последовательностями, в том числе с $A_i(t)$ и $A_j(t)$. Полученное в результате такой процедуры значение «+1» или «-1» однозначно определяет соответствующий информационный элемент «0» или «1» [15].

Наиболее известный на сегодняшний день класс ортогональных последовательностей Уолша [16], которые удовлетворяют условию (1) и вполне справляются с задачей кодового уплотнения (см.

рисунок 1). Однако, в силу своей природы, эти функции обладают рядом особенностей.

Во-первых, размер ансамбля функций Уолша определяется их периодом $n = 2^l$, где $l = 1, 2, 3, 4, \dots$, то есть можно сформировать наборы взаимно ортогональных последовательностей лишь в количестве 2, 4, 8, 16, ..., длина которых будет соответствовать их числу.

Также необходимо отметить далекие от идеальных автокорреляционные свойства последовательностей Уолша, которые ограничивают их применение в асинхронных системах передачи данных, делая фактически невозможным некогерентные формы приема и, вместе с тем, серьезно повышая требования к цикловой синхронизации [7].

В качестве альтернативы ортогональным функциям Уолша для метода DSSS предлагается использовать рассмотренные в работах [17–19] ортогональные структуры, построенные на основе рекуррентных последовательностей максимальной длины [20].

Общая идея формирования взаимно ортогональных адресных сигналов A_i и A_j (3), полностью удовлетворяющих условию (1) и соответственно пригодных для выполнения задач множественного доступа в CDMA, строится на уникальных свойствах M -последовательностей [7], где M_a, M_b, M_c, M_d – различные последовательности максимальной длины периода L из одного ансамбля, построенные на основе общего минимального многочлена $P(x)$ степени l над полем $GF(2^l)$ и преобразованные в биполярные сигналы по принципу (2).

Выражения (3) фактически предполагают усреднение результата сложения элементов любых двух различных M -последовательностей из ансамбля, представленных в биполярном виде, с элементами их несовпадающих инверсных копий, сдвинутых во времени. Кроме того, частью данного ансамбля также является вырожденная последовательность максимальной длины M_L , которая, в двоичном виде будет содержать L нулей [7].

Таким образом, каждый переданный источником q элемент E информационной последовательности, имеющий значение «0» или «1», будет преобразован в соответствии с правилом (4).

$$\begin{cases} A_i = \frac{M_a + \bar{M}_b}{2}; & i, j = 1, 2, \dots, \left(\frac{L+1}{2}\right), \quad a, b, c, d = 0, 1, 2, \dots, L, \\ A_j = \frac{M_c + \bar{M}_d}{2}; & i \neq j, \quad a \neq b \neq c \neq d, \quad L = 2^l - 1, \quad GF(2^l), \end{cases} \quad (3)$$

$$E = \begin{cases} A_q, & \text{«0»}; \\ \bar{A}_q, & \text{«1»}; \end{cases} \quad q = 1, 2, \dots, \left(\frac{L+1}{2}\right), \quad L = 2^l - 1, \quad GF(2^l). \quad (4)$$

Приведем пример набора ортогональных адресных комбинаций с периодом $L = 15$, построенных по принципу (4) на основе многочлена $P(x) = x^4 + x + 1$.

Для выполнения условий (3) были выбраны пары M -последовательностей в соответствии со своими начальными фазами [7], то есть M_i порождаются начальными элементами ϵ^i поля $GF(2^l)$, где $i = 0, 1, 2, \dots, (L - 1)$, при этом M_{15} является вырожденной (5). Не составляет труда убедиться в том, что все комбинации, представленные в (5), ортогональны,

а их нормированное на длину периода скалярное произведение подчиняется свойству (1). Таким образом, они вполне годятся для реализации схемы множественного доступа в CDMA (см. рисунок 1). Емкость данного набора адресных последовательностей составляет $(L + 1) / 2$, при этом сами они состоят из биполярных элементов с амплитудами $(-1, 0, +1)$, которые можно в последствии подвергнуть фазовой модуляции, как и предполагалось изначально.

$$\begin{aligned}
 A_1 &= \frac{M_0 + \bar{M}_1}{2} = (0 \ 0 \ +1 \ -1 \ 0 \ +1 \ 0 \ -1 \ +1 \ -1 \ +1 \ 0 \ 0 \ 0 \ -1), \\
 A_2 &= \frac{M_2 + \bar{M}_3}{2} = (+1 \ -1 \ 0 \ +1 \ 0 \ -1 \ +1 \ -1 \ +1 \ 0 \ 0 \ 0 \ -1 \ 0 \ 0), \\
 A_3 &= \frac{M_4 + \bar{M}_5}{2} = (0 \ +1 \ 0 \ -1 \ +1 \ -1 \ +1 \ 0 \ 0 \ 0 \ -1 \ 0 \ 0 \ +1 \ -1), \\
 A_4 &= \frac{M_6 + \bar{M}_7}{2} = (0 \ -1 \ +1 \ -1 \ +1 \ 0 \ 0 \ 0 \ -1 \ 0 \ 0 \ +1 \ -1 \ 0 \ +1), \\
 A_5 &= \frac{M_8 + \bar{M}_9}{2} = (+1 \ -1 \ +1 \ 0 \ 0 \ 0 \ -1 \ 0 \ 0 \ +1 \ -1 \ 0 \ +1 \ 0 \ -1), \\
 A_6 &= \frac{M_{10} + \bar{M}_{11}}{2} = (+1 \ 0 \ 0 \ 0 \ -1 \ 0 \ 0 \ +1 \ -1 \ 0 \ +1 \ 0 \ -1 \ +1 \ -1), \\
 A_7 &= \frac{M_{12} + \bar{M}_{13}}{2} = (0 \ 0 \ -1 \ 0 \ 0 \ +1 \ -1 \ 0 \ +1 \ 0 \ -1 \ +1 \ -1 \ +1 \ 0), \\
 A_8 &= \frac{M_{14} + \bar{M}_{15}}{2} = (-1 \ 0 \ 0 \ 0 \ -1 \ 0 \ 0 \ -1 \ -1 \ 0 \ -1 \ 0 \ -1 \ -1 \ -1).
 \end{aligned} \tag{5}$$

Если рассматривать процедуру такого кодового уплотнения в рамках задачи параллельной передачи данных из некоторой центральной точки множеству устройств, то набор адресных комбинаций увеличивается вплоть до полного периода используемых последовательностей. В частности, в работе [19] описана методика формирования самосинхронизирующегося широкополосного сигнала, который подвергается обработке на приеме двойственным базисом поля Галуа [7, 20] с целью определения начальной фазы заложенной в него синхронизирующей последовательности и, вместе с тем, декодируется подобно помехоустойчивому циклическому коду.

Так или иначе, рассмотренный подход к расширению спектра методом DSSS сохраняет принцип, согласно которому адресные комбинации определяют источник информации, как это было реализовано в классических системах с кодовым разделением каналов. При этом вопросы с адресацией получателя возлагаются на уровни выше. Предлагаемый механизм двойного расширения спектра позволил бы значительно упростить требования к верхним уровням системы передачи данных и фактически решил бы вопрос адресации на физическом уровне.

Таким образом, предварительное расширение спектра методом DSSS позволило бы установить однозначные связи между узлом-получателем и всеми узлами-отправителями информации, обеспечивая вместе с тем одновременную параллельную передачу данных между ними. Для решения данной задачи предлагается использовать эквивалентные коды Голда.

Коды Голда как рекуррентные последовательности

Классический код Голда [7, 20] представляет собой последовательность, формируемую двумя M -последовательностями одного периода $n = 2^k$, которые были построены на базе разных характеристических многочленов вида:

$$\begin{aligned}
 P(x) &= \sum_{i=0}^k p_i x^{k-i} = p_0 x^k + \\
 &+ p_1 x^{k-1} + \dots + p_{k-1} x + p_k, \quad p_i \in GF(2).
 \end{aligned} \tag{6}$$

Приведем пример построения кода Голда $\{\Gamma\} = (\gamma_0 \gamma_1 \gamma_2 \gamma_3 \dots \gamma_{14})$ на основе суммы по mod 2 последовательностей максимальной длины $\{A\} = (a_0 a_1 a_2 a_3 \dots a_{14})$ и $\{B\} = (b_0 b_1 b_2 b_3 \dots b_{14})$ с перио-

дом 15. В качестве порождающих полиномов вида (5) выберем примитивные многочлены, на основе которых не составит труда построить генератор такого кода Голда (рисунок 2), $P_1(x) = x^4 + x + 1$ и $P_2(x) = x^4 + x^3 + 1$.

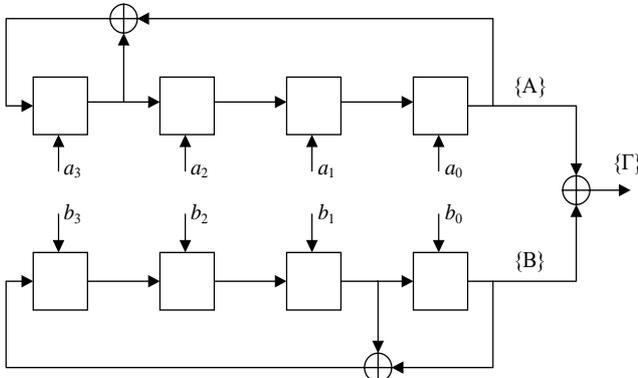


Рис. 2. Генератор последовательности Голда на основе $P_1(x)$ и $P_2(x)$

Fig. 2. Gold Sequence Generator Based on $P_1(x)$ and $P_2(x)$

Так, например, установив произвольные ненулевые начальные значения векторов $(a_0 a_1 a_2 a_3) = (1101)$ и $(b_0 b_1 b_2 b_3) = (0010)$ в схеме (см. рисунок 2), реализуем правило, позволяющее получить на ее выходе последовательность $\{\Gamma\}$:

$$\begin{aligned} \{A\} &= (110101111000100) \\ \oplus \\ \{B\} &= (001000111101011) \cdot \\ \hline \{\Gamma\} &= (111101000101111). \end{aligned} \quad (7)$$

Отметим, что, согласно своей природе, последовательности $\{A\}$ и $\{B\}$, используемые в сумме (7), удовлетворяют рекуррентному уравнению с коэффициентами p_i своих многочленов (6):

$$S_i = p_1 S_{i-1} + p_2 S_{i-2} + \dots + p_{k-1} S_{i-k+1} + p_k S_{i-k}, \quad (8)$$

$p_i \in GF(2),$

где $[i \pmod{(2^k-1)}] \geq k$.

Параметр k в уравнении (8) определяется старшей степенью полиномов $P_1(x)$ и $P_2(x)$ и в данном примере равен 4. Он же определяет показатель расширенных полей $GF(2^k)$, построенных на основе данных многочленов. Элементы этих полей $GF(2^4)$, в свою очередь, будут соответствовать фазам рекуррентных последовательностей $\{A\}$ и $\{B\}$.

Что касается последовательности $\{\Gamma\}$, полученной в результате сложения по правилу (7), то она также будет удовлетворять рекуррентному уравнению, аналогичному (8), но с коэффициентами p_i некоторого нового многочлена $P(x)$:

$$S_i = p_1 S_{i-1} + p_2 S_{i-2} + \dots + p_{m-1} S_{i-m+1} + p_m S_{i-m}, \quad (9)$$

$p_i \in GF(2),$

где $[i \pmod{(2^k-1)}] \geq m$.

Параметр m в уравнении (9) определяется старшей степенью многочлена $P(x)$, содержащего произведение минимальных полиномов, на основе которых были построены M -последовательности, входящие в состав кода Голда:

$$P(x) = P_1(x)P_2(x) = x^8 + x^7 + x^5 + x^4 + x^3 + x + 1. \quad (10)$$

Последовательности Голда, построенные на основе рекуррентного соотношения (9) и обрабатываемые соответствующим образом, принято называть эквивалентными [20]. Более того, характеристический многочлен (10), определяющий (9), в общем виде представляет собой произведение V минимальных многочленов $f_i(x)$ и позволяет построить рекуррентную последовательность $\{S\}$ общего вида [7]:

$$S_j = \sum_{i=1}^V T(C_i \eta_i^j) = T(C_1 \eta_1^j) + T(C_2 \eta_2^j) + \dots + T(C_V \eta_V^j), \quad (11)$$

где η_i – корни соответствующих многочленов $f_i(x)$; $T(C_i \eta_i^j)$ – функция-след от элемента поля Галуа $\alpha^i = C_i \eta_i^j$, которая определяется выражением [7, 20]:

$$T(\alpha^i) = \sum_{j=0}^{k-1} (\alpha^i)^{2^j} = \alpha^i + (\alpha^i)^2 + (\alpha^i)^{2^2} + \dots + (\alpha^i)^{2^{k-1}}. \quad (12)$$

Коэффициенты C_i в выражении (11) также являются элементами поля Галуа $GF(2^k)$, построенного на основании своего минимального многочлена $f_i(x)$ степени k , и могут быть вычислены по начальному участку $(S_0 S_1 S_2 \dots S_{m-1})$ рекуррентной последовательности $\{S\}$ следующим образом [7]:

$$C_i = \eta_i^{-\delta} \sum_{j=1}^m \omega_{ij} S_{\delta+j-1}, \quad i = 1 \dots V, \quad (13)$$

где δ – расстояние текущего m -элементного участка относительно начала последовательности $\{S\}$, сформированной на основе выражения (11) через функцию (12).

Коэффициенты ω_{ij} в равенстве (13) также являются элементами поля Галуа $GF(2^k)$, построенного на основании соответствующего многочлена $f_i(x)$, их принято называть базисными или двойственным базисом [7, 20].

Для вычисления базисных коэффициентов может быть использовано выражение [7]:

$$\omega_{i\rho} = \frac{\sum_{l=0}^{m-\rho} p_{m-\rho-l}(\eta_i)^l}{P'(\eta_i)}, \quad \rho = 1, 2, \dots, m, \quad (14)$$

где m – старшая степень многочлена $P(x)$; $P'(\eta_i)$ – значение его производной в точке, которая соот-

ветствует примитивному элементу η_i поля $GF(2^k)$, построенного на основе соответствующего многочлена $f_i(x)$.

Вернувшись к примеру с последовательностью Голда, состоящей из двух M -последовательностей (7), обозначим примитивные элементы ε и μ для двух полей $GF(2^4)$, построенных, соответственно, на основе многочленов $P_1(x)$ и $P_2(x)$. В данном случае формула (14) без труда позволит вычислить базисные коэффициенты $\omega_{1\rho} = \lambda_\rho$ и $\omega_{1\rho} = \nu_\rho$ на основе следующих выражений [7]:

$$\lambda_\rho = \frac{\sum_{l=0}^{m-\rho} p_{m-\rho-l}(\varepsilon)^l}{P'(\varepsilon)}, \quad \nu_\rho = \frac{\sum_{l=0}^{m-\rho} p_{m-\rho-l}(\mu)^l}{P'(\mu)}, \quad (15)$$

$$\rho = 1, 2, \dots, m.$$

Так, применяя (15), определим коэффициенты двойственного базиса, которые в данном случае будут постоянными для характеристического многочлена (8):

$$\{\lambda\} = (\varepsilon^5 \varepsilon^8 \varepsilon^7 \varepsilon^9 \varepsilon^4 \varepsilon^{11} \varepsilon^{10} \varepsilon^6),$$

$$\{\nu\} = (\mu^2 \mu^{13} \mu^{12} \mu^4 \mu^{14} \mu^1 \mu^3). \quad (16)$$

Теперь, обладая наборами элементов (16) из двух полей $GF(2^4)$ и учитывая свойство (11), можем вычислить коэффициенты C и D , которые, используя выражение $\gamma_j = T(C\varepsilon^j) + T(D\mu^j)$, позволят определить произвольный элемент последовательности Голда $\{\Gamma\} = (\gamma_0 \gamma_1 \gamma_2 \gamma_3 \dots \gamma_{14})$:

$$C = \varepsilon^{-\delta} \sum_{i=1}^m \lambda_i \gamma_{\delta+i-1}, \quad D = \mu^{-\delta} \sum_{i=1}^m \nu_i \gamma_{\delta+i-1}, \quad (17)$$

где δ – расстояние m -элементного участка относительно начала $\{\Gamma\}$.

Отметим, что элементы C и D принято считать начальными фазами M -последовательностей $\{A\}$ и $\{B\}$, то есть теми элементами своих полей $GF(2^4)$, которые порождают эти последовательности [7, 20]. Задача определения начальных фаз рекуррентных последовательностей $\{A\}$ и $\{B\}$ сводится к обработке m -элементных участков $\{\Gamma\}$ по принципу (17).

Произведем такую обработку нескольких последовательных участков $\{\Gamma\} = (\gamma_0 \gamma_1 \gamma_2 \gamma_3 \dots \gamma_{14})$ длины $m = 8$ и определим значения начальных фаз M -последовательностей, составляющих данный код Голда [7].

Нулевой участок $(\gamma_0 \gamma_1 \gamma_2 \gamma_3 \gamma_4 \gamma_5 \gamma_6 \gamma_7) = (11110100)$:

$$C = \varepsilon^5 + \varepsilon^8 + \varepsilon^7 + \varepsilon^9 + \varepsilon^{11} = \varepsilon^6,$$

$$D = \mu^2 + \mu^{13} + \mu^{12} + \mu^4 + \mu = \mu^{10}.$$

Первый участок $(\gamma_1 \gamma_2 \gamma_3 \gamma_4 \gamma_5 \gamma_6 \gamma_7 \gamma_8) = (11101000)$:

$$C = \varepsilon^{-1}(\varepsilon^5 + \varepsilon^8 + \varepsilon^7 + \varepsilon^4) = \varepsilon^6,$$

$$D = \mu^{-1}(\mu^2 + \mu^{13} + \mu^{12} + \mu^{14}) = \mu^{10}.$$

Второй участок $(\gamma_2 \gamma_3 \gamma_4 \gamma_5 \gamma_6 \gamma_7 \gamma_8 \gamma_9) = (11010001)$:

$$C = \varepsilon^{-2}(\varepsilon^5 + \varepsilon^8 + \varepsilon^9 + \varepsilon^6) = \varepsilon^6,$$

$$D = \mu^{-2}(\mu^2 + \mu^{13} + \mu^4 + \mu^3) = \mu^{10}.$$

Третий участок $(\gamma_3 \gamma_4 \gamma_5 \gamma_6 \gamma_7 \gamma_8 \gamma_9 \gamma_{10}) = (10100010)$:

$$C = \varepsilon^{-3}(\varepsilon^5 + \varepsilon^7 + \varepsilon^{10}) = \varepsilon^6,$$

$$D = \mu^{-3}(\mu^2 + \mu^{12} + 1) = \mu^{10}.$$

Четвертый участок $(\gamma_4 \gamma_5 \gamma_6 \gamma_7 \gamma_8 \gamma_9 \gamma_{10} \gamma_{11}) = (01000101)$:

$$C = \varepsilon^{-4}(\varepsilon^8 + \varepsilon^{11} + \varepsilon^6) = \varepsilon^6,$$

$$D = \mu^{-4}(\mu^{13} + \mu + \mu^3) = \mu^{10}.$$

Пятый участок $(\gamma_5 \gamma_6 \gamma_7 \gamma_8 \gamma_9 \gamma_{10} \gamma_{11} \gamma_{12}) = (10001011)$:

$$C = \varepsilon^{-5}(\varepsilon^5 + \varepsilon^4 + \varepsilon^{10} + \varepsilon^6) = \varepsilon^6,$$

$$D = \mu^{-5}(\mu^2 + \mu^{14} + 1 + \mu^3) = \mu^{10}.$$

Полученные результаты говорят о том, что для формирования последовательности Голда были использованы M -последовательности с начальными фазами ε^6 и μ^{10} .

Кодовое уплотнение на основе кодов Голда

Рассмотрев пример с классическим кодом Голда, который представляет собой сумму лишь двух M -последовательностей, имеет смысл перейти к более интересному примеру, когда выражение (11) включает в себя несколько слагаемых.

Действительно, ничто не мешает построить эквивалентный код Голда, сложив по mod 2 более двух последовательностей максимальной длины, принадлежащих разным ансамблям. Ограничением при этом будет только число характеристических полиномов V степени k из разложения двучлена $x^n - 1$, где $n = 2^k - 1$.

Согласно принципу разложения $x^n - 1$ на составляющие, число таких многочленов V степени k будет определяться следующим выражением:

$$V = \frac{\varphi(2^k - 1)}{k}, \quad (18)$$

где $\varphi(2^k - 1)$ – функция Эйлера от $n = 2^k - 1$.

Рассмотрим пример для $k = 5$, когда, согласно формуле (18), многочленов, пригодных для построения поля $GF(2^5)$, будет:

$$V = \varphi(2^k - 1)/k = \varphi(31)/5 = 30/5 = 6,$$

а их M -последовательности будут иметь период 31 (таблица 1). Представленные последовательности максимальной длины имеют каноническую форму [20], при этом их начальной фазой в любом поле $GF(2^5)$ является элемент $\eta^0 = 1$. Когда речь заходит о передаче информации при помощи M -последовательностей, необходимо обеспечить смещение их фазы на определенное количество разрядов.

ТАБЛИЦА 1. Минимальные многочлены для $GF(2^5)$ и их M -последовательностиTABLE 1. Minimum Polynomials for $GF(2^5)$ and Their M -Sequences

Минимальный полином	M -последовательность в канонической форме
$P_1(x) = x^5 + x^2 + 1$	$\{S\}_1 = (1001011001111100011011101010000)$
$P_2(x) = x^5 + x^4 + x^3 + x^2 + 1$	$\{S\}_2 = (1111101110001010110100001100100)$
$P_3(x) = x^5 + x^3 + 1$	$\{S\}_3 = (1000010101110110001111100110100)$
$P_4(x) = x^5 + x^3 + x^2 + x + 1$	$\{S\}_4 = (1001001100001011010100011101111)$
$P_5(x) = x^5 + x^4 + x^3 + x + 1$	$\{S\}_5 = (1110110011100001101010010001011)$
$P_6(x) = x^5 + x^4 + x^2 + x + 1$	$\{S\}_6 = (1110100010010101100001110011011)$

Таким образом, текущая фаза M -последовательности $\{S\}_i$, где $i = 1, 2, \dots, 6$, однозначно определяет «где содержится информация?» одним из следующих способов:

1) в первых $k = 5$ разрядах M -последовательности $\{S_0S_1S_2S_3S_4\}_i$;

2) в элементе η^j поля $GF(2^5)$, который порождает данную M -последовательность $\{S\}_i$.

При этом второй способ имеет две возможные вариации – информация содержится в разрядах вектора, или в показателе степени j вектора, представляющего элемент η^j поля $GF(2^k)$.

Ограничения, которые накладываются на все вышеперечисленные способы представления информации, очевидны. Так, в случае варианта 1 участок $\{S_0S_1S_2S_3S_4\}_i$ для всех $i = 1, 2, \dots, 6$ не должен быть полностью нулевым, иначе M -последовательность, удовлетворяющая условию (7), также станет нулевой или вырожденной [7]. Это, в свою очередь, приведет к тому, что ее присутствие в общем коде Голда будет равносильно отсутствию.

То же условие невозможности использования нулевого значения информационного вектора характерно и для варианта, когда информация содержится в разрядах вектора. Ведь нулевой элемент поля Галуа также приведет к формированию вырожденной рекуррентной последовательности максимальной длины.

Таким образом, возможные значения информационных векторов в этих двух случаях должны лежать в диапазоне от 1 до $(2^k - 1) = 31$, то есть (00001)–(11111).

Вариант, когда информация содержится в показателе степени j вектора, напротив, допускает нулевое значение информационного вектора, но вынуждает игнорировать значение $(2^k - 1) = 31$. Это

связано с тем, что каждое поле $GF(2^5)$ является циклически замкнутой группой, в которой выполняется равенство $\eta^{31} = \eta^0 = 1$. Поэтому данный вариант позволяет задать информацию на диапазоне от 0 до $(2^k - 2) = 30$, то есть (00000)–(11110).

Используя этот подход, необходимо учесть, что появление нулевого значения в результате обработки последовательности Голда на приеме следует расценивать как отсутствие информации в канале, так как не существует степени для η , которая бы привела к появлению нулевого вектора поля.

Рассмотрим пример с передачей информации по всем шести каналам, остановившись на варианте представления информации в разрядах вектора (таблица 2).

ТАБЛИЦА 2. Организация передачи данных по шести каналам

TABLE 2. Organization of Data Transmission Over Six Channels

Номер канала i	Информация (элемент поля η^j)	Адресная последовательность $\{S\}_i$
1	$(00011) = \eta^{21}$	(1101010000100101100111110001101)
2	$(11000) = \eta^{20}$	(0000110010011111011100010101101)
3	$(10010) = \eta^5$	(1010111011000111110011010010000)
4	$(00110) = \eta^{14}$	(1101010001110111110010011000010)
5	$(11110) = \eta^8$	(1110000110101001000101111101100)
6	$(11111) = \eta^{10}$	(0101011000011100110111110100010)

Информационные векторы (см. таблицу 2) сопоставляются элементам η^j своих полей $GF(2^5)$, а M -последовательности $\{S\}_i$, выступающие в качестве адресных, могут быть получены путем сдвига на j разрядов соответствующих канонических $\{S\}_i$ из таблицы 1.

Последовательность Голда, сформированная по принципу (7) для шести M -последовательностей, будет иметь вид:

$$\{G\} = (0001010110111111001000100111100). \quad (19)$$

Целью обработки последовательности (19) на приеме является определение всех элементов η^j , которые являются начальными фазами входящих в ее состав адресных M -последовательностей.

Первым шагом на пути к этому должно стать построение общего характеристического многочлена, который является произведением (20) всех шести минимальных полиномов [7]. Далее определяется производная для (20), которая будет иметь вид (21) из [7].

$$P(x) = P_1(x)P_2(x)P_3(x)P_4(x)P_5(x)P_6(x) = x^{30} + x^{29} + x^{28} + x^{27} + x^{26} + x^{25} + x^{24} + x^{23} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1. \quad (20)$$

$$P'(x) = x^{28} + x^{26} + x^{24} + x^{22} + x^{20} + x^{18} + x^{16} + x^{14} + x^{12} + x^{10} + x^8 + x^6 + x^4 + x^2 + 1. \quad (21)$$

Полученные многочлены (20) и (21) при помощи выражения (14) позволяют определить для всех шести каналов, соответствующих своим полям, полные наборы из $m = 6k = 30$ базисных коэффициентов (таблица 3).

ТАБЛИЦА 3. Базисные коэффициенты для последовательности Голда

TABLE 3. Basic Coefficients for the Gold Sequence

Базисные коэффициенты	Каналы					
	1	2	3	4	5	6
	$P_1(x)$	$P_2(x)$	$P_3(x)$	$P_4(x)$	$P_5(x)$	$P_6(x)$
λ_1	η^{18}	η^{20}	η^{14}	η^{12}	η^{13}	η^{19}
λ_2	η^4	η^8	η^{27}	η^{23}	η^{25}	η^6
λ_3	η^{27}	η^{24}	η^3	η^6	η^{21}	η^9
λ_4	η^7	η^{15}	η^{22}	η^{14}	η^{18}	η^{11}
λ_5	η^{29}	η^4	η^{30}	η^{24}	η^3	η^{25}
λ_6	η^{22}	η^{16}	η^5	η^{11}	η^{10}	η^{17}
λ_7	η^{16}	η^{23}	η^{10}	η^3	η^{30}	η^{27}
λ_8	η^{13}	η^{29}	η^{12}	η^{27}	η^4	η^{21}
λ_9	η^8	η^{25}	η^{16}	η^{30}	η^{17}	η^7
λ_{10}	η^{26}	η^7	η^{28}	η^{16}	η^5	η^{18}
λ_{11}	η^9	η^2	η^{13}	η^{20}	η^{29}	η^{24}
λ_{12}	η^{12}	1	η^9	η^{21}	η^{19}	η^2
λ_{13}	η^2	η^5	η^{18}	η^{15}	η^{20}	1
λ_{14}	1	η^{14}	η^{19}	η^5	η^{28}	η^{22}
λ_{15}	η^{10}	η^{11}	η^8	η^7	η^{23}	η^{26}
λ_{16}	η^{25}	η^{26}	η^{23}	η^{22}	η^7	η^{10}
λ_{17}	η^{14}	η^{28}	η^2	η^{19}	η^{11}	η^5
λ_{18}	η^{15}	η^{18}	1	η^{28}	η^2	η^{13}
λ_{19}	η^{24}	η^{12}	η^{21}	η^2	1	η^{14}
λ_{20}	η^{20}	η^{13}	η^{24}	1	η^9	η^4
λ_{21}	η^5	η^{17}	η^7	η^{26}	η^{15}	η^{28}
λ_{22}	η^{17}	η^3	η^{25}	η^8	η^{26}	η^{16}
λ_{23}	η^{21}	η^6	η^{20}	η^4	η^{12}	η^{29}
λ_{24}	η^{23}	η^{30}	η^{17}	η^{10}	η^6	η^3
λ_{25}	η^{28}	η^{22}	η^{11}	η^{17}	η^{16}	η^{23}
λ_{26}	η^3	η^9	η^4	η^{29}	η^8	η^{30}
λ_{27}	η^{11}	η^{19}	η^{26}	η^{18}	η^{22}	η^{15}
λ_{28}	η^{30}	η^{27}	η^6	η^9	η^{24}	η^{12}
λ_{29}	η^6	η^{10}	η^{29}	η^{25}	η^{27}	η^8
λ_{30}	η^{19}	η^{21}	η^{15}	η^{13}	η^{14}	η^{20}

Теперь, используя формулу (13), нетрудно вычислить элементы поля, соответствующие текущим фазам M -последовательностей, составляющих последовательность (19). Произведем разложение начального m -элементного участка (19) на базисные коэффициенты, что, в данном случае, равнозначно вычислению суммы следующих базисных

коэффициентов из таблицы 3: $\lambda_4, \lambda_6, \lambda_8, \lambda_9, \lambda_{11}, \lambda_{12}, \lambda_{13}, \lambda_{14}, \lambda_{15}, \lambda_{16}, \lambda_{19}, \lambda_{23}, \lambda_{26}, \lambda_{27}, \lambda_{28}, \lambda_{29}$.

Таким образом, выделим информацию в каждом из шести каналов:

Канал 1: $\eta^7 + \eta^{22} + \eta^{13} + \eta^8 + \eta^9 + \eta^{12} + \eta^2 + 1 + \eta^{10} + \eta^{25} + \eta^{24} + \eta^{21} + \eta^3 + \eta^{11} + \eta^{30} + \eta^6 = \eta^{21}$,
 $\eta \in GF(2^5), P_1(x) = x^5 + x^2 + 1$;

Канал 2: $\eta^{15} + \eta^{16} + \eta^{29} + \eta^{25} + \eta^2 + 1 + \eta^5 + \eta^{14} + \eta^{15} + \eta^{16} + \eta^{29} + \eta^{25} + \eta^2 + 1 + \eta^5 + \eta^{14} + \eta^{11} + \eta^{26} + \eta^{12} + \eta^6 + \eta^9 + \eta^{19} + \eta^{27} + \eta^{10} = \eta^{20}$,
 $\eta \in GF(2^5), P_2(x) = x^5 + x^4 + x^3 + x^2 + 1$;

Канал 3: $\eta^{22} + \eta^5 + \eta^{12} + \eta^{16} + \eta^{13} + \eta^9 + \eta^{18} + \eta^{19} + \eta^8 + \eta^{23} + \eta^{21} + \eta^{20} + \eta^4 + \eta^{26} + \eta^6 + \eta^{29} = \eta^5$,
 $\eta \in GF(2^5), P_3(x) = x^5 + x^3 + 1$;

Канал 4: $\eta^{14} + \eta^{11} + \eta^{27} + \eta^{30} + \eta^{20} + \eta^{21} + \eta^{15} + \eta^5 + \eta^7 + \eta^{22} + \eta^2 + \eta^4 + \eta^{29} + \eta^{18} + \eta^9 + \eta^{25} = \eta^{14}$,
 $\eta \in GF(2^5), P_4(x) = x^5 + x^3 + x^2 + x + 1$;

Канал 5: $\eta^{18} + \eta^{10} + \eta^4 + \eta^{17} + \eta^{29} + \eta^{19} + \eta^{20} + \eta^{28} + \eta^{23} + \eta^7 + 1 + \eta^{12} + \eta^8 + \eta^{22} + \eta^{24} + \eta^{27} = \eta^8$,
 $\eta \in GF(2^5), P_5(x) = x^5 + x^4 + x^3 + x + 1$;

Канал 6: $\eta^{11} + \eta^{17} + \eta^{21} + \eta^7 + \eta^{24} + \eta^2 + 1 + \eta^{22} + \eta^{26} + \eta^{10} + \eta^{14} + \eta^{29} + \eta^{30} + \eta^{15} + \eta^{12} + \eta^8 = \eta^{10}$,
 $\eta \in GF(2^5), P_6(x) = x^5 + x^4 + x^2 + x + 1$.

Обработка последовательности (19) базисными коэффициентами, как показано в примере, позволила однозначно определить информационные векторы, соответствующие начальным фазам (см. таблицу 2). Таким образом, одна двоичная последовательность Голда (19) обеспечила одновременную передачу пяти информационных разрядов по каждому из шести независимых каналов.

Приведем второй пример, где в один момент времени будет задействована только половина всех каналов. То есть три канала являются активными, а другие три не передают информации. В таком случае общая последовательность Голда строится на основе суммы по mod 2 трех M -последовательностей (см. таблицу 1) с учетом их начальных фаз, которые будут определять саму информацию. Отсутствие информации в неиспользуемых каналах обозначим векторами $(00000) = \text{NULL}$ (таблица 4, где i – номер канала, Q – элемент поля η^i , R – адресная последовательность $\{S\}_i$).

ТАБЛИЦА 4. Организация передачи данных по трем каналам
TABLE 4. Organization of Data Transmission Over Three Channels

i	Q	R
1	$(00011) = \eta^{15}$	$(0011011101010000100101100111110)$
2	$(11000) = \eta^7$	$(1100010101101000011001001111101)$
3	$(10010) = \eta^{24}$	$(0110100100001010111011000111110)$
4	$(00000) = \text{NULL}$	-
5	$(00000) = \text{NULL}$	-
6	$(00000) = \text{NULL}$	-

Три адресные комбинации, соответствующие первым трем активным каналам, образуют последовательность Голда:

$$\{G\} = (1001101100110010000111101111101). \quad (22)$$

Как и в предыдущем примере, целью здесь является определение всех элементов η^i , которые являются начальными фазами входящих в состав (22) адресных M -последовательностей или определение факта их отсутствия.

Используя уже вычисленные ранее базисные коэффициенты (см. таблицу 3), разложим начальный m -элементный участок (22). Для этого достаточно определить сумму следующего набора базисных коэффициентов: $\lambda_1, \lambda_4, \lambda_5, \lambda_7, \lambda_8, \lambda_{11}, \lambda_{12}, \lambda_{15}, \lambda_{20}, \lambda_{21}, \lambda_{22}, \lambda_{23}, \lambda_{25}, \lambda_{26}, \lambda_{27}, \lambda_{28}, \lambda_{29}$.

Определим информацию во всех каналах:

Канал 1: $\eta^{18} + \eta^7 + \eta^{29} + \eta^{16} + \eta^{13} + \eta^9 + \eta^{12} + \eta^{10} + \eta^{20} + \eta^5 + \eta^{17} + \eta^{21} + \eta^{28} + \eta^3 + \eta^{11} + \eta^{30} + \eta^6 = \eta^{15}$,
 $\eta \in \text{GF}(2^5)$, $P_1(x) = x^5 + x^2 + 1$;

Канал 2: $\eta^{20} + \eta^{15} + \eta^4 + \eta^{23} + \eta^{29} + \eta^2 + 1 + \eta^{11} + \eta^{13} + \eta^{17} + \eta^3 + \eta^6 + \eta^{22} + \eta^9 + \eta^{19} + \eta^{27} + \eta^{10} = \eta^7$,
 $\eta \in \text{GF}(2^5)$, $P_2(x) = x^5 + x^4 + x^3 + x^2 + 1$;

Канал 3: $\eta^{14} + \eta^{22} + \eta^{30} + \eta^{10} + \eta^{12} + \eta^{13} + \eta^9 + \eta^8 + \eta^{24} + \eta^7 + \eta^{25} + \eta^{20} + \eta^{11} + \eta^4 + \eta^{26} + \eta^6 + \eta^{29} = \eta^{24}$,
 $\eta \in \text{GF}(2^5)$, $P_3(x) = x^5 + x^3 + 1$;

Канал 4: $\eta^{12} + \eta^{14} + \eta^{24} + \eta^3 + \eta^{27} + \eta^{20} + \eta^{21} + \eta^7 + 1 + \eta^{26} + \eta^8 + \eta^4 + \eta^{17} + \eta^{29} + \eta^{18} + \eta^9 + \eta^{25} = \text{NULL}$,
 $\eta \in \text{GF}(2^5)$, $P_4(x) = x^5 + x^3 + x^2 + x + 1$;

Канал 5: $\eta^{13} + \eta^{18} + \eta^3 + \eta^{30} + \eta^4 + \eta^{29} + \eta^{19} + \eta^{23} + \eta^9 + \eta^{15} + \eta^{26} + \eta^{12} + \eta^{16} + \eta^8 + \eta^{22} + \eta^{24} + \eta^{27} = \text{NULL}$,
 $\eta \in \text{GF}(2^5)$, $P_5(x) = x^5 + x^4 + x^3 + x + 1$;

Канал 6: $\eta^{19} + \eta^{11} + \eta^{25} + \eta^{27} + \eta^{21} + \eta^{24} + \eta^2 + \eta^{26} + \eta^4 + \eta^{28} + \eta^{16} + \eta^{29} + \eta^{23} + \eta^{30} + \eta^{15} + \eta^{12} + \eta^8 = \text{NULL}$,
 $\eta \in \text{GF}(2^5)$, $P_6(x) = x^5 + x^4 + x^2 + x + 1$.

Как видно из обработки m -элементного участка, информация присутствует в первых трех каналах, а в остальных трех регистрируется ее отсутствие. При этом вычисленные значения начальных фаз для первых трех каналов являются абсолютно верными и совпадают со значениями из таблицы 4.

Множественный доступ на основе двухэтапного расширения спектра

Пусть имеется некоторое число узлов N , которые являются равнозначными участниками обмена данными в сети связи. Каждый из них в любой момент времени может осуществить одновременную передачу k индивидуальных бит информации остальным узлам. При этом широкополосный сигнал, передаваемый в открытом канале связи, не должен выдавать информацию о связи отправителем с получателем.

Учитывая рассмотренные выше методы кодового уплотнения, подобная схема может быть реализована в два этапа, которые призваны обеспечить первичное и вторичное расширение спектра исходного сигнала методом DSSS (рисунок 3).

На первом этапе k бит информации, предназначенные для каждого узла, расширяются до $n = 2^k - 1$ разрядов. При этом для каждого узла из множества N используется M -последовательность, построенная на основании своего минимального многочлена (таблица 5).

ТАБЛИЦА 5. Матрица соответствия между отправителями и получателями

TABLE 5. Correspondence Matrix between Senders and Recipients

Номера узлов	Отправители (адресные последовательности)							
	1	2	3	4	5	...	N	
Получатели	1		$P_1(x)$	$P_2(x)$	$P_3(x)$	$P_4(x)$...	$P_N(x)$
	2	$P_N(x)$		$P_1(x)$	$P_2(x)$	$P_3(x)$...	$P_{N-1}(x)$
	3	$P_{N-1}(x)$	$P_N(x)$		$P_1(x)$	$P_2(x)$...	$P_{N-2}(x)$
	4	$P_{N-2}(x)$	$P_{N-1}(x)$	$P_N(x)$		$P_1(x)$...	$P_{N-3}(x)$
	5	$P_{N-3}(x)$	$P_{N-2}(x)$	$P_{N-1}(x)$	$P_N(x)$...	$P_{N-4}(x)$

	N	$P_1(x)$	$P_2(x)$	$P_3(x)$	$P_4(x)$	$P_5(x)$...	

Затем производится формирование эквивалентного кода Голда путем суммирования по mod 2 всех построенных ранее M -последовательностей.

На втором этапе каждый из n разрядов эквивалентного кода Голда умножается на адресную последовательность длины $L = 2^l - 1$ в соответствии с принципом (4). Полученные в результате этого преобразования прямые и инверсные адресные комбинации модулируются QPSK и передаются в общий канал связи, где в силу своей ортогональности не будут оказывать влияния на адресные комбинации других узлов.

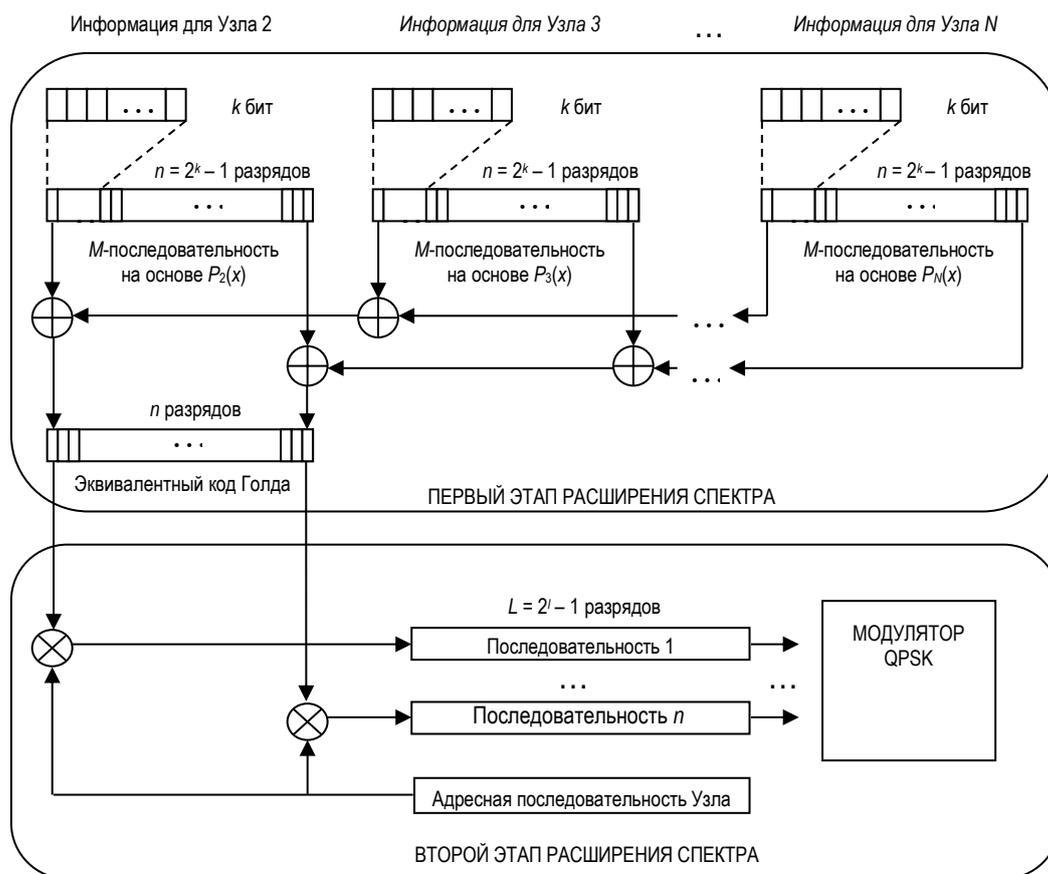


Рис. 3. Обмен данными Узла 1 с остальными узлами

Fig. 3. Node 1 Data Exchange with Other Nodes

На приеме каждый узел выделяет адресные последовательности, полученные от всех узлов. После этого, используя матрицу соответствия (см. таблицу 5), узел-получатель определяет переданные индивидуально для него M -последовательности, входящие в состав принятого им кода Голда. Начальные фазы этих M -последовательностей (первые k элементов или порождающий элемент поля Галуа) будут соответствовать информационным битам, переданным соответствующими узлами-отправителями.

Анонимность внутри сети, когда отдельно взятый узел не знает, какая информация была адресована остальным узлам, реализуется путем исключения из его матрицы соответствия (см. таблицу 5) лишних строк и столбцов. Так, узлу, производящему передачу данных, необходим только столбец с его номером, а узлу, принимающему данные, только его строка.

Число строк и столбцов матрицы соответствия (см. таблицу 5) определяется количеством узлов сети N , между которыми осуществляется параллельная передача данных. Данная характеристика задает требования к длине последовательностей, применяемых на первом и втором этапах расширения спектра сигнала:

$$\begin{cases} (N - 1) \leq \left\lfloor \frac{\Phi(2^k - 1)}{k} \right\rfloor \\ N \leq 2^{l-1} \end{cases} \quad (23)$$

Верхнее условие (23) показывает, что число связей между каждым из N узлов сети со всеми остальными узлами, определяемое как $(N - 1)$, не должно превышать количества используемых системой минимальных многочленов на первом этапе расширения спектра сигнала. Зависимость максимально допустимого числа N узлов сети от параметра k приведена ниже (таблица 6).

ТАБЛИЦА 6. Максимально допустимое число узлов сети

TABLE 6. Maximum Allowed Number of Network Nodes

k	3	4	5	6	7	8	9	10	11	12
N	3	3	7	7	19	17	49	61	177	145

Второе условие целиком и полностью применимо к методике построения ортогональных последовательностей, базирующейся на принципе (3). Вместе с тем, ничто не мешает использовать на втором этапе расширения спектра сигнала альтернативные наборы адресных последовательностей, длина которых обеспечит уникальность узлов, передающих информацию.

Рассмотрим пример сети, где на первом этапе расширения спектра для информационного блока, состоящего из $k = 5$ бит, планируется использовать сформированный ранее набор минимальных многочленов степени k над полями $GF(2^5)$. Количество таких многочленов составляет $V = 6$ (см. таблицу 1). Таким образом, число связей между каждым отдельно взятым узлом и всеми остальными узлами сети не должно превышать $N - 1 = 6$.

Очевидно, такая сеть может включать в себя максимум $N = 7$ узлов, для каждого из которых в дальнейшем должна быть определена своя уникальная адресная последовательность A_i , где $i = 1, 2, \dots, 7$ (рисунок 4). Общий вид матрицы соответствия для сети представлена в таблице 7.

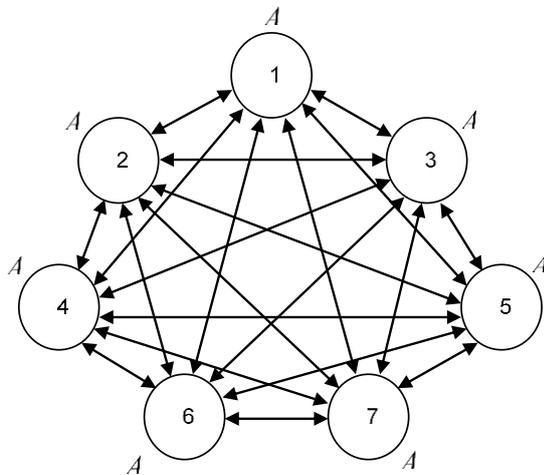


Рис. 4. Сеть параллельной передачи данных, состоящая из $N = 7$ узлов

Fig. 4. Parallel Data Transmission Network Consisting of $N = 7$ Nodes

В качестве адресных последовательностей на втором этапе расширения спектра сигнала, как вариант, могут быть использованы классические функции Уолша длины 8 или комбинации периода $L = 2^4 - 1 = 15$, построенные ранее из линейных рекуррентных последовательностей максимальной длины на основе многочлена $P(x) = x^4 + x + 1$ над полем $GF(2^4)$.

ТАБЛИЦА 7. Матрица соответствия для сети из семи узлов
TABLE 7. Matching Matrix for a Network of Seven Nodes

Номера узлов	Отправители						
	1	2	3	4	5	6	7
Получатели	1	$P_1(x)$	$P_2(x)$	$P_3(x)$	$P_4(x)$	$P_5(x)$	$P_6(x)$
	2	$P_6(x)$	$P_1(x)$	$P_2(x)$	$P_3(x)$	$P_4(x)$	$P_5(x)$
	3	$P_5(x)$	$P_6(x)$	$P_1(x)$	$P_2(x)$	$P_3(x)$	$P_4(x)$
	4	$P_4(x)$	$P_5(x)$	$P_6(x)$	$P_1(x)$	$P_2(x)$	$P_3(x)$
	5	$P_3(x)$	$P_4(x)$	$P_5(x)$	$P_6(x)$	$P_1(x)$	$P_2(x)$
	6	$P_2(x)$	$P_3(x)$	$P_4(x)$	$P_5(x)$	$P_6(x)$	$P_1(x)$
	7	$P_1(x)$	$P_2(x)$	$P_3(x)$	$P_4(x)$	$P_5(x)$	$P_6(x)$

Таким образом, на первом этапе расширения спектра любой, передающий информацию узел-отправитель, определяет, какие узлы-получатели должны будут принять каждый свои $k = 5$ информационных бит. Для этого столбец матрицы соответствия (см. таблицу 7) задает шесть M -последовательностей с соответствующими начальными фазами на основе минимальных многочленов. Эти M -последовательности будут в последствии просуммированы по mod 2 и упакованы в код Голда.

Второй этап расширения спектра произведет замену каждого разряда последовательности Голда на прямую или инверсную адресную последовательность с последующей модуляцией QPSK в режиме передачи одного разряда. Таким образом, каждый узел должен отправить свои разряды последовательности эквивалентного кода Голда в канал связи, используя последовательный принцип передачи данных или разделение частот. На приемной стороне ортогональная природа адресных последовательностей позволит узлу-получателю определить, от каких узлов-отправителей были получены адресные последовательности, восстановить их коды Голда целиком, а затем, используя строку матрицы соответствия (см. таблицу 7), выделить начальные фазы входящих в их состав M -последовательностей.

Заключение

Данная работа рассматривает технологию двойного расширения спектра сигнала, где на первом этапе задаются адреса получателей, а на втором – адреса отправителей информации. Таким образом, идентификация сторон определяется на физическом уровне, что снимает последующую нагрузку на верхние уровни системы передачи данных.

Несомненным преимуществом данного метода расширения спектра сигнала является анонимность, которая обеспечивается матрицами соответствия, хранимыми на узлах сети. При этом возможна также реализация анонимности узлов между собой путем удаления из этих матриц лишних строк и столбцов, отвечающих за связность других узлов-отправителей с узлами-получателями.

Метод кодового уплотнения на основе эквивалентных кодов Голда, применяемый на первом этапе расширения спектра сигнала, вполне можно считать альтернативой используемым до настоящего времени ортогональным методам. Несмотря на свою квазиортогональную природу, последовательности максимальной длины в данном случае ее не используют, так как вся обработка уплотненного сигнала строится на разложении по двойственному базису поля Галуа.

Еще раз отметим основные особенности неортогонального кодового уплотнения на основе последовательностей Голда.

Во-первых, в отличие от классических, эквивалентные последовательности Голда могут включать в себя произвольное число M -последовательностей от разных характеристических полиномов. В приведенных примерах таких рекуррентных последовательностей было шесть.

Во-вторых, последовательности максимальной длины формируют общий сигнал не на основе линейной суммы M -последовательностей, а по mod 2. Полученный при этом код Голда будет иметь единичную максимальную амплитуду сигнала, что в дальнейшем позволит применить к нему фазовый тип модуляции.

В-третьих, отсутствует требование к ортогональности адресных последовательностей, входящих в состав кода Голда, так как не планируется вычисление их скалярного произведения с ним.

В-четвертых, в качестве недостатка рассмотренного метода кодового уплотнения следует отметить исключение нулевого или единичного информационного вектора из адресного пространства, в зависимости от способа представления информации.

Также необходимо учесть ошибки, которые могут возникнуть на приеме после выделения адресных последовательностей. Очевидно, что для их исправления можно было бы использовать некоторый помехоустойчивый код.

Список источников

1. Бабков В.Ю., Никитин А.Н., Осенний К.Н., Сиверс М.А. Системы связи с кодовым разделением каналов. СПб.: ТРМАДА, 2003. 239 с.
2. Бобровский В.И. Многопользовательское детектирование. Ульяновск: Вектор-С, 2007. 346 с.
3. Бобровский В.И. Фрактальные алгоритмы многопользовательского детектирования «плотных» ансамблей сигналов // Техника средств связи. 2019. № 4(148). С. 15–28. EDN:YFHTZY
4. Шахнович И.В. Современные технологии беспроводной связи. М.: Техносфера, 2006. 288 с. EDN:QMPRPT
5. Hajar A., Namamreh J.M., Abewa M., Belallou Y. A Spectrally Efficient OFDM-Based Modulation Scheme for Future Wireless Systems // Proceedings of Scientific Meeting on Electrical-Electronics & Biomedical Engineering and Computer Science (EBBT, Istanbul, Turkey, 24–26 April 2019). IEEE, 2019. DOI:10.1109/EBBT.2019.8742049
6. Du Y., Liu J., Chen Y. Performance Analysis of Nonlinear SFBC OFDM Systems Over TWDP Fading Channel // IEEE Access. 2019. Vol. 7. PP. 101981–101991. DOI:10.1109/ACCESS.2019.2927753
7. Кукунин Д.С., Когновицкий О.С., Березкин А.А., Киричек Р.В. Перспективы использования рекуррентных последовательностей в современной телекоммуникационной среде. СПб.: СПбГУТ, 2023. 289 с.
8. Когновицкий О.С. Широкополосные сигналы данных с расширением спектра прямой последовательностью и их характеристика // Труды учебных заведений связи. 2016. Т. 2. № 1. С. 82–89. EDN:XCGQHP
9. Khudhair A.Y., Abd Khalid R.A. Reduction of the Noise Effect to Detect the DSSS Signal using the Artificial Neural Network // Proceedings of the 1st Babylon International Conference on Information Technology and Science (BICITS, Babil, Iraq, 28-29 April 2021). IEEE, 2021. PP. 185–188. DOI:10.1109/BICITS51482.2021.9509880
10. Visan D.A., Jurian M., Lita I., Ionescu L.M., Mazare A.G. Direct Sequence Spread Spectrum Communication Module for Efficient Wireless Sensor Networks // Proceedings of the 11th International Conference on Electronics Computers and Artificial Intelligence (ECAI, Pitesti, Romania, 27–29 June 2019). IEEE, 2019. DOI:10.1109/ECAI46879.2019.9041979
11. Dmitriyev E.M., Rogozhnikov E.V., Movchan A.K., Mukhamadiev S.M., Krukov Y.V., Duplishcheva N.V. Spread spectrum technology research and its application in power line communication systems // T-Comm. 2020. Vol. 14. Iss. 10. PP. 45–52. DOI:10.36724/2072-8735-2020-14-10-45-52. EDN:VZDBDQ
12. Qiu Z., Peng H., Li T. A Blind Despreading and Demodulation Method for QPSK-DSSS Signal With Unknown Carrier Offset Based on Matrix Subspace Analysis // IEEE Access. 2019. Vol. 7. PP. 125700–125710. DOI:10.1109/ACCESS.2019.2938785
13. Варакин Л.Е. Системы связи с шумоподобными сигналами. М.: Радио и связь, 1985. 384 с.
14. Деев В.В. Методы модуляции и кодирования в современных системах связи. СПб.: Наука, 2007. 268 с.
15. Прокис Дж. Цифровая связь. Пер. с англ. М.: Радио и связь, 2000. 797 с.
16. Никитин Г.И. Применение функций Уолша в сотовых системах связи с кодовым разделением каналов: учебное пособие. СПб.: ГУАП, 2003. 86 с.
17. Кукунин Д.С., Березкин А.А., Киричек Р.В. Многослойные ортогональные структуры на основе последовательностей максимальной длины // Инфокоммуникационные технологии, 2022. Т. 20. № 2(78). С. 42–50. DOI:10.18469/ikt.2022.20.2.05. EDN:DOLLWE
18. Kukunin D., Berezkin A., Kirichek R. Asynchronous Address System Using Code Division Based on Maximum Length Sequences // Proceedings of International Conference on Information, Control, and Communication Technologies (ICCT, As-trakhan, Russian Federation, 03–07 October 2022). IEEE, 2022. DOI:10.1109/ICCT56057.2022.9976772
19. Кукунин Д.С., Березкин А.А., Киричек Р.В., Елисеева К.А. Асинхронная передача данных с использованием многослойных ортогональных структур в системах с кодовым разделением каналов // Электросвязь. 2023. № 1. С. 26–35. DOI:10.34832/ELSV2023.38.1.003. EDN:HNTXND
20. Когновицкий О.С. Двойственный базис и его применение в телекоммуникациях. СПб.: Линк, 2009.

References

1. Babkov V.Yu., Nikitin A.N., Osenniy K.N., Sievers M.A. *Code Division Communication Systems*. St Petersburg: TPMADA Publ.; 2003. 239 p. (in Russ.)
2. Bobrovsky V.N.I. *Multi-user detection*. Ulyanovsk: Vector-C, 2007. 346 p. (in Russ.)
3. Bobrovsky V.I. Fractal algorithms for multiple user detecting of "dense" signal assemblies. *Means of communication equipment*. 2019;4(148):15–28. (in Russ.) EDN:YFHTZY).
4. Shakhnovich I.V. *Modern Wireless Communication Technology*. Moscow: Tekhnosfera Publ.; 2006. 288 c. p. (in Russ.) EDN:QMPRPT
5. Hajar A., Hamamreh J.M., Abewa M., Belallou Y. A Spectrally Efficient OFDM-Based Modulation Scheme for Future Wireless Systems. *Proceedings of Scientific Meeting on Electrical-Electronics & Biomedical Engineering and Computer Science, EBBT, 24–26 April 2019, Istanbul, Turkey*. IEEE; 2019. DOI:10.1109/EBBT.2019.8742049
6. Du Y., Liu J., Chen Y. Performance Analysis of Nonlinear SFBC OFDM Systems Over TWDP Fading Channel. *IEEE Access*. 2019;7:101981–101991. DOI:10.1109/ACCESS.2019.2927753
7. Kukunin D.S., Kognovitsky O.S., Berezkin A.A., Kirichek R.V. *Prospects for the use of recurrent sequences in the modern telecommunications environment*. St Petersburg: The Bonch-Bruевич Saint Petersburg State University of Telecommunications Publ.; 2023. 289 p. (in Russ.)
8. Kognovitskiy O. Wideband Data Signals with Direct Sequence Spread Spectrum and Their Properties. *Proceedings of Telecommunication Universities*. 2016;2(1):82–89. EDN:XCGQHP
9. Khudhair A.Y., Abd Khalid R.A. Reduction of the Noise Effect to Detect the DSSS Signal using the Artificial Neural Network. *Proceedings of the 1st Babylon International Conference on Information Technology and Science, BICITS, 28–29 April 2021, Babil, Iraq*. IEEE; 2021. p.185–188. DOI:10.1109/BICITSS1482.2021.9509880
10. Visan D.A., Jurian M., Lita I., Ionescu L.M., Mazare A.G. Direct Sequence Spread Spectrum Communication Module for Efficient Wireless Sensor Networks. *Proceedings of the 11th International Conference on Electronics Computers and Artificial Intelligence, ECAI, 27–29 June 2019, Pitesti, Romania*. IEEE; 2019. DOI:10.1109/ECAI46879.2019.9041979
11. Dmitriyev E.M., Rogozhnikov E.V., Movchan A.K., Mukhamadiev S.M., Krukov Y.V., Duplishcheva N.V. Spread spectrum technology research and its application in power line communication systems. *T-Comm*. 2020;14(10):45–52. DOI:10.36724/2072-8735-2020-14-10-45-52. EDN:VZDBDQ
12. Qiu Z., Peng H., Li T. A Blind Despreading and Demodulation Method for QPSK-DSSS Signal With Unknown Carrier Offset Based on Matrix Subspace Analysis. *IEEE Access*. 2019;7:125700–125710. DOI:10.1109/ACCESS.2019.2938785
13. Varakin L.E. *Communication Systems with Noise-Like Signals*. Moscow: Radio i svyaz' Publ.; 1985. 384 p. (in Russ.)
14. Deev V.V. *Modulation and Coding Methods in Modern Communication Systems*. St Petersburg: Nauka Publ.; 2007. 268 p. (in Russ.)
15. Proakis J. *Digital Communication*. Translated from English. Moscow: Radio and Communications Publ.; 2000. 797 p. (in Russ.)
16. Nikitin G.I. *Application of Walsh Functions in Cellular Communication Systems with Code Division of Channels*. St Petersburg: Saint-Petersburg State University of Aerospace Instrumentation Publ.; 2003. 86 p. (in Russ.)
17. Kukunin D.S., Berezkin A.A., Kirichek R.V. Multilayer Orthogonal Structures Based on Maximum Length Sequences. *Infokommunikacionnye Tekhnologii*. 2022;20(2-78):42–50. (in Russ.) DOI:10.18469/ikt.2022.20.2.05. EDN:DOLLWE
18. Kukunin D., Berezkin A., Kirichek R. Asynchronous Address System Using Code Division Based on Maximum Length Sequences. *Proceedings of International Conference on Information, Control, and Communication Technologies, ICCT, 03–07 October 2022, Astrakhan, Russian Federation*. IEEE; 2022. DOI:10.1109/ICCT56057.2022.9976772
19. Kukunin D.S., Berezkin A.A., Kirichek R.V., Eliseeva K.A. Asynchronous data transfer using multilayer orthogonal structures in CDMA systems. *Elektrosvyaz*. 2023;1:26–35. (in Russ.) DOI:10.34832/ELSV2023.38.1.003. EDN:HNTXND
20. Kognovitsky O.S. *Dual basis and its application in telecommunications*. St Petersburg: Link Publ.; 2009. (in Russ.)

Статья поступила в редакцию 04.04.2024; одобрена после рецензирования 11.06.2024; принята к публикации 12.06.2024.

The article was submitted 04.04.2024; approved after reviewing 11.06.2024; accepted for publication 12.06.2024.

Информация об авторе:

**КУКУНИН
Дмитрий Сергеевич**

кандидат технических наук, доцент кафедры сетей связи и передачи данных
Санкт-Петербургского государственного университета телекоммуникаций
им. проф. М.А. Бонч-Бруевича
 <https://orcid.org/0000-0002-2674-5217>

Автор сообщает об отсутствии конфликтов интересов.

The author declares no conflicts of interests.

Научная статья

УДК 004.735

<https://doi.org/10.31854/1813-324X-2024-10-3-59-65>

Исследование средней задержки в сетях связи, предоставляющих телемедицинские услуги

Мария Александровна Маколкина, makolkina@sut.ru

Мария Владимировна Шарлаева ✉, masha110.97@mail.ru

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация

Аннотация

Актуальность. По данным исследований консалтинговой компании *Global Market Insights*, объем рынка телемедицины на территории Российской Федерации к 2025 году оценивается в 96 млрд. руб., что более чем в 3 раза превышает показатели 2023 года. Изменения в области систем и сетей телекоммуникаций напрямую влияют на пересмотр архитектуры сети и расширение перечня предоставляемых услуг. Так, появление сетей связи пятого поколения является вынужденной мерой для обеспечения высокой плотности устройств (1 млн. на 1 кв. м) и величины круговой задержки 1 мс. Сети связи 2030 позволят расширить услуги первого набора телемедицинских услуг за счет голографических аватаров, услуг дополненной реальности, Тактильного Интернета.

Цель. Определение зависимости задержки от интенсивности трафика и длительности обслуживания пакетов для первого набора телемедицинских услуг в сетях связи пятого и последующих поколений. Анализ способов оценки качества предоставления услуг телемедицины.

Методы. В работе использованы методы системного анализа, кластерного анализа и теории телетрафика. Выполнено математическое моделирование сети связи.

Решение. Представлены характеристики медицинских данных, которыми оперирует телемедицинская сеть. Сформулированы показатели качества телемедицинских услуг. Разработана модель сети связи пятого и последующих поколений на основе качества предоставления услуг и кластеризации территории. Получены результаты расчетов для пиковых скоростей 5G и 4G, что позволяет определить зависимость задержки от коэффициента вариации длительности обслуживания и от коэффициента вариации интервала между заявками.

Новизна. Элементами научной новизны обладает идея создания и расчета модели сети для предоставления первого набора телемедицинских услуг в сетях связи пятого и последующих поколений, а также использование термина «*Quality of Experience*» для оценки качества в сетях связи, предоставляющих услуги телемедицины.

Значимость. Расположение центров обработки данных в областных или региональных центрах способно обеспечить повсеместное предоставление первого набора телемедицинских услуг в сетях связи с ультрамалыми задержками. За счет формирования цифровых кластеров повышается доступность обращений за медицинской помощью, что позволяет частично сократить цифровой разрыв без необходимости расширения числа медицинских организаций и увеличения численности кадров в удаленных населенных пунктах. Полученные в работе результаты могут быть использованы для определения характеристик оборудования, используемого для предоставления услуг реального времени в сетях связи пятого и последующих поколений.

Ключевые слова: показатели качества телемедицинских услуг, задержка, модель GI/G/1, интенсивность трафика, коэффициент вариации интервала между пакетами, коэффициент вариации времени обслуживания

Ссылка для цитирования: Маколкина М.А., Шарлаева М.В. Исследование средней задержки в сетях связи, предоставляющих телемедицинские услуги // Труды учебных заведений связи. 2024. Т. 10. № 3. С. 59–65. DOI:10.31854/1813-324X-2024-10-3-59-65. EDN:DRRDAM

Original research

<https://doi.org/10.31854/1813-324X-2024-10-3-59-65>

Research of Average Delay in Telecommunication Networks Providing Telemedicine Services

✉ **Maria A. Makolkina**, makolkina@sut.ru

✉ **Maria V. Sharlaeva** ✉, masha110.97@mail.ru

The Bonch-Bruевич Saint Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Annotation

Relevance. According to the research of the consulting company Global Market Insights the volume of the market of telemedicine in the territory of the Russian Federation by 2025 is estimated at 96 billion. Rub. which is more than 3 times higher than the figures of 2023. Changes in telecommunications systems and networks have a direct impact on redesigning the network architecture and expanding the range of services provided. Thus, the emergence of fifth-generation communication networks is a necessary measure to ensure a high density of devices (1 million. per 1 sq. m) and the virtues of circular delay 1 ms. Communication networks 2030 will expand the services of the first set of telemedicine services through holographic avatars, augmented reality services, Tactile Internet.

Purpose. Determination of the dependence of the delay on the intensity of traffic and the duration of packet servicing for the first set of telemedicine services in the communications networks of the fifth and subsequent generations. Analysis of ways to assess the quality of telemedicine services.

Methods. The work uses methods of system analysis, cluster analysis and the theory of teletraffic. Mathematical modeling of the communication network is carried out.

Solution. The characteristics of medical data used by telemedicine network are presented. Quality indicators of telemedicine services have been formulated. The model of communication network of the fifth and subsequent generations based on the quality of service provision and clustering of the territory was developed. The results of calculations for peak speeds 5G and 4G are obtained, which makes it possible to determine the dependence of delay on the coefficient of variation of service duration and on the coefficient of variation of interval between applications.

Novelty. The idea of creating and calculating a network model for the provision of the first set of telemedicine services in fifth- and succeeding-generation networks has elements of scientific novelty, as well as the use of the term «Quality of Experience» for quality assessment in communication networks providing telemedicine services.

Significance (theoretical). The location of data-processing centers in regional or regional centers could provide the first set of telemedicine services on ultra-low latency networks worldwide. The creation of digital clusters improves access to health care, partially reducing the digital divide without the need to expand the number of health organizations and increase the number of staff in remote locations.

Relevance (practical). The results obtained in the work can be used to determine the characteristics of equipment used to provide real-time services in the communications networks of the fifth and subsequent generations.

Keywords: quality indicators of telemedicine services, delay, GI/G/1 model, traffic intensity, variation coefficient of intervals between packets, variation coefficient of service time

For citation: Makolkina M.A., Sharlaeva M.V. Research of Average Delay in Telecommunication Networks Providing Telemedicine Services. *Proceedings of Telecommunication Universities*. 2024;10(3):59–65. (in Russ.) DOI:10.31854/1813-324X-2024-10-3-59-65. EDN:DRRDAM

Введение

Исследование и стандартизация сетей связи пятого и последующих поколений доказывают значительное расширение предоставляемых услуг за счет обеспечения пиковой скорости свыше 1 Тбит/с, минимизации задержки в передаче сигнала до уровня

менее 1 мс, сверхвысоконадежности (коэффициент готовности – 0,999999), недоступности сети не более 4 мс в сутки [1]. Одним из направлений являются медицинские сети. Сфера медицины попадает в различные программы цифровизации федерального масштаба еще с 2011 г. [2]. Например, проекты

«Электронное здравоохранение», «Первичная медико-санитарная помощь», «Цифровой контур здравоохранения» и т. д. Основным приоритетом является повышение доступности получения медицинской помощи. Так как медицина – очень консервативная отрасль, телемедицине удалось стать частью врачебной практики только лишь во время пандемии Covid-19.

Рынок продуктов телемедицины на территории Российской Федерации до начала 2018 г. предусматривал лишь проведение телеконсультации формата «врач–врач» из-за отсутствия законодательной базы. На текущий момент также допускается предоставление телемедицинских услуг формата «врач–пациент». Благодаря национальному проекту «Здравоохранение», телемедицина включена в поликлиническое звено, и возможность получения телеконсультаций имеется у всех пациентов, проходящих лечение в амбулаторных условиях [3]. Частные медицинские организации также предлагают телеконсультации в разных направлениях: телепатология, телехирургия, телерентгенология, теледерматология, телепсихиатрия и др.

В связи с тем, что услуги телемедицины развиваются и становятся популярными, предлагают возможность следить за своим здоровьем, не теряя время на дорогу до медицинского учреждения, а также расширяют возможности для жителей удаленных территорий, вопрос исследования показателей качества предоставления услуг является важным и актуальным.

Показатели качества телемедицинских услуг

Все показатели качества предоставления услуг телемедицины можно разделить на 2 группы: объективные и субъективные. Объективные показатели характеризуют качество обслуживания (QoS, аббр. от англ. Quality of Service) и включают в себя следующие факторы: передачу информации, функционирование приложений, услуги [4]. Примеры наиболее часто используемых показателей представлены в таблице 1 [5–7].

ТАБЛИЦА 1. Показатели QoS

TABLE 1. Indicators of QoS

Группа факторов	Показатели качества
Передача данных	Задержка, скорость передачи данных, джиттер, потери пакетов, полоса пропускания, надежность
Функционирование приложений	Параметры кодека, разрешение видеоданных источника, скорость кодирования, схема маскировки ошибок, схема нивелирования потерь
Услуги	Время переключения между каналами, возможность выбора контента, время отклика

Субъективные показатели представляют компоненты восприятия услуги человеком. Согласно Рекомендации МСЭ-T P.10/G.100, качество восприятия – это общая приемлемость работы приложения или предоставления услуги, которая субъективно воспринимается конечным пользователем [8]. На текущий момент активно проводятся исследования по выявлению объективных показателей восприятия услуг. Объективные и субъективные показатели в сумме дают понимание термина QoE (аббр. от англ. Quality of Experience).

Для проведения субъективной оценки предоставления телемедицинских услуг разработана схема, учитывающая 4 направления: «Доступность», «Эффективность», «Безопасность» и «Ответственность» с позиций всех участников процесса дистанционного взаимодействия, а именно пациента или его законного представителя, медицинского консультанта, оператора телемедицинской информационной системы, медицинской организации, системы здравоохранения [9]. В ней учтены интересы каждого участника процесса телемедицинского консультирования в формате «врач–пациент». Предполагается, что такой подход можно использовать как систематизированную методологию для оценки деятельности медицинских организаций, оказывающих телемедицинские услуги пациентам.

Характеристики телемедицинских услуг

Первый набор услуг телемедицины включает в себя телеконсультации, телемониторинг, телеобучение. Содержание перечисленных видов должно быть понятно, исходя из названий. Телеконсультации предназначены для выдачи рекомендаций и сбора анамнеза. Телемониторинг выполняет функцию контроля за показателями здоровья посредством использования специальных датчиков. Телеобучение предназначено главным образом для поддержания и повышения уровня знаний медицинского персонала. Во всех случаях услуги позволяют оказывать медицинскую помощь населению вне зависимости от территориального расположения.

Телемедицинские услуги оперируют различными типами данных: медицинская запись (текстовые или числовые данные, отражающие сведения мониторинга, ФИО, диагноз, назначенное лечение), данные (результаты анализов, отчеты и другие электронные сведения), черно-белые или цветные статические 2D-изображения, трехмерные изображения, потоковая передача аудиоданных или видеоизображения.

Каждый вид характеризуется объемом передаваемых данных и показателями качества, которые следует обеспечить (таблица 2). На текущий момент одним из основных параметров, характеризующим

ющих качество предоставления телемедицинской услуги, является задержка. Для услуг реального времени, где выполняется передача видеопотоков, т. е. для телеконсультаций и телеобучения, должна обеспечиваться задержка в 10 мс [4].

На горизонте планирования сетей связи 2030, в которых плотность устройств может достигать 1 млн. устройств на 1 км², задержки в передаче сигнала составят менее 1 мс, коэффициент готовности – 0,999999, недоступность сети не более 4 мс в сутки, представляется возможным расширение телемедицинских услуг за счет использования Тактильного Интернета. В частности, в вопросах удаленного проведения хирургических операций и других неинвазивных или инвазивных процедур. В таком случае список требований дополнится синхронностью передачи аудиовизуальной и тактильной информации и обеспечением производительности каналов связи, сопоставимой с возможностями восприятия.

ТАБЛИЦА 2. Характеристики медицинских данных

TABLE 2. Characteristics of medical data

№ п/п	Тип медицинских данных	Средний объем, Мб	Допустимая задержка
1.	Медицинская запись	< 1	1 с
2.	Данные	< 50	Не нормируется
3.	Черно-белое статическое 2D-изображение	< 100	1 с
4.	Цветное статическое 2D-изображение	< 500	1 с
5.	Трехмерное изображение (3D-модель)	< 1000	400 мс
6.	Потоковые аудиоданные, видеоизображение	Зависит от длительности конференции	< 100 мс

Модель сети

Переходя к моделированию сети, следует заметить, что величина задержки зависит от объема передаваемых данных, скорости передачи по линии связи на каждом участке маршрута, возможных задержек на узлах маршрута, вызванных ожиданием в буфере из-за занятости линии ранее обслуживаемыми пакетами данных, времени передачи данных в среде передачи или по каналам и времени распространения сигнала, необходимого пакету для пересечения среды передачи.

Это позволяет представить формулу задержки N_L как сумму всех задержек:

$$N_L = D_P + D_Q + D_T + D_{PR}, \quad (1)$$

где D_P – задержка обработки (от *англ.* Processing Delay); D_Q – задержка постановки в очередь (от *англ.* Queuing Delay); D_T – задержка передачи (от *англ.* Transmission Delay); D_{PR} – задержка распространения (от *англ.* Propagation Delay).

Задержка передачи пакета D_T и задержка распространения пакета D_{PR} могут быть рассчитаны по выражениям:

$$D_T = \frac{N_B}{T_R}, \quad (2)$$

$$D_{PR} = \frac{D}{S_p}, \quad (3)$$

где N_B – объем передаваемых данных; T_R – скорость передачи; D – расстояние; S_p – скорость пакета.

Используя идею кластерного анализа, можно представить структуру модели сети как совокупность окружностей с некоторыми центроидами – точками предоставления услуги доступа (S), которые соединены прямыми с точками предоставления услуг линиями связи (A), а они, в свою очередь, обслуживают несколько пользовательских терминалов (U). В таком случае максимальное расстояние, которое преодолевает сигнал, складывается из расстояния от точки предоставления услуги до точки доступа (R_{S-A}) и от точки доступа до терминала (R_{A-U}):

$$d_{\max} = R_{S-A} + R_{A-U}. \quad (4)$$

Очевидно, что расстояние от точки доступа до терминала много меньше расстояния от точки предоставления услуги до точки доступа:

$$R_{A-U} \ll R_{S-A}. \quad (5)$$

На всем маршруте величина средней задержки складывается из значений задержки на каждом участке:

$$T = \sum_{i=1}^k N_i, \quad (6)$$

где N_i – задержка i -го участка.

Если территория разбивается на некоторое количество кластеров, то каждый кластер можно принять за систему массового обслуживания (СМО) с одним сервером обработки заявок. Обслуживание заявок выполняется по принципу FIFO без использования приоритетов [10].

Входящий поток является Пуассоновским, т. е. случайная величина, характеризующая количество заявок в потоке, распределяется по закону:

$$P_k = \frac{\lambda^k}{k!} * e^{-\lambda}, \quad (7)$$

где k – число заявок в единицу времени; λ – интенсивность потока, т. е. среднее число заявок в единицу времени.

Число пользователей на 1 м² является случайной величиной, в связи с чем вероятность попадания m пользователей в зону обслуживания точкой предоставления услуги также можно описать Пуассоновским распределением.

Тогда интенсивность потока λ сопоставима количеству пользователей в зоне обслуживания ν :

$$\nu = \pi R_{S-A}^2 \eta, \tag{8}$$

где η – плотность пользователей на территории (чел/м²).

Таким образом, вероятность попадания m числа пользователей в зону обслуживания точкой предоставления услуги будет определяться как:

$$P_m = \frac{(\pi R_{S-A}^2 \eta)^m}{m!} * e^{-(\pi R_{S-A}^2 \eta)}. \tag{9}$$

Модель сети GI/G/1 с произвольным распределением интервала поступления между заявками и произвольным распределением длительности обслуживания предполагает, что поток обслуживается одним сервером. Для расчета задержки одного участка сети допускается, что в СМО поступают запросы одного типа. В таких условиях при известных значениях коэффициента вариации и нагрузке, поступающей на узлы, можно рассчитать среднее время пребывания запроса в соответствующем узле при помощи приближенной формулы Манфреда Лангенбаха-Бельца [11]:

Тогда интенсивность потока λ сопоставима количеству пользователей в зоне обслуживания ν :

$$\bar{w} = \frac{\rho_i \bar{t}}{2(1 - \rho_i)} \times \tag{10}$$

$$\times (C(i)_a^2 + C(i)_t^2) g(C(i)_a^2, C(i)_t^2, \rho_i), \tag{11}$$

$$g(C_a^2, C_t^2, \rho) = \begin{cases} e^{-\frac{2(1-\rho)(1-C_a^2)^2}{3\rho(C_a^2+C_t^2)}}, & C_a^2 \leq 1 \\ e^{-(1-\rho)\frac{(C_a^2-1)^2}{C_a^2+4C_t^2}}, & C_a^2 > 1 \end{cases}, \tag{11}$$

где $\rho_i \bar{t}$ – интенсивность нагрузки на i -й узел, $i \in M$ (множество узлов СМО); C_a – коэффициент вариации интервала между заявками (пакетами); C_t – коэффициент вариации времени обслуживания.

Использование канала рассчитывается как произведение числа заявок в единицу времени на среднее время обслуживания в узле:

$$\rho = \lambda \bar{t}. \tag{12}$$

Поскольку расчет выполняется для одного участка сети, номер узла i не фигурирует в формулах (11 и 12).

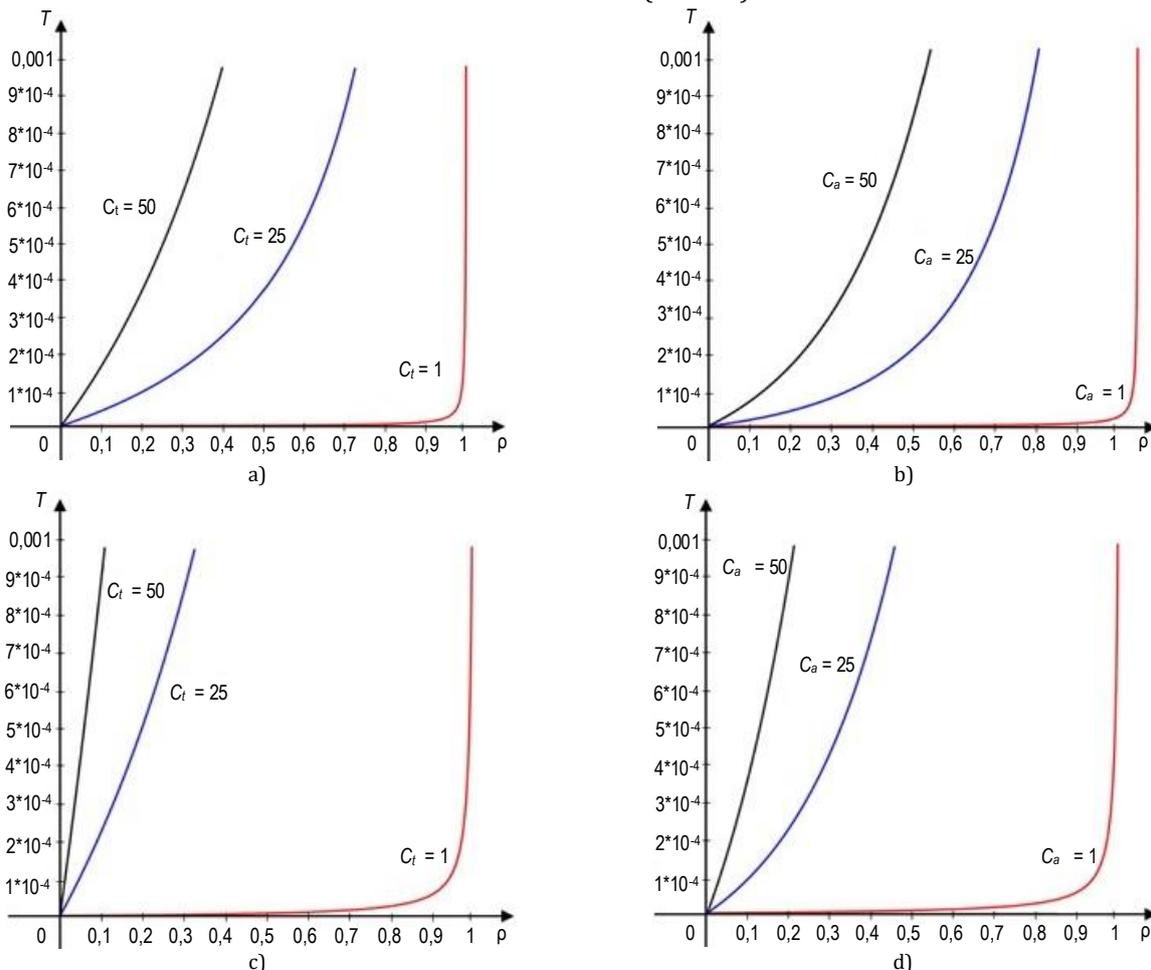


Рис. 1. Зависимость задержки от интенсивности трафика и коэффициента вариации длительности обслуживания C_t и коэффициента вариации для потока C_a для скорости передачи 10 Гбит/с (а и б) и 1 Гбит/с (с и д)

Fig. 1. Delay Dependence on Traffic Intensity and Variation Coefficient of Service Duration C_t and Variation Coefficient for C_a Stream for 10 Gbit/s (a and b) and 1 Gbit/s (c and d) Transmission Rate

Расчет значений задержки для модели GI/G/1

Для выполнения вычислений использован пакет программ MatLab. В качестве значений скорости передачи данных решено использовать пиковые – это 10 Гбит/с в сетях 5G и 1 Гбит/с в сетях 4G [12]. На практике сети 4G и 5G демонстрируют более низкую скорость: 15 и 100 Мбит/с, соответственно. Скорость передачи данных 1 Гбит/с можно считать характерной для сетей доступа в 5G, а 10 Гбит/с – для линий связи между элементами такой сети [13]. По стандартам Ethernet, минимальный размер кадра равен 64 байта (6 байт адрес назначения, 6 – адрес источника, 2 – длина или тип поля данных, 46 – данные, 4 – контрольная последовательность проверки кадра), а максимальный – 1518 байт (6 – адрес назначения, 6 – адрес источника, 2 – длина или тип поля данных, 1500 – данные, 4 – контрольная последовательность проверки кадра). При разработке новых стандартов Ethernet размер кадра остался прежним, чтобы избежать фрагментации и сбора кадров из составляющих.

Очевидно, что при предоставлении нескольких услуг телемедицины размеры передаваемых пакетов будут отличаться от некоторого константного значения. Но так как стоит задача оценить зависимость задержки на ожидание от интенсивности трафика ρ , коэффициента вариации для потока C_a и коэффициента вариации длительности обслуживания C_t , в качестве длины кадра использовано среднее значение выборки, полученной при захвате трафика с помощью среды Wireshark в течение 21345,85 с, равное 755 байт.

Список источников

1. Волков А.Н., Мутханна А.С.А., Кучерявый А.Е. Сети связи пятого поколения: на пути к сетям 2030 // Информационные технологии и телекоммуникации. 2020. № 8. № 2. С. 32–43. DOI:10.31854/2307-1303-2020-8-2-32-43. EDN:ZWNTDB
2. Информационные технологии в медицине // Цифровое здравоохранение на платформе N3.Health. URL: <https://n3health.ru/informacionnye-tehnologii-v-medicine> (дата обращения 10.05.2024)
3. Как внедрение телемедицины повлияло на работу поликлиник // ФГБУ «Редакция «Российской газеты». URL: <https://rg.ru/amp/2022/08/31/telemost-s-vrachom.html> (дата обращения 10.05.2024)
4. Маколкина М.А. Разработка и исследование комплекса моделей трафика и методов оценки качества для дополненной реальности. дис. ... докт. техн. наук. СПб: СПбГУТ, 2020. 436 с. EDN:WTFOWG
5. QoS // Яндекс.Облако. URL: <https://yandex.cloud/ru/docs/glossary/qos> (дата обращения 10.05.2024)
6. Щукина О.Н. К моделированию трафика услуг IP TV с учетом массовой миграции пользователей в периоды рекламных пауз equation section (Next) // T-Comm - Телекоммуникации и Транспорт. 2011. Т. 5. № 7. С. 168–171. EDN:OPICFZ
7. Кодексы, стандарты и форматы кодирования видео // Технофорум Телекоммуникации. URL: <https://forumtech.ru/povosti-v-sfere-telekommunikacij/kodeki-standarty-formaty-vidео> (дата обращения 10.05.2024)
8. Rec. ITU-T P.10/G.100 (11/2017). Vocabulary for performance, quality of service and quality of experience.
9. Владимирский А.В. Матрица оценки качества телемедицинского консультирования «пациент-врач» // Журнал телемедицины и электронного здравоохранения. 2020. Т. 6. № 4. С. 37–44. DOI:10.29188/2542-2413-2020-6-4-34-44. EDN:SLLMVO
10. Захарова Т.В. Оптимальные размещения систем массового обслуживания с дисциплиной обслуживания FIFO // Вестник Московского университета. Серия 15: Вычислительная математика и кибернетика. 2007. № 4. С. 32–37. EDN:JUVAYP
11. Вихрова О.Г. Применение приближенного метода анализа времени установления сессии в подсистеме IMS // Всероссийская конференция с международным участием «Информационно-телекоммуникационные технологии и математическое моделирование высокотехнологичных систем (Москва, Российская Федерация, 22–25 апреля 2014). М.: РУДН, 2014. С. 74–76. EDN:UTBU1B

Результаты полученных расчетов представлены в виде графиков на рисунке 1. Входные данные отличаются только скоростью передачи.

Заключение

С использованием модели сети с произвольным распределением интервала поступления между заявками и произвольным распределением длительности обслуживания получены зависимости задержки от интенсивности трафика и длительности обслуживания пакетов для первого набора телемедицинских услуг в сетях связи пятого и последующих поколений.

Задержка на ожидание в большей степени зависит от коэффициента вариации длительности обслуживания C_t , чем от коэффициента вариации интервала между заявками C_a . Данный факт наблюдается вне зависимости от скорости передачи, ведь при аналогичных показателях интенсивности нагрузки задержка на ожидание имеет большие значения, особенно это прослеживается при повышении коэффициента вариации длительности обслуживания.

В условиях расчета задержки на участке сети модели GI/G/1, где поток обслуживается одним сервером, время между прибытиями имеет общее произвольное распределение, время обслуживания соответствует другому общему закону распределения, а в СМО поступают запросы одного типа, наблюдается линейная зависимость задержки от скорости передачи при равных коэффициентах вариации C_a и C_t .

12. Мордачев В.И. Необходимые ограничения на характеристики систем мобильной (сотовой) связи 4G/5G для обеспечения их безопасности для пользователей // Доклады Белорусского государственного университета информатики и радиоэлектроники. 2022. Т. 20. № 3. С. 54–62. DOI:10.35596/1729-7648-2022-20-3-54-62. EDN:BYMZMW
13. Чистова Н.А. Исследование влияния на сокращение цифрового разрыва и разработка методов формирования цифровых кластеров сетей связи с ультра малыми задержками. Дис. ... канд. техн. наук. СПб: СПбГУТ, 2021. 124 с. EDN:GIIDBP

References

1. Volkov A., Muthanna A., Koucheryavy A. Fifth generation communications networks: on the way to networks 2030. *Telecom IT*. 2020;8(2):32–43. (in Russ.). DOI:10.31854/2307-1303-2020-8-2-32-43. EDN:ZWNTDB
2. *Digital healthcare on the N3.Health platform*. Information technology in medicine. (in Russ.) URL: <https://n3health.ru/informacionnye-tehnologii-v-medicine> [Accessed 10.05.2024]
3. *FSFI «Rossiyskaya gazeta»*. How the introduction of telemedicine has affected the work of polyclinics (in Russ.) URL: <https://rg.ru/amp/2022/08/31/telemost-s-vrachom.html> [Accessed 10.05.2024]
4. Makolkina M.A. *Development and study of a complex of traffic models and methods of quality assessment for augmented reality*. D.Sc Thesis. St. Petersburg: The Bonch-Bruевич Saint-Petersburg State University of Telecommunications Publ.; 2020. 436 p. (in Russ.) EDN:WTFOWG
5. *Yandex.Cloud*. QoS. (in Russ.) URL: <https://yandex.cloud/ru/docs/glossary/qos> [Accessed 10.05.2024]
6. Shchukina O. Modeling IPTV bandwidth demand increased by channel surfing at commercial breaks. *T-Comm*. 2011;5(7):168–171. (in Russ.) EDN:OPICFZ
7. *Technology Forum Telecommunications*. Codecs, standards and video encoding formats. (in Russ.) URL: <https://forumtech.ru/novosti-v-sfere-telekommunikaczij/kodeki-standarty-formaty-video> [Accessed 10.05.2024]
8. Rec. ITU-T P.10/G.100. *Vocabulary for performance, quality of service and quality of experience*. November 2017.
9. Vladzimirsky A.V. Matrix for direct-to-consumer telemedicine quality assessing. *Journal of telemedicine and e-health*. 2020;6(4):37–44. (in Russ.). DOI:10.29188/2542-2413-2020-6-4-34-44. EDN:SLLMVO
10. Zakharova T.V. Optimal arrangements of queuing systems with FIFO service discipline. *Moscow University Computational Mathematics and Cybernetics*. 2007;31(4):163–169. EDN:PGBUJN
11. Vihrova O. Application of the approximate method of analyzing the session establishment time in the subsystem IMS. *Proceedings of the All-Russian Conference with International Participation on Information and Telecommunication Technologies and Mathematical Delimitation of High-Tech Systems, 22–25 April 2014, Moscow, Russian Federation*. Moscow: RUDN University Publ.; 2014. p.74–76. (in Russ.) EDN:UTBUIB
12. Mordachev V.I. Required restrictions on characteristics of 4G/5G mobile (cellular) communications to ensure their safety for users. *Doklady BGUIR*. 2022;20(3):54–62. (in Russ.) DOI:10.35596/1729-7648-2022-20-3-54-62. EDN:BYMZMW
13. Chistova N.A. *Study of influence on reduction of digital gap and development of methods of formation of digital clusters of communication networks with ultra-small support*. PhD Thesis. St. Petersburg: The Bonch-Bruевич Saint-Petersburg State University of Telecommunications Publ.; 2021. 124 p. (in Russ.) EDN:GIIDBP

Статья поступила в редакцию 10.05.2024; одобрена после рецензирования 13.06.2024; принята к публикации 19.06.2024.

The article was submitted 10.05.2024; approved after reviewing 13.06.2024; accepted for publication 19.06.2024.

Информация об авторах:

МАКОЛКИНА
Мария Александровна

доктор технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича

 <https://orcid.org/0000-0002-4251-2691>

ШАРЛАЕВА
Мария Владимировна

аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

 <https://orcid.org/0009-0008-6168-8001>

Авторы сообщают об отсутствии конфликтов интересов.

The authors declare no conflicts of interests.

Научная статья

УДК 621.371.334

<https://doi.org/10.31854/1813-324X-2024-10-3-66-73>

Методика автоматического профилирования электрических характеристик подстилающей поверхности на трассе распространения радиоволн ОНЧ-диапазона

- Алексей Алексеевич Типикин ✉, alextip@mail.ru
- Владимир Александрович Пахотин, v.pakhotin@mail.ioffe.ru
- Денис Сергеевич Потапов, denpotapow@yandex.ru

Научно-исследовательский институт оперативно-стратегических исследований строительства ВМФ ВУНЦ ВМФ «Военно-морская академия имени Адмирала Флота Советского Союза Н.Г. Кузнецова», Санкт-Петербург, 198514, Российская Федерация

Аннотация

Актуальность. Сведения об электрических характеристиках подстилающей поверхности оказывают существенное влияние на результаты расчетов энергетических параметров радиотрасс диапазона очень низких частот. В настоящее время разработаны различные варианты цифровых карт, которые потенциально способны повысить точность расчетов и упростить действия оператора по вводу исходных данных, однако возможности цифровой картографии не внедрены в существующие методики прогнозирования. **Целью исследования** является снижение количества ручных операций в ходе прогнозирования энергетических параметров радиотрасс диапазона очень низких частот путем разработки методики, позволяющей автоматизировать ввод электрических характеристик подстилающей поверхности. **Методы.** Для рационального обоснования выбора уровней квантования электрических параметров радиотрасс в работе использованы методы математической статистики. Для получения профиля электрических характеристик, отвечающего требованиям методики прогнозирования, использован метод интерполяции с заданным коэффициентом децимации. **Результаты.** С помощью статистических оценок выбраны уровни и интервалы квантования электрических характеристик подстилающей поверхности, которые используются при формировании горизонтальных профилей. Далее для исключения участков с частым изменением значений характеристик выполняется интерполяция методом «ближайшего соседа» с заданным коэффициентом децимации, который выбирается исходя из того, что наименьшая длина однородного участка не должна быть меньше длины волны. Разработанная методика реализована в среде моделирования Matlab и представляет собой совокупность скриптов и вспомогательных функций. Приведен пример использования методики в рамках прогнозирования напряженности поля земной волны на разнородной трассе. **Новизна** заключается в разработке оригинальной методики, обеспечивающей рациональное профилирование электрической проводимости и диэлектрической проницаемости земной поверхности для последующего использования полученных данных в задачах прогнозирования энергетических параметров радиотрасс диапазона очень низких частот. **Практическая значимость.** Разработанная методика позволяет снизить нагрузку на оператора при вводе исходных данных и повысить точность представления этих данных. Методика может быть использована в скачковом методе прогнозирования энергетических параметров радиотрасс для определения векторной суммы пространственной и земной волн в точке приема.

Ключевые слова: подстилающая поверхность, электрические характеристики, очень низкие частоты, радиотрасса, горизонтальный профиль, прогнозирование энергетических параметров

Ссылка для цитирования: Типикин А.А., Пахотин В.А., Потапов Д.С. Методика автоматического профилирования электрических характеристик подстилающей поверхности на трассе распространения радиоволн диапазона очень низких частот // Труды учебных заведений связи. 2024. Т. 10. № 3. С. 66–73. DOI:10.31854/1813-324X-2024-10-3-66-73. EDN:MHACGD

Original research

<https://doi.org/10.31854/1813-324X-2024-10-3-66-73>

Technique for Automatic Profiling of Underlying Surface Electric Parameters on the Very Low Frequencies Radio Path

✉ **Aleksey A. Tipikin**, alextip@mail.ru
✉ **Vladimir A. Pakhotin**, v.pakhotin@mail.ioffe.ru
✉ **Denis S. Potapov**, denpotapow@yandex.ru

Navy Development of the Military Research and Educational Center of the Navy "Naval Academy named after Admiral of the Fleet of the Soviet Union N.G. Kuznetsov"
St. Petersburg, 198514, Russian Federation

Annotation

Relevance. Information about the electrical characteristics of the underlying surface has a significant impact on the calculations results of the radio tracks energy parameters in the very low frequency band. Currently, various versions of developed digital maps can potentially improve the accuracy of calculations and simplify the operator's activities in the initial data input. However, the capabilities of digital cartography are not integrated into existing forecasting techniques. The **purpose of the study** is to reduce the number of manual operations during the forecasting of the radio tracks energy parameters in the very low frequency band by developing a technique that allows to automate the input of the underlying surface electrical parameters. **Methods.** In this study we used methods of mathematical statistics to choose the quantization levels of radio tracks electrical parameters rationally. We used an interpolation method with a given decimation coefficient to obtain an electrical characteristics profile that meets the requirements of the forecasting methodology. **Result.** We selected the levels and quantization intervals of the underlying surface electrical characteristics which are needed to obtain the horizontal profiles, using statistical estimates. Further, we performed interpolation with the «nearest neighbor» method with a given decimation coefficient to exclude areas with frequent changes in the profiling parameters values. The decimation coefficient relies on the condition that the smallest length of a homogeneous section should not be less than the wavelength. The developed technique is implemented in the Matlab modeling environment as a combination of scripts and auxiliary functions. We provided an example of the technique application as the forecasting the ground wave field strength on a heterogeneous track. The **novelty** lies in the development of an original technique that provides rational profiling of the underlying surface electrical conductivity and dielectric permittivity for the subsequent usage of the obtained data in the forecasting the radio tracks energy parameters in the very low frequency band. **Practical significance.** The developed technique makes it possible to reduce the operator load during the initial data input and increases the accuracy of presenting this data. The technique can be used in a wavehop method for the predicting the radio tracks energy parameters to determine the vector sum of spatial and ground waves at the receiver.

Keywords: *underlying surface, electrical characteristics, very low frequencies, radio path, horizontal profile, energy parameters prediction*

For citation: Tipikin A.A., Pakhotin V.A., Potapov D.S. Technique for Automatic Profiling of Underlying Surface Electric Parameters on the Very Low Frequencies Radio Path. *Proceedings of Telecommunication Universities*. 2024;10(3): 66–73. (in Russ.) DOI:10.31854/1813-324X-2024-10-3-66-73. EDN:MHACGD

Введение

Определение характеристик подстилающей поверхности на трассе распространения радиоволн – одна из важнейших проблем прогнозирования энергетических параметров радиотрасс. От проводимости и диэлектрической проницаемости под-

стилающей поверхности напрямую зависит дальность распространения радиоволн [1, 2], в том числе волн диапазона очень низких частот (ОНЧ), занимающего промежуток частот от 3 до 30 кГц. В модели распространения радиоволн ОНЧ-диапазона поверхность Земли и ионосфера образуют сферический волновод, поэтому для наиболее

адекватного прогнозирования энергетических параметров радиотрасс необходимо как можно точнее знать характеристики стенок этого волновода. Для ионосферы получена и периодически уточняется международная эталонная модель ионосферы, находящаяся в свободном доступе [3–5]; для земной поверхности разработаны карты электрических характеристик в ОНЧ-диапазоне [6–8], отличающиеся от известных карт [9, 10] более высокой детализацией, глобальным охватом и наличием сведений о диэлектрической проницаемости. Основой для картирования электрических характеристик земной поверхности могут также служить карты геоэлектрических разрезов [11].

Общим недостатком всех существующих карт является невозможность их непосредственного использования при прогнозировании распространения радиоволн. Это связано с тем, что карты, представленные на бумажных носителях, требуют оцифровки. Если карта уже оцифрована, то необходимо составить горизонтальный профиль электрических характеристик земной поверхности. Указанная задача не является тривиальной по следующим причинам: во-первых, электрические характеристики земной поверхности вдоль радиотрассы могут меняться либо непрерывно, либо весьма часто, поэтому необходим обоснованный выбор количества участков профиля, с одной стороны, не слишком большого, чтобы не перегружать вычисления, а с другой стороны не слишком малого, чтобы чрезмерно не загроублять их; во-вторых, операция профилирования должна быть автоматической и обходиться без участия оператора по вводу дополнительных данных.

Таким образом, указанные недостатки определяют цель исследования, которая заключается в разработке методики автоматического профилирования электрических характеристик земной поверхности с использованием глобальных цифровых карт [7, 8] и входных данных на основе задачи расчета напряженности поля пространственной волны, описанной в [12].

Методика

Первым этапом методики является квантование картографических данных. Процесс квантования представляет собой отображение переменной x , зафиксированной на карте и определенной на множестве N непрерывных непересекающихся интервалов \mathcal{R}_i , $i = 1, 2, \dots, N$, называемых интервалами квантования, во множество дискретных значений \hat{x}_i , $i = 1, 2, \dots, N$, называемых уровнями квантования, причем \hat{x}_i находится в пределах интервала \mathcal{R}_i [13]. Для выполнения процедуры квантования необходимо разбить непрерывное множество \mathcal{R} на интервалы квантования \mathcal{R}_i и назначить уровни квантования \hat{x}_i .

Формально процедуру квантования можно записать в виде выражения:

$$Q(x|x \in \mathcal{R}) \Rightarrow \hat{x}|\hat{x}_i \in \mathcal{R}_i; \quad i = 1, 2, \dots, N. \quad (1)$$

Для электрической проводимости в диапазоне от 10^{-6} до $1,7$ См/м квантование осуществляется в соответствии с таблицей 1 рекомендации [10]. В области $\sigma > 1,7$ См/м границы интервалов квантования выбираются, исходя из статистических характеристик данных таким образом, чтобы в полученные интервалы попадали пики гистограммы. Часть гистограммы в диапазоне от $1,5$ до 6 См/м показана на рисунке 1, где штриховыми линиями обозначены границы интервалов квантования. В качестве уровней квантования выбираются медианы соответствующих интервалов.

ТАБЛИЦА 1. Интервалы и уровни квантования проводимости подстилающей поверхности

TABLE 1. Intervals and Levels of Quantization of the Underlying Surface Conductivity

Проводимость, См/м	
Интервал квантования	Уровень квантования
$\sigma < 1,7 \cdot 10^{-5}$	10^{-5}
$1,7 \cdot 10^{-5} \leq \sigma < 5,5 \cdot 10^{-5}$	$3 \cdot 10^{-5}$
$5,5 \cdot 10^{-5} \leq \sigma < 1,7 \cdot 10^{-4}$	10^{-4}
$1,7 \cdot 10^{-4} \leq \sigma < 5,5 \cdot 10^{-4}$	$3 \cdot 10^{-4}$
$5,5 \cdot 10^{-4} \leq \sigma < 1,7 \cdot 10^{-3}$	10^{-3}
$1,7 \cdot 10^{-3} \leq \sigma < 5,5 \cdot 10^{-3}$	$3 \cdot 10^{-3}$
$5,5 \cdot 10^{-3} \leq \sigma < 1,7 \cdot 10^{-2}$	0,01
$0,017 \leq \sigma < 0,055$	0,03
$0,055 \leq \sigma < 0,17$	0,11
$0,17 \leq \sigma < 0,55$	0,36
$0,55 \leq \sigma < 1,7$	1,13
$1,7 \leq \sigma < 3,3$	2,69
$3,3 \leq \sigma < 4,7$	3,94
$\sigma \geq 4,7$	5,49

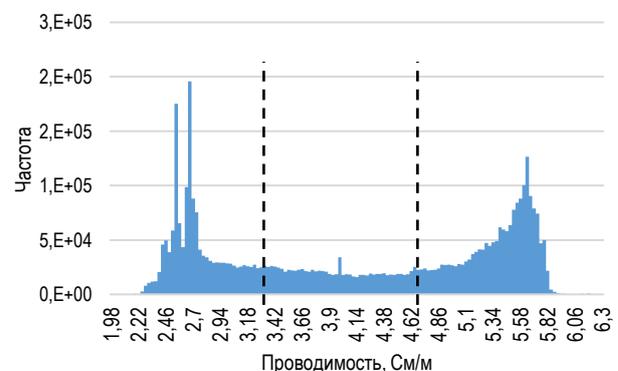


Рис. 1. Гистограмма значений проводимости подстилающей поверхности

Fig. 1. Histogram of Underlying Surface Conductivity Values

Аналогичные подходы применены для квантования диэлектрической проницаемости, с той разницей, что интервалы квантования выбирались исходя из частот значений проницаемости во всем возможном диапазоне (в данном случае под частотой понимается термин математической статистики – частота признака). Границы интервалов квантования и уровни квантования представлены в таблице 2.

Вторым этапом после квантования является интерполяция, которая заключается в вычислении неизвестного значения зависимой переменной, внутри некоторого отрезка, по известным значениям этой переменной на концах этого отрезка. Интерполяция выполняется путем поиска функции f , которая принимает известные значения y_i в заданных точках x_i , т. е. выполняется $f(x_i) = y_i$ для всех i . Метод ближайшего соседа заключается в том, что функции на заданном интервале присваивается значение, равное ближайшему известному значению функции [14].

ТАБЛИЦА 2. Интервалы и уровни квантования диэлектрической проницаемости подстилающей поверхности

TABLE 2. Intervals and Levels of Quantization of the underlying Surface Dielectric Permittivity

Диэлектрическая проницаемость, 1/м	
Интервал квантования	Уровень квантования
$\epsilon < 2,5$	1,9
$2,5 \leq \epsilon < 4,5$	3,9
$4,5 \leq \epsilon < 7$	5,4
$7 \leq \epsilon < 10$	8,3
$10 \leq \epsilon < 15$	12,8
$15 \leq \epsilon < 67$	41
$67 \leq \epsilon < 72$	69,6
$72 \leq \epsilon < 77$	74,6
$\epsilon \geq 77$	79,5

В данном случае интерполяция методом ближайшего соседа используется совместно с децимацией интерполируемых точек в необходимой пропорции, чтобы исключить участки с частым изменением значений электрических характеристик. Для этого задается условие, в соответствии с которым наименьшая длина однородного участка не может быть меньше длины волны.

Реализация методики

Методика реализована в виде скрипта Matlab. Блок-схема методики показана на рисунке 2. После запуска скрипта загружаются исходные данные, включающие интерполяционные объекты с электрическими параметрами подстилающей поверхности, объект геопривязки, расчетные частоты, координаты начала и конца радиотрассы и границы

интервалов квантования проводимости и диэлектрической проницаемости поверхности Земли (блок 1). Все данные, кроме границ интервалов квантования, берутся из решения задачи об определении напряженности поля пространственной волны [12].

Далее открывается цикл для определения квантованных значений проводимости (блоки 2–8), в котором с помощью операторов ветвления (блоки 3 и 5) рассматриваются три различных случая:

$$\sigma < \sigma_1, \sigma \geq \sigma_n,$$

$$\sigma_{i-1} \leq \sigma < \sigma_i, i = 2, 3, \dots, n,$$

где n – количество интервалов квантования.

В блоках 4, 6 и 7 вычисляются медианные значения параметров на интервале. Аналогичные операции выполняются в цикле для определения квантованных значений проницаемости (блоки 9 и 10), квантованные значения параметров записываются в соответствующие переменные (блок 11). Затем открывается цикл по расчетным частотам (блок 12), для каждой из которых составляется горизонтальный профиль подстилающей поверхности с помощью функции mapprofile (блок 13). В блоке 14 выполняется квантование профилей с помощью найденных квантованных значений и заданных интервалов квантования путем вызова функции quantiz. В блоке 15 осуществляется интерполирование квантованного профиля с децимацией интерполируемых точек. Полученные данные записываются в структуру segsData, которая содержит входные данные для расчета напряженности поля земной волны (блок 16). Операции, указанные в блоках 2–12, являются предварительными и непосредственно во время профилирования не выполняются, так как используются уже найденные квантованные значения, загружаемые из сохраненных переменных.

Пример расчета напряженности Земной волны с помощью полученного профиля

В качестве примера на рисунке 3 показана трасса Нижний Новгород (56,25° с. ш., 44,00° в. д.) – Гренландское море (75,00° с. ш., 0,00° в. д.), протяженность трассы составляет 2775,9 км. Около 2/3 трассы составляет континентальный участок, проходящий через северо-западную часть Восточно-Европейской равнины с проводимостью 0,01–0,03 См/м и Скандинавский полуостров с преимущественной горной и каменистой поверхностью, проводимость которой составляет 0,001–0,003 См/м. Оставшаяся часть трассы проходит через Гренландское море с высокой проводимостью и диэлектрической проницаемостью. Для указанной трассы выполнено горизонтальное профилирование электрических характеристик земной поверхности с последующим квантованием и интерполяцией полученного профиля. Результаты профилирования показаны на рисунке 4.

На основе найденного профиля получена зависимость напряженности поля земной волны от расстояния с помощью методики [15], где для выполнения серии расчетов и построения зависимости напряженности поля земной волны от расстояния на каждом однородном i -м участке трассы ($i \geq 2$) использовано сглаживание экспоненциальной функцией вида $1/\exp[(x - a)/b]$. Коэффициенты a

и b подбираются таким образом, чтобы выполнялось условие $E(d) = \frac{1}{2} (E_{i-1}(d) + E_i(d))$, где E_i – рассчитывается исходя из однородности оставшегося участка трассы с параметрами σ_i и ϵ_i , E_{i-1} берется с предыдущей итерации цикла и $d = d_{i-1}^2 + 2(d_{i-1}^2 - d_{i-1}^1)$. Здесь верхний индекс 1 обозначает начальную точку соответствующего однородного участка, 2 – конечную.

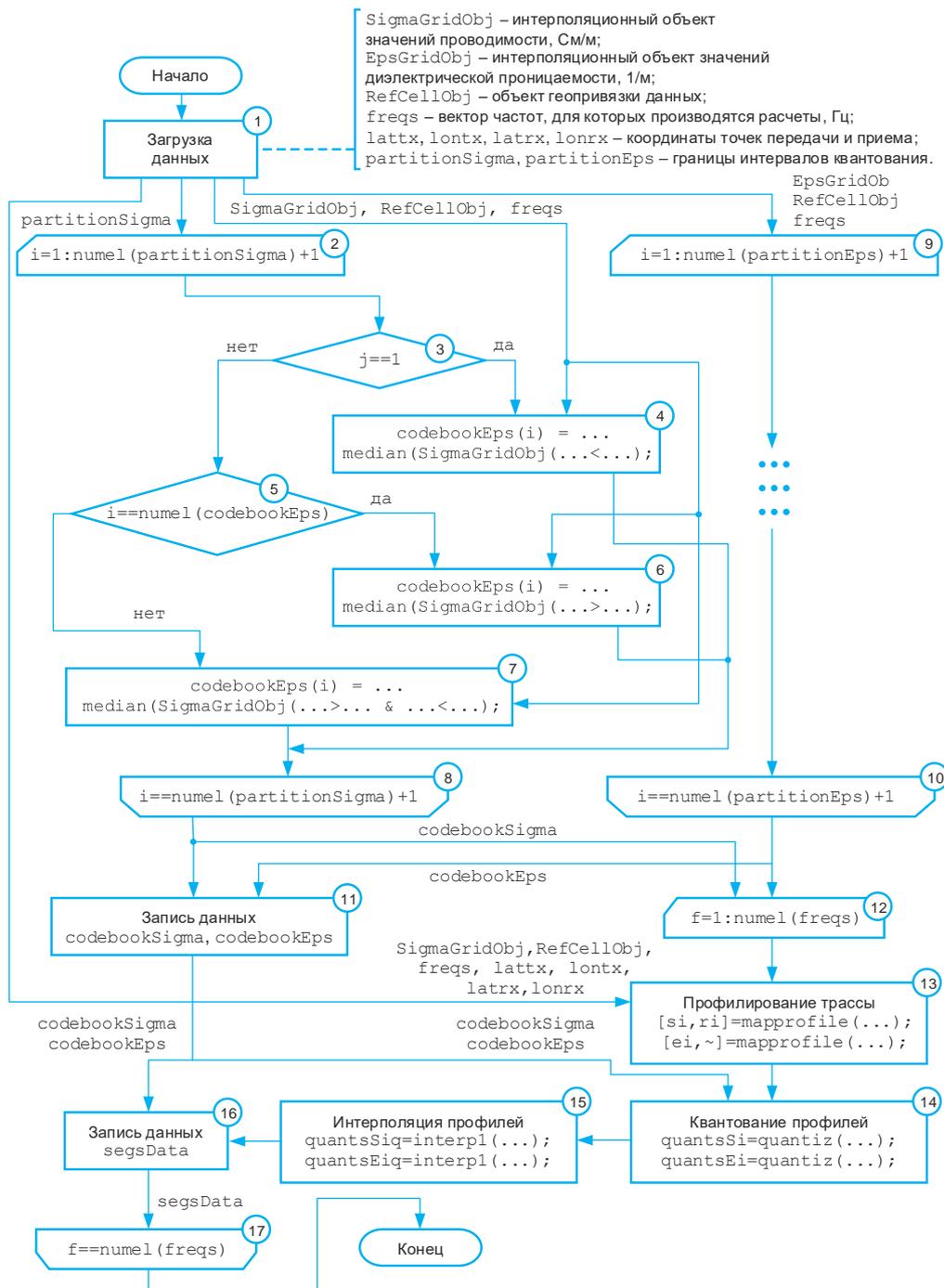


Рис. 2. Блок-схема методики
Fig. 2. Flowchart of the Technique

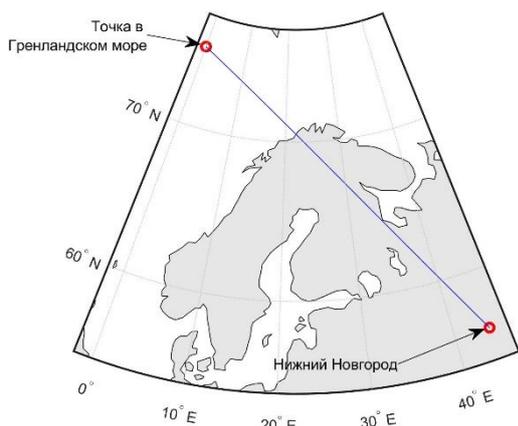


Рис. 3. Радиотрасса Нижний Новгород – Гренландское море
Fig. 3. Radio Path Nizhny Novgorod – Greenland Sea

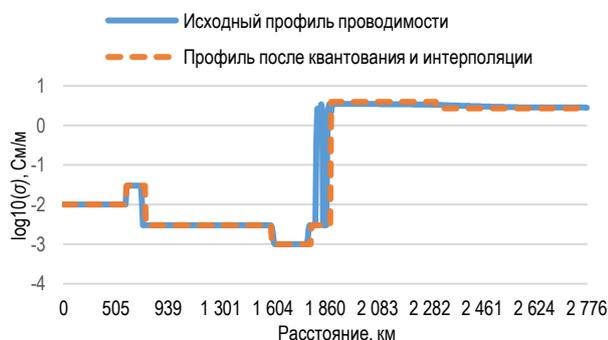


Рис. 4. Профили электрических параметров подстилающей поверхности
Fig. 4. Profiles of Underlying Surface Electric Parameters

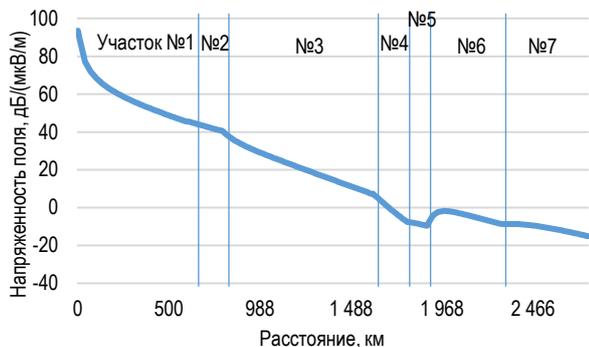


Рис. 5. График зависимости напряженности поля земной волны от расстояния
Fig. 5. Groundwave E-Field versus Distance Plot

Результаты расчетов для частоты 150 кГц графически отображены на рисунке 5, из которого видно, что для первых пяти участков наблюдается примерно равномерное затухание сигнала за исключением участка № 4, где значение проводимости наиболее низкое. После перехода трассы от континентальной части к морской (участки № 6 и № 7) виден эффект «восстановления» [16, 17], так как проводимость морской поверхности существенно выше, чем континентальной. Электрические параметры профиля показаны в таблице 3.

ТАБЛИЦА 3. Горизонтальный профиль электрических параметров подстилающей поверхности на трассе Нижний Новгород – Гренландское море

TABLE 3. Horizontal Profile of Underlying Surface Electric Parameters on the Path Nizhny Novgorod – Greenland Sea Radio Path

Номер участка	Проводимость, См/м	Диэлектрическая проницаемость, 1/м	Длина участка, км
1	0,01	8,3	607,5
2	0,03	12,8	170,6
3	0,003	5,4	820,1
4	0,001	3,9	196,3
5	0,003	14,3	93,5
6	3,94	76,4	418,2
7	2,69	78,7	469,7

Выводы

Таким образом, разработана методика автоматического профилирования электрических характеристик земной поверхности на трассе распространения радиоволн, которая позволяет получить горизонтальный профиль квантованных характеристик земной поверхности и использовать полученные данные для расчета напряженности поля земной волны. Расчеты напряженности поля земной волны являются составной частью комплексных вычислений для определения энергетических параметров радиотрассы скачковым методом [18]. Однако точный характер влияния прогнозных значений напряженности поля земной волны на суммарное поле в точке приема требует дополнительных исследований.

Методика также может быть использована для получения горизонтальных профилей радиотрассы с целью их использования в других расчетных методиках, основанных на волновом методе [19] и методах вычислительной электродинамики [20].

Практическая значимость полученной методики заключается в автоматизации процесса ввода исходных данных при прогнозировании энергетических параметров радиотрасс ОНЧ-диапазона. Все необходимые сведения для выполнения профилирования получают в ходе решения задачи прогнозирования напряженности поля пространственной (ионосферной) волны [12], являющейся обязательным этапом при поиске суммарного поля в точке приема, включающего пространственную и земную волны. Непосредственно профили электрических характеристик подстилающей поверхности строятся на базе цифровых карт [7, 8], но могут быть использованы и другие карты, например [11]. Еще один аспект практической значимости заключается в снижении нагрузки на оператора, выполняющего прогнозирование, и сокращении времени, затрачиваемого на решение данной задачи.

Список источников

1. Coleman C. *Analysis and Modeling of Radio Wave Propagation*. Cambridge: Cambridge University Press, 2017. 296 p. DOI:10.1017/9781316798607
2. Gonzalez G. *Advanced Electromagnetic Wave Propagation Methods*. Boca Raton: CRC Press, 2022. 708 p.
3. Bilitza D. IRI the international Standard for the ionosphere // *Advances in Radio Science*. 2018. Vol. 16. PP. 1–11. DOI:10.5194/ars-16-1-2018
4. Froñ A., Galkin I., Krankowski A., Bilitza D., Hernández-Pajares M., Reinisch B., et al. Towards Cooperative Global Mapping of the Ionosphere: Fusion Feasibility for IGS and IRI with Global Climate VTEC Maps // *Remote Sensing*. 2020. Vol. 12. Iss. 21. P. 3531. DOI:10.3390/rs12213531
5. Galkin I., Fron A., Reinisch B., Hernández-Pajares M., Krankowski A., Nava B., et al. Global Monitoring of Ionospheric Weather by GIRO and GNSS Data Fusion // *Atmosphere*. 2022. Vol. 13. Iss. 3. P. 371. DOI:10.3390/atmos13030371
6. Типикин А.А., Потапов Д.С. Методика оценки электрических характеристик почвы на трассе распространения земных радиоволн // *Техника радиосвязи*. 2022. № 1(52). С. 19–29. DOI:10.33286/2075-8693-2022-52-19-29
7. Типикин А.А. Методика формирования глобальных цифровых карт электрических характеристик подстилающей поверхности в диапазоне очень низких частот // *Информатика, телекоммуникации и управление*. 2022. Т. 15. № 1. С. 7–18. DOI:10.18721/JCSTCS.15101
8. Типикин А.А., Парафейник Д.В., Потапов Д.С. Результаты исследований по формированию цифровых картографических данных электрических характеристик подстилающей поверхности в диапазоне СДВ // *Морской вестник*. 2023. № S1(16). С. 27–29. EDN:JDEEVY
9. Morgan R.R. World-wide VLF effective conductivity map. Report 8013F-1 Westinghouse Electric Corporation, 1968. 62 p.
10. Рекомендация МСЭ-R P.832-4 (07/2015) Мировой атлас проводимости почвы.
11. Башкуев Ю.Б., Ангархаева Л.Х., Буянова Д.Г., Адвокатов В.Р. Прогнозная карта геоэлектрических разрезов континентов земного шара // V Международная научно-техническая конференция «Радиотехника, электроника и связь» (Омск, Российская Федерация, 07–09 октября 2019). Омск: Омский научно-исследовательский институт приборостроения, 2019. С. 17–24. DOI:10.33286/978-5-6041917-2-9.17-24. EDN:DKVXOV
12. Типикин А.А. Методика расчета напряженности поля ионосферной волны в диапазоне очень низких частот на основе скачкового метода // *Информационно-управляющие системы*. 2023. № 5. С. 12–21. DOI:10.31799/1684-8853-2023-5-12-21. EDN:FTXMCY
13. Кучмин Н.А., Никитин О.Р. Квантователи речевого сигнала // *The Scientific Heritage*. 2021. № 81-1(81). С. 46–50. DOI:10.24412/9215-0365-2021-81-1-46-50. EDN:WBHCVJ
14. Трубаков А.О., Селейкович М.О. Сравнение интерполяционных методов масштабирования растровых изображений // *Научно-технический сборник Брянского государственного университета*. 2017. № 1. С. 92–97. DOI:10.22281/2413-9920-2017-03-01-92-98. EDN:YHFCGF
15. Типикин А.А. Обобщённая методика расчёта напряжённости поля земной волны диапазона очень низких частот для трассы с произвольным количеством однородных участков // *Вестник Рязанского государственного радиотехнического университета*. 2023. № 87. С. 21–28. DOI:10.21667/1995-4565-2024-87-21-28. EDN:NRQFAG
16. Дембелов М.Г., Башкуев Ю.Б., Мельчинов В.П. Поле земной волны над протяженными неоднородными радиотрассами // *Журнал радиоэлектроники*. 2019. № 11. DOI:10.30898/1684-1719.2019.11.11. EDN:NASWEE
17. Рекомендация МСЭ-R P.368-9 (2007) Кривые распространения земной волны для частот между 10 кГц и 30 МГц.
18. Pal S., Basak T., Chakrabarti S.K. Results of Computing Amplitude and Phase of the VLF Wave Using Wave Hop Theory // *Advances in Geosciences*. 2011. Vol. 27. PP. 1–11. DOI:10.1142/9789814355414_0001
19. Gasdia F., Marshall R.A. A New Longwave Mode Propagator for the Earth-Ionosphere Waveguide // *IEEE Transactions on Antennas and Propagation*. 2021. Vol. 69. Iss. 12. PP. 8675–8688. DOI:10.1109/TAP.2021.3083753
20. Marshall R.A., Wallace T., Turbe M. Finite-difference modeling of very-low-frequency propagation in the Earth-ionosphere waveguide // *IEEE Transactions on Antennas and Propagation*. 2017. Vol. 65. Iss. 12. PP. 7185–7197. DOI:10.1109/TAP.2017.2758392

References

1. Coleman C. *Analysis and Modeling of Radio Wave Propagation*. Cambridge: Cambridge University Press; 2017. 296 p. DOI:10.1017/9781316798607
2. Gonzalez G. *Advanced Electromagnetic Wave Propagation Methods*. Boca Raton: CRC Press; 2022. 708 p.
3. Bilitza D. IRI the international Standard for the ionosphere. *Advances in Radio Science*. 2018;16:1–11. DOI:10.5194/ars-16-1-2018
4. Froñ A., Galkin I., Krankowski A., Bilitza D., Hernández-Pajares M., Reinisch B., et al. Towards Cooperative Global Mapping of the Ionosphere: Fusion Feasibility for IGS and IRI with Global Climate VTEC Maps. *Remote Sensing*. 2020;12(21):3531. DOI:10.3390/rs12213531
5. Galkin I., Fron A., Reinisch B., Hernández-Pajares M., Krankowski A., Nava B., et al. Global Monitoring of Ionospheric Weather by GIRO and GNSS Data Fusion. *Atmosphere*. 2022;13(3):371. DOI:10.3390/atmos13030371
6. Tipikin A.A., Potapov D.S. Evaluation of the electrical characteristics of the soil on the path of propagation of surface radio waves. *Tekhnika radiosvyazi*. 2022;1(52):19–29. (in Russ.) DOI:10.33286/2075-8693-2022-52-19-29
7. Tipikin A.A. Method of obtaining global digital maps of underlying surface electric characteristics in the very low frequency band. *Computing, telecommunication and control*. 2022;15(1):7–18. (In Russ.) DOI:10.18721/JCSTCS.15101

8. Tipikin A.A., Parafejnik D.V., Potapov D.S. The Research Results on the Development of Digital Cartographic Data of the Electrical Characteristics of the Underlying Surface in the Very Low Frequency Band. *Morskoy vestnik*. 2023;S1(16):27–29. (In Russ.) EDN:JDEEVY
9. Morgan R.R. *World-wide VLF effective conductivity map*. Report 8013F-1. Morgan R.R. Westinghouse Electric Corporation, 1968. 62 p.
10. ITU-R Recommendation P.832-4. *World atlas of ground conductivities*. July 2015.
11. Bashkuev Yu.B., Angarkhaeva L.Kh., Buyanova D.G., Advokatov V.R. Predictive map of geoelectric sections of continents of the world. *Proceedings of the V International Scientific-Technical Conference on Radio Engineering, Electronics and Communications, 07–09 October 2019, Omsk, Russian Federation*. Omsk: Omsk Scientific-Research Institute of Instrument Engineering Publ.; 2019. p.17–24. (In Russ.) DOI:10.33286/978-5-6041917-2-9.17-24. EDN:DKVXOV
12. Tipikin A.A. The technique of calculating the field strength of the ionospheric wave in the very low frequency band based on the wavehop method. *Information and Control Systems*. 2023;5:12–21. (In Russ.) DOI:10.31799/1684-8853-2023-5-12-21. EDN:FTXMCY
13. Kuchmin N.A., Nikitin O.R. Quantizers for speech signal. *The Scientific Heritage*. 2021;81-1(81):46–50. (In Russ.) DOI:10.24412/9215-0365-2021-81-1-46-50. EDN:WBHCVJ
14. Trubakov A.O., Seleykovich M.O. Comparison of interpolation methods for raster images scaling. *Scientific and Technical Journal of Bryansk State University*. 2017;1:92–97. (In Russ.) DOI:10.22281/2413-9920-2017-03-01-92-98. EDN:YHFCGF
15. Tipikin A.A. Generalized method to calculate field strength of ground wave in very low frequency band for a path with arbitrary number of homogeneous segments. *Vestnik of Ryazan State Radio Engineering University*. 2024;87:21–28. (In Russ.) DOI:10.21667/1995-4565-2024-87-21-28. EDN:NRQFAG
16. Dembelov M.G., Bashkuev Yu.B., Melchinov V.P. Field of the earth wave over long inhomogeneous radio paths. *Journal of Radio Electronics*. 2019;11. (In Russ.) DOI:10.30898/1684-1719.2019.11.11. EDN:NASWEE
17. ITU-R Recommendation P.368-9. *Ground-wave propagation curves for frequencies between 10 kHz and 30 MHz*. 2007.
18. Pal S., Basak T., Chakrabarti S.K. Results of Computing Amplitude and Phase of the VLF Wave Using Wave Hop Theory. *Advances in Geosciences*. 2011;27:1–11. DOI:10.1142/9789814355414_0001
19. Gasdia F., Marshall R.A. A New Longwave Mode Propagator for the Earth-Ionosphere Waveguide. *IEEE Transactions on Antennas and Propagation*. 2021;69(12):8675–8688. DOI:10.1109/TAP.2021.3083753
20. Marshall R.A., Wallace T., Turbe M. Finite-difference modeling of very-low-frequency propagation in the Earth-ionosphere waveguide. *IEEE Transactions on Antennas and Propagation*. 2017;65(12):7185–7197. DOI:10.1109/TAP.2017.2758392

Статья поступила в редакцию 28.03.2024; одобрена после рецензирования 15.05.2024; принята к публикации 24.05.2024.

The article was submitted 28.03.2024; approved after reviewing 15.05.2024; accepted for publication 24.05.2024.

Информация об авторах:

ТИПИКИН
Алексей Алексеевич

кандидат технических наук, начальник отдела Научно-исследовательского института оперативно-стратегических исследований строительства ВМФ Военного учебно-научного центра ВМФ «Военно-морская академия имени Адмирала Флота Советского Союза Н.Г. Кузнецова»

 <https://orcid.org/0000-0002-0940-4285>

ПАХОТИН
Владимир Александрович

доктор технических наук, профессор, ведущий научный сотрудник Научно-исследовательского института оперативно-стратегических исследований строительства ВМФ Военного учебно-научного центра ВМФ «Военно-морская академия имени Адмирала Флота Советского Союза Н.Г. Кузнецова»

 <https://orcid.org/0000-0002-8499-8650>

ПОТАПОВ
Денис Сергеевич

младший научный сотрудник Научно-исследовательского института оперативно-стратегических исследований строительства ВМФ Военного учебно-научного центра ВМФ «Военно-морская академия имени Адмирала Флота Советского Союза Н.Г. Кузнецова»

 <https://orcid.org/0009-0008-2289-1576>

Авторы сообщают об отсутствии конфликтов интересов.

The authors declare no conflicts of interests.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

**2.3.1 – Системный анализ,
управление и обработка
информации, статистика**

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

Научная статья

УДК 004.056

<https://doi.org/10.31854/1813-324X-2024-10-3-75-86>

Алгоритм защиты роевых робототехнических систем от атак вредоносных роботов с координированной стратегией поведения

- Игорь Алексеевич Зикратов¹, zikratov.ia@sut.ru
Татьяна Викторовна Зикратова², ztv64@mail.ru
Егор Анатольевич Новиков¹ ✉, novikov.ea@sut.ru

¹Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация

²Военно-морской политехнический институт ВУНЦ ВМФ «Военно-морская академия имени Адмирала Флота Советского Союза Н.Г. Кузнецова»
Санкт-Петербург, г. Пушкин, 196602, Российская Федерация

Аннотация

Актуальность: Атаки вредоносных роботов относятся к так называемым «мягким» атакам, использующим перехват сообщений, формирование и передачу членам роя дезинформации, а также осуществляющих иные действия, которые не имеют идентифицируемых признаков вторжения роботов-диверсантов, и приводят к принятию ошибочного, или не являющегося оптимальным консолидированного решения группой роботов. Известные методы выявления и противодействия скоординированным деструктивным информационным воздействиям в роях роботов показывают свою эффективность при концентрации вредоносных элементов в рое не более 45 %. Данная статья посвящена описанию алгоритма, который позволит расширить возможности роя противодействовать «мягким» атакам.

Постановка задачи: построение механизмов защиты мобильных мультиагентных робототехнических систем от атак со стороны вредоносных роботов с координированной стратегией поведения. **Цель работы:** повышение вероятности противодействия атакам вредоносных роботов с координированной стратегией поведения на самоорганизующиеся мультиагентные робототехнические системы. **Используемые методы:** предлагаемый алгоритм является развитием механизма самоорганизации роя роботов на основе метрик доверия и репутации для решения задачи выявления и устранения влияния вредоносных роботов. Корректность предлагаемых решений подтверждалась имитационным моделированием типовой задачи коллективного восприятия заданного полигона. **Новизна:** алгоритм основан на квантификации процесса достижения консенсуса членами гомогенной группы (роя) на последовательные такты (периоды), с последующей внутри- и межпериодной обработкой информации, продуцируемой роботами роя и вредоносными роботами в процессе информационного взаимодействия. **Результат:** эксперимент показал способность самоорганизующегося роя противодействовать координированной атаке вредоносных роботов при превышении их концентрации 51 % с вероятностью, близкой к 1. **Практическая значимость:** разработанный алгоритм может быть использован при построении систем защиты мультиагентных робототехнических систем от атак вредоносных роботов, осуществляемых в процессе информационного взаимодействия при решении роем поставленной задачи. Алгоритм позволяет успешно отражать скоординированные атаки типа атака «51 процент».

Ключевые слова: групповая робототехника, коллектив роботов, роевый интеллект, мультиагентные робототехнические системы, атака «51 процент»

Ссылка для цитирования: Зикратов И.А., Зикратова Т.В., Новиков Е.А. Алгоритм защиты роевых робототехнических систем от атак вредоносных роботов с координированной стратегией поведения // Труды учебных заведений связи. 2024. Т. 10. № 3. С. 75–86. DOI:10.31854/1813-324X-2024-10-3-75-86. EDN:XUDVOR

Original research

<https://doi.org/10.31854/1813-324X-2024-10-3-75-86>

Swarm Robotics System Algorithm for Defense Against Coordinated Behavior Strategy Attacks

✉ Igor A. Zikratov¹, zikratov.ia@sut.ru

✉ Tatyana V. Zikratova², ztv64@mail.ru

✉ Egor A. Novikov¹ ✉, novikov.ea@sut.ru

¹The Bonch-Bruевич Saint Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

²Naval polytechnic institute of Navy Development of the Military Research and Educational Center of the Navy
“Naval Academy named after Admiral of the Fleet of the Soviet Union N.G. Kuznetsov”
St. Petersburg, Pushkin, 196602, Russian Federation

Annotation

Problem statement: designing the defense mechanism against coordinated behavior strategy attacks for mobile multiagent robotic systems. Possible attacks of that kind may be carried out by use message interception, creating and transmitting disinformation, and other actions, that does not have identifiable characteristics of saboteur intrusion, and lead to making incorrect or non-optimal decision by group of robots. **The purpose of the work:** the increase of probability of detection coordinated behavior strategy attacks on mobile multiagent robotic systems. **Methods used:** proposed algorithm is further development of self organization mechanism, using trust and reputation metrics for detection and counteraction against malicious robots. Accuracy of proposed method is confirmed using imitation model of collective exploration task. **The novelty:** algorithm is based on quantification of consensus achievement process into consecutive time periods, which is followed by inter- and intraperiod processing of information, produces by robots of the swarm and by malicious robots during communication. **The result:** experiment shows that the swarm is capable to counteract against coordinated attack of malicious robots, when concentration of malicious units is more than 51 %. The probability of such counteraction is close to 1. Known detection and counteraction methods for destructive informational influence in homogeneous swarms of robots prove to be effective in cases, when concentration of malicious units is less than 45 %. **Practical significance:** developed algorithm may be used for multiagent robotic systems security system design to protect against attack, executed during interactions between agents of the swarm. Algorithm allows to successfully counteract coordinated attacks similar to «51 percent attack».

Keywords: group robotics, robot collective, swarm intelligence, multiagent robotics system, 51 percent attack

For citation: Zikratov I.A., Zikratova T.V., Novikov E.A. Swarm Robotics System Algorithm for Defense Against Coordinated Behavior Strategy Attacks. *Proceedings of Telecommunication Universities*. 2024;10(3):75–86. (in Russ.) DOI:10.31854/1813-324X-2024-10-3-75-86. EDN:XUDVOR

Введение

Стремительное развитие групповой робототехники, которое находит отражение в совершенствовании теории и практики построения интеллектуальных систем управления роботами, обусловлено очевидными преимуществами таких систем. Групповая робототехника реализует парадигму «умной пыли» (от англ. Smartdust) [1], когда группы или рои роботов (от англ. Swarm Robotics) состоят из самоорганизующихся агентов, обменивающихся сигналами по беспроводным локальным каналам связи, и работают как единая

система. Применение самоорганизующихся групп (или роев – далее эти понятия используются контекстно как синонимы) относительно простых и дешевых роботов в ряде ситуаций приводит к уменьшению размерности решаемых вычислительных задач, увеличению радиуса действия за счет рассредоточения отдельных роботов (агентов) по всей рабочей зоне, более высокой вероятности выполнения задания, обусловленной возможностью перераспределения целей (задач) между роботами группы в случае выхода из строя части из них.

Вместе с тем применение самоорганизующихся групп мобильных роботов сопровождается воздействием следующих факторов:

- фрагментарность, а порой и противоречивость знаний агентов о состоянии внешней среды и других участников;
- стохастическая природа параметров внешней среды;
- разнообразие вариантов распределения ролей агентов в коллективе и способов достижения цели, стоящей перед роем;
- отсутствие или неустойчивость единого канала связи между центром управления и роем;
- сложность обеспечения устойчивой коммуникации между агентами роя ввиду распределенной группировки в пространстве и во времени.

Очевидно, что перечисленные факторы можно расценивать как системные уязвимости, позволяющие третьим лицам осуществлять сознательное противодействие роя в процессе выполнения ими задачи путем физического внедрения в рой вредных роботов (ВР) [2]. Это обстоятельство приводит к необходимости совершенствования механизмов обеспечения информационной безопасности самоорганизующихся мультиагентных робототехнических систем.

В данной работе рассмотрены механизмы защиты роев от так называемых «мягких» атак ВР. Суть этих атак заключается в предоставлении по штатным каналам связи и протоколам, внедренными в рой ВР, недостоверной информации о своем состоянии и состоянии окружающей среды. На основе этой недостоверной информации роем может быть принято ошибочное решение, которое часто связано с выбором из некоторого числа N доступных альтернатив A_i , ($i = 1, 2, \dots, N$), или приведет к выбору способа достижения цели, отличного от оптимального. Опасность «мягких» атак на рой состоит в том, что факт проведения атаки в процессе выполнения задачи выявить затруднительно, так как роботы, их системы и каналы связи функционируют в штатном режиме, однако вероятность выбора консенсусом роботов искомой альтернативы A_{opt} снижается до неприемлемого уровня.

Угрозы безопасности гомогенных телекоммуникационных сетей и групп роботов с децентрализованным управлением от воздействия ВР обсуждались в работах [3–6]. Предлагались методы защиты, основанные на введении метрик доверия и репутации агентов [7–11] на основе технологий распределенного реестра [12, 13] путем вычисления степени уверенности [14], и другие подходы [15, 16].

При этом в литературе выделяют три типа стратегий ВР при осуществлении «мягких» атак:

- 1) случайная стратегия поведения (ССП);

- 2) оппозиционная стратегия поведения (ОСП);
- 3) координированная стратегия поведения (КСП).

Формальное описание этих стратегий подробно приведено в работе [14]. Суть ССП состоит в том, что каждый ВР на каждой итерации процедуры достижения консенсуса предлагает альтернативу A_i из множества доступных, выбранную случайным образом. ВР с ОСП предлагает любую A_i , но которая никогда не совпадает с A_{opt} . Главное отличие КСП от других стратегий ВР заключается в том, что все ВР с КСП изначально имеют глобальную предустановку, и выбор на каждой итерации процесса достижения консенсуса происходит в пользу некой альтернативы A^* всеми ВР с КСП [14]. Здесь:

$$A^* \in \{A_1, A_2, \dots, A_L\}, A_{opt} \in \{A_1, A_2, \dots, A_L\}, A^* \neq A_{opt}.$$

Указанные выше методы защиты децентрализованных самоорганизующихся групп обеспечивают эффективную защиту от ВР с ССП и ОСП. Однако эффективность защиты резко снижается в случае использования ВР с КСП при концентрации диверсантов в рое более 50 %. Это обусловлено тем, что гомогенные рои с децентрализованным управлением принимают решение о выборе альтернативы A_i путем достижения консенсуса независимых агентов, поэтому для принятия деструктивного решения, основанного на выборе альтернативы A^* , лоббируемой группой ВР, достаточно обеспечить 51 % голосов участников голосования. Подобные атаки в среде распределенных реестров, осуществляемые хакерскими группировками для захвата контроля над криптовалютами, получили название атаки «51 процент».

Целью настоящей работы является повышение степени защищенности самоорганизующихся групп роботов от атак ВР с КСП.

Проблемный сценарий коллективного принятия решения

Для того, чтобы быть эффективными, стратегии коллективного принятия решений должны быть не только быстрыми и точными, но и достаточно общими, чтобы их можно было адаптировать и повторно использовать в различных проблемных областях. В работе [17] предложен новый проблемный сценарий – коллективное восприятие, суть которого состоит в том, что роботы должны исследовать окружающую среду, оценить частоту определенных функций и коллективно определить, какая функция встречается чаще всего.

В работе [14] реализован такой сценарий коллективного восприятия в роевой робототехнической системе и проведены эксперименты с ВР со всеми рассмотренными стратегиями. В качестве

полигона использована модель внешней среды в виде сцены, раскрашенной плитками пяти цветов. На сцене иницируются роботы со случайными начальными координатами и случайными маршрутами движения. Передвигаясь по сцене, роботы выбирают для каждой клетки одну из пяти альтернатив – цвет, в который окрашена текущая клетка. Цель роя – на основе консенсуса определить, клетки какого именно цвета преобладают на сцене. Очевидно, что сложность задачи можно варьировать, изменяя соотношение между процентами плиток преобладающего цвета и других цветов. Используемая в данной статье модель сценария коллективного восприятия альтернативы также содержит сцену из клеток разных цветов (рисунок 1).

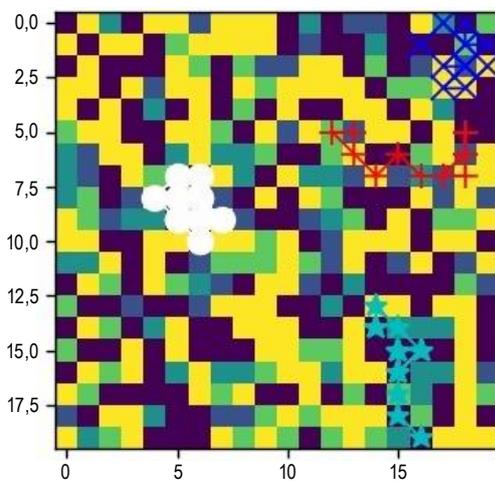


Рис. 1. Пример сцены, состоящей из 400 клеток с пятью альтернативами и маршрутами 4 роботов; 40 % клеток окрашены в желтый цвет

Fig. 1. Example of a Scene, Which Consists of 400 Cells, Each with 5 Alternative and Routes of 4 Robots; 40% of Cells are Colored Yellow

Считывание альтернатив каждым отдельно взятым роботом происходит при последовательном перемещении из расчета того, что в течение всего процесса достижения консенсуса робот подсчитывает частоту всех альтернатив на сцене (рисунок 2, блоки синим цветом). После запуска итерационного цикла j -й робот последовательно обходит клетки сцены: $r_j \in R$, где R – множество роботов группы. При достижении количества итераций j -го робота $k_{rj}^{ит}$ заданного числа K r_j вырабатывает решение в отношении альтернативы A_{ij} . Вероятность события $P(A_{ij} = A_{opt})$ зависит от количества клеток разного цвета, встретившихся роботу на пути.

Коллективное решение задачи предполагает обмен альтернативами в процессе обследования сцены [18]. В этом случае алгоритм действий робота будет иметь вид, также представленный на рисунке 2 (блоки синим + красным цветом). На каждой итерации j -й робот получает статус активного агента, перемещается на k -ю соседнюю свободную клетку, оценивает ее свойства (цвет) посредством своих

сенсоров, и выбирает для текущей клетки соответствующую альтернативу A_{ij}^k . О принятом решении он сообщает по сети связи членам коллектива, находящимся в пассивной фазе итерационного цикла: $r \in R$. В зависимости от расстояния до активного агента и внешних условий члены коллектива могут либо принять информацию от j -го робота, либо не «услышать» ее в случае неустойчивой радиосвязи. Т.е. роботы, которые приняли информацию, записывают альтернативу A_{ij}^k в соответствующую хэш-таблицу. Для каждого члена коллектива каждый агент имеет отдельную хэш-таблицу. Статус активного агента поочередно получают все роботы группы.

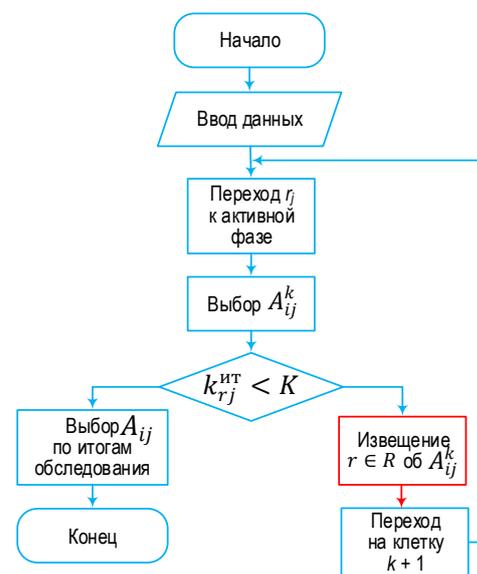


Рис. 2. Итерационный алгоритм обследования сцены одиночным роботом (блоки синим цветом) и в активной фазе итерационного цикла при коллективном принятии решения (блоки синим + красным цветом)

Fig. 2. Iterative Algorithm of Scene Exploration by Single Robot (Blue Blocks) and in Active Phase of Iterative Cycle in Case of Group Decision Making (Blue + Red Blocks)

После каждой итерации роботы на основе анализа всех хэш-таблиц оценивают частоту каждой альтернативы на исследуемой сцене и делают вывод об оптимальной альтернативе A_{opt} . Такой обмен информацией позволяет сформировать более полное представление каждого робота об окружающей среде, которое выходит за рамки исследованной области непосредственно самим роботом. Проиллюстрируем это на примере рисунка 1.

Пример 1. Анализ ситуации показывает, что робот белого цвета (далее – «белый» робот) обследовал 9 клеток, из которых 3 клетки оказались желтого цвета, 1 – зеленого, 4 – фиолетового, 1 – серого. Клетки голубого цвета роботу не встретились. Результаты сведены в таблицу 1; аналогично для «красного» и «синего» роботов.

Таким образом, первый робот выбирает альтернативу A_3 (преобладающий цвет сцены – фиолетовый). Второй робот – альтернативу A_1 или A_4 , и только третий робот – альтернативу $A_1 = A_{opt}$ (преобладающий цвет сцены – желтый). Очевидно, что в такой ситуации для достижения консенсуса в рое потребуются дополнительные итерации. Если же эти три робота будут находиться в зоне радиосвязи, тогда в результате информационного обмена у каждого сформируется итоговая таблица (см. таблицу 1).

ТАБЛИЦА 1. Результаты оценки сцены роботами: «белым» / «красным» / «синим» / группой

TABLE 1. Results of Scene Assessing by Robots: by «white» One / by «Red» One / by «Blue» One / by Group

Цвет клетки	Альтернативы	Процент
Желтый	3 / 3 / 4 / 10	33,3 / 30,0 / 40,0 / 34,5
Зеленый	1 / 1 / 1 / 3	11,1 / 10,1 / 10,0 / 10,3
Фиолетовый	4 / 2 / 3 / 9	44,4 / 20,0 / 30,0 / 31,0
Серый	1 / 3 / 1 / 5	11,1 / 30,0 / 10,0 / 17,2
Голубой	0 / 1 / 1 / 2	0,0 / 10,0 / 10,0 / 6,9
Всего	9 / 10 / 10 / 29	

Очевидно, что наличие информационного обмена приводит к увеличению вероятности выбора альтернативы $A_1 = A_{opt}$ при тех же затратах вычислительных и временных ресурсов каждого робота. Синергетический эффект усиливается при увеличении количества роботов на сцене (рисунок 3).

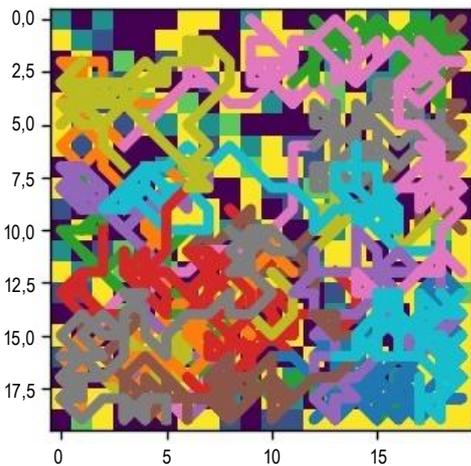


Рис. 3. Сцена, состоящая из 400 клеток с пятью альтернативами и маршруты 20 роботов после 60 итераций

Fig. 3. Scene, Which Consists of 400 Cells with 5 Alternatives and Routes for 20 Robots after 60 Iterations

Как видно на рисунке 4, при 20 роботах в рое, когда каждый отдельный робот исследовал не более 10 % сцены, за счет информационного взаимодействия в его итоговой хэш-таблице будет содержаться информация о более, чем 90 % клеток.

Ситуация меняется, если даже один из трех роботов, например «красный» (см. рисунок 1), ока-

жется вредоносным. Если он будет руководствоваться случайной стратегией поведения, то выбор альтернативы на каждой итерации будет осуществляться не сенсорными устройствами робота, а датчиком случайных чисел. При этом не исключено совпадение на k -м шаге реального цвета клетки со сгенерированным датчиком случайных чисел ВР ($A^* = A_{opt}$). Пример реализации такой атаки представлен в таблице 2. Если ВР использует ОСП, то для каждой клетки будет выполняться условие $A^* \neq A_{opt}$. В случае использования КСП, ВР на каждой итерации выбирает одну и ту же стратегию $A^* = A_2$ – якобы все обследованные «красным» роботом клетки на сцене зеленого цвета.

ТАБЛИЦА 2. Результаты совместной оценки сцены тремя роботами при 1 ВР с ССП / ОСП / КСП

TABLE 2. Results of Cooperative Assessing of Scene by three Robots in Case of 1 Malicious Robot with Random Behavior Strategy / Opposing Behavior Strategy / Coordinated Behavior Strategy

Цвет клетки	Альтернативы	Процент
Желтый	8 / 7 / 7	27,6 / 24,1 / 24,1
Зеленый	6 / 6 / 12	20,7 / 20,7 / 41,4
Фиолетовый	9 / 9 / 7	31,0 / 31,0 / 24,1
Серый	2 / 3 / 3	6,9 / 10,3 / 10,3
Голубой	4 / 4 / 1	13,8 / 13,8 / 3,4
Всего	29 / 30 / 29	

Как видно из этих тривиальных примеров, все стратегии ВР приводят к снижению вероятности выбора искомой альтернативы $P(A_1 = A_{opt})$. Причем в наибольшей степени вероятность сделать ошибочный выбор возникает при использовании ВР стратегии КСП. Очевидно, что если количество таких ВР с КСП превысит 50 % от количества роботов в рое, то $P(A_1 = A_{opt}) = 0$.

Как показано в ряде приведенных выше работ, выявление ВР с ССП и ОСП успешно решается различными методами. Например, использование метрики доверия и/или репутации позволяет выявить случаи дезинформации, продуцируемой ВР, и роботы с метрикой меньшей некоего порога исключаются из дальнейшего информационного обмена [19]. В ряде сценариев метод, основанный на расчете доверия и репутации агентов друг к другу, позволяет успешно выполнить задачу и при атаке «51 процент». К такому сценарию относится задача целераспределения [18], когда роботы, имеющие высокий уровень доверия, способны достичь поставленной цели без достижения консенсуса с агентами всего роя.

Однако для рассматриваемого сценария коллективного принятия решения атака «51 процент» является фатальной даже при наличии механизма оценки доверия и репутации. Это обусловлено тем, что оценки доверия и репутации, выставляемые агентами роя друг другу в процессе обследования

сцены, являются взаимными. Иначе говоря, если «обычные» роботы на основе проверки информации, сообщаемой ВР, выставляют им низкие значения доверия и репутации, то ВР, используя тот же самый алгоритм определения метрик доверия и репутации, будут выставлять такие же низкие оценки всем другим роботам. Тогда, при наличии большинства ВР в рою (> 50 %), в результате консенсуса будет принята альтернатива, «лоббируемая» ВР.

Во избежание такого явления возможно проведение следующих мероприятий:

1) осуществлять непрерывный контроль за количеством роботов в группе; такой способ позволит избежать атаки «51 процент», но потребует дополнительных механизмов защиты от влияния ВР – независимых систем объективного контроля, не интегрированных в рой, резервных (защищенных) каналов связи с центром управления и наличие весомого запаса дронов;

2) обеспечить наличие в рою специальных роботов, выполняющих функции полицейских участков [20].

Указанные мероприятия потребуют дополнительных материальных затрат и усложнения организационной структуры роя, и по сути, лишают его преимуществ самоорганизующейся системы. Отсюда вытекает необходимость в разработке алгоритма, который в процессе информационного взаимодействия позволит однозначно идентифицировать ВР с КСП всеми участниками процедуры достижения консенсуса.

Алгоритм действия роботов группы, находящихся в пассивной фазе итерационного цикла

Предлагаемый в данной статье алгоритм противодействия атакам ВР с КСП основан на предположении о разности статистических характеристик сигналов, продуцируемых ВР и иными агентами роя, и на свойствах объектов сцены. Для этого каждому цвету сцены необходимо присвоить определенное числовое значение, в соответствии с некоторой таблицей кодировки (таблица 3).

ТАБЛИЦА 3. Таблица кодировки альтернатив

TABLE 3. Alternative Encodings

Цвет клетки	Желтый	Зеленый	Фиолет	Серый	Голубой
Номер и обозначение альтернативы	$A_1 - '1'$	$A_2 - '2'$	$A_3 - '3'$	$A_4 - '4'$	$A_5 - '5'$

Работу алгоритма удобно пояснить на простейшем примере.

Пример 2. Рассмотрим сцену размером 10 на 10, состоящую из клеток пяти цветов, которую исследуют два робота. Тогда при движении «белого» и

«красного» робота по сцене (рисунок 4) их сообщения за пять итераций будут содержать, помимо сведений о текущем времени и номере посещаемой клетки, информацию о кодировке ее цвета в соответствии с таблицей 8:

$$C_{\text{белый}}^{\text{кортеж 1}} = \{4, 1, 5, 3, 2\},$$

$$C_{\text{красный}}^{\text{кортеж 1}} = \{1, 2, 2, 4, 1\}.$$

Средние значения $\mu(C)$ этих числовых рядов будут соответственно равны:

$$\mu(C_{\text{белый}}^{\text{кортеж 1}}) = 3 \text{ и } \mu(C_{\text{красный}}^{\text{кортеж 1}}) = 2.$$

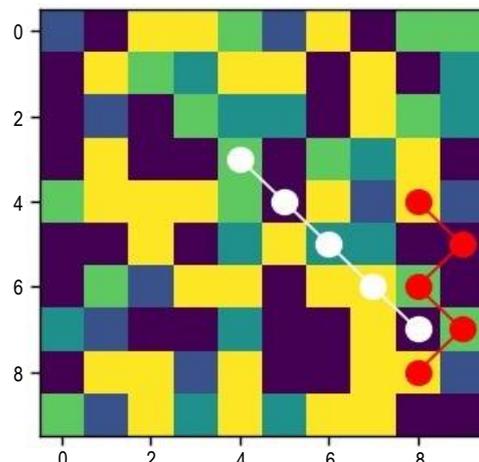


Рис. 4. Маршруты движения двух роботов по сцене 10×10 за 5 итерации

Fig. 4. Routes for 2 Robots in 5 Iterations in 10×10 Scene

Еще через пять итераций роботы проделают определенный путь (рисунок 5) и сформируют следующие кортежи:

$$C_{\text{белый}}^{\text{кортеж 2}} = \{3, 1, 3, 1, 1\}, \quad C_{\text{красный}}^{\text{кортеж 2}} = \{5, 2, 1, 3, 3\}.$$

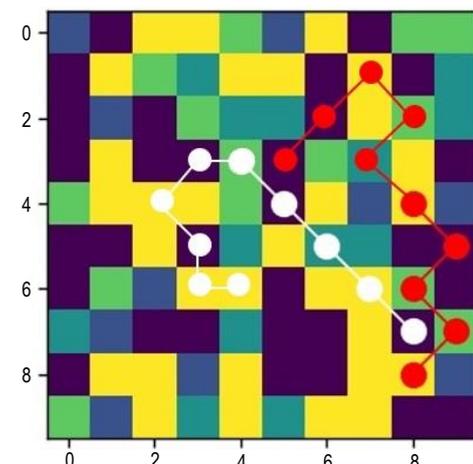


Рис. 5. Маршруты движения двух роботов по сцене 10×10 за 10 итерации

Fig. 5. Routes for Two Robots in 10 Iterations in 10×10 Scene

Средние значения $\mu(C)$ кортежей будут, соответственно, равны:

$$\mu(C_{\text{белый}}^{\text{кортеж 2}}) = 1,8 \text{ и } \mu(C_{\text{красный}}^{\text{кортеж 2}}) = 3.$$

Если предположить, что «красный» робот является ВР с КСП, который реализует предустановленную стратегию, например $A^* = '2'$, т. е. «лоббирует» преобладание клеток зеленого цвета на сцене, тогда:

$$C_{\text{красный}}^{\text{кортеж 1}} = \{2, 2, 2, 2, 2\}, C_{\text{красный}}^{\text{кортеж 2}} = \{2, 2, 2, 2, 2\} \text{ и}$$

$$\mu(C_{\text{красный}}^{\text{кортеж 1}}) = \mu(C_{\text{красный}}^{\text{кортеж 2}}) = 2.$$

Таким образом, средние значения кортежей, продуцируемых роботами за первые пять итераций обследования сцены и последующие пять итераций для ВР, не изменяются, а для всех остальных роботов – изменяются. Это обстоятельство позволяет реализовать процедуру череспериодного вычитания средних значений смежных кортежей, продуцируемых j -м роботом посредством реализации схемы, приведенной на рисунке 6.

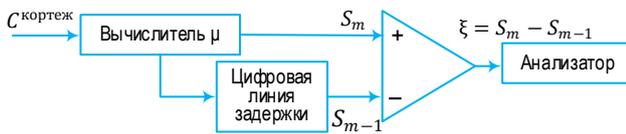


Рис. 6. Функциональная схема череспериодного вычитания
Fig. 6. Functional Diagram of Through-Period Subtraction

Здесь $S_m = \mu(C^{\text{кортеж 2}})$, $S_{m-1} = \mu(C^{\text{кортеж 1}})$. Величина ξ вычисляется как разность:

$$\xi = S_m - S_{m-1}. \tag{1}$$

Если «белый» и «красный» роботы продуцируют истинные значения кодов цветов, то, согласно приведенной схеме, для рассмотренного примера на выходе компаратора получим для «белого» робота:

$$\xi_{\text{белый}} = S_m - S_{m-1} = 3 - 1,8 = 1,2;$$

для «красного»:

$$\xi_{\text{красный}} = S_m - S_{m-1} = 2 - 3 = -1.$$

Если «красный» робот является вредоносным, то:

$$\xi_{\text{красный}} = S_m - S_{m-1} = 2 - 2 = 0.$$

Задача анализатора в этой схеме заключается в оценке полученных на выходе компаратора случайных величин ξ . В простейшем случае его роль может сводиться к правилу:

$$r_i = \begin{cases} \text{ВР,} & \text{если } \xi = 0 \\ \text{ДР,} & \text{иначе} \end{cases}, \tag{2}$$

где ДР – действующий робот группы.

Также можно использовать статистические критерии принятия решения [19].

Алгоритм, реализующий процедуру череспериодного вычитания, показан на рисунке 7.

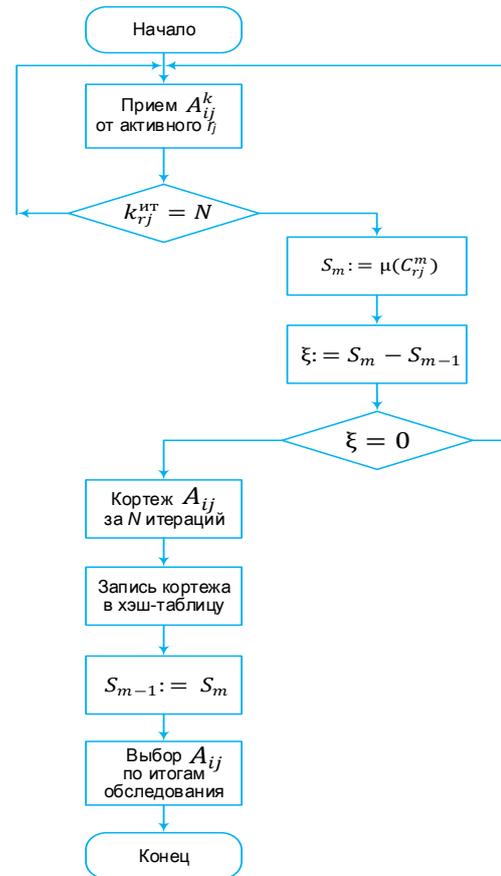


Рис. 7. Алгоритм действия робота в пассивной фазе итерационного цикла, реализующий схему череспериодной компенсации

Fig. 7. Passive Phase of Iterative Cycle Behavior Algorithm, Which Implements Through-Period Subtraction

В пассивной фазе итерационного цикла коллективного принятия решения роботы роя, получая извещения о выбранной альтернативе A_{ij}^k от агента r_j , находящегося в активной фазе (см. рисунок 3), формируют m -й кортеж кодировок альтернатив C_{rj}^m из N элементов и вычисляют S_m . Далее по формуле (1) вычисляя разность ξ , и, используя правило (2), каждый робот принимает решение, является ли r_j ВР, или нет.

В зависимости от принятого решения, данные, полученные от активного агента r_j и записанные в хэш-таблицу, либо будут учитываться роботом при выборе альтернативы, либо не будут. Следует учесть, что из-за разных условий радиосвязи информация, получаемая роботами от активного агента, может отличаться. Вследствие этого решения, принимаемые роботами, как в отношении соседних роботов, так и выбираемой ими альтернативы также могут отличаться. Так как процедура череспериодного вычитания является циклической, когда роботы постоянно проверяют корректность полученных сведений от соседей, выполняется операция запоминания на период текущего значения S_m .

Программная реализация модели роя с внедренными ВР с КСП

Для экспериментальной проверки работоспособности предложенного алгоритма разработана имитационная модель, представляющая собой программную реализацию рассмотренного проблемного сценария в среде Python с использованием объектно-ориентированного подхода. Цель эксперимента – оценить работоспособность алгоритма череспериодного вычитания при обследовании сцены из 400 клеток пяти цветов двадцатью роботами (см. рисунок 4) при наличии в рое группы ВР с КСП.

Оцениваемой величиной (показателем степени защищенности роя от атаки «51 процент») являлась вероятность $P(A_{opt})$ того, что в результате консенсуса группой роботов будет выбрана альтернатива $A_1 = A_{opt}$ – «цвет сцены желтый». Консенсус достигался простым большинством голосов «не-ВР» роботов. Варьируемыми параметрами являлись: $N_{ВР}$ – концентрация ВР с КСП в рое; D_{CB} – дальность радиосвязи между роботами; L – длина кортежа; Sc – сложность сцены.

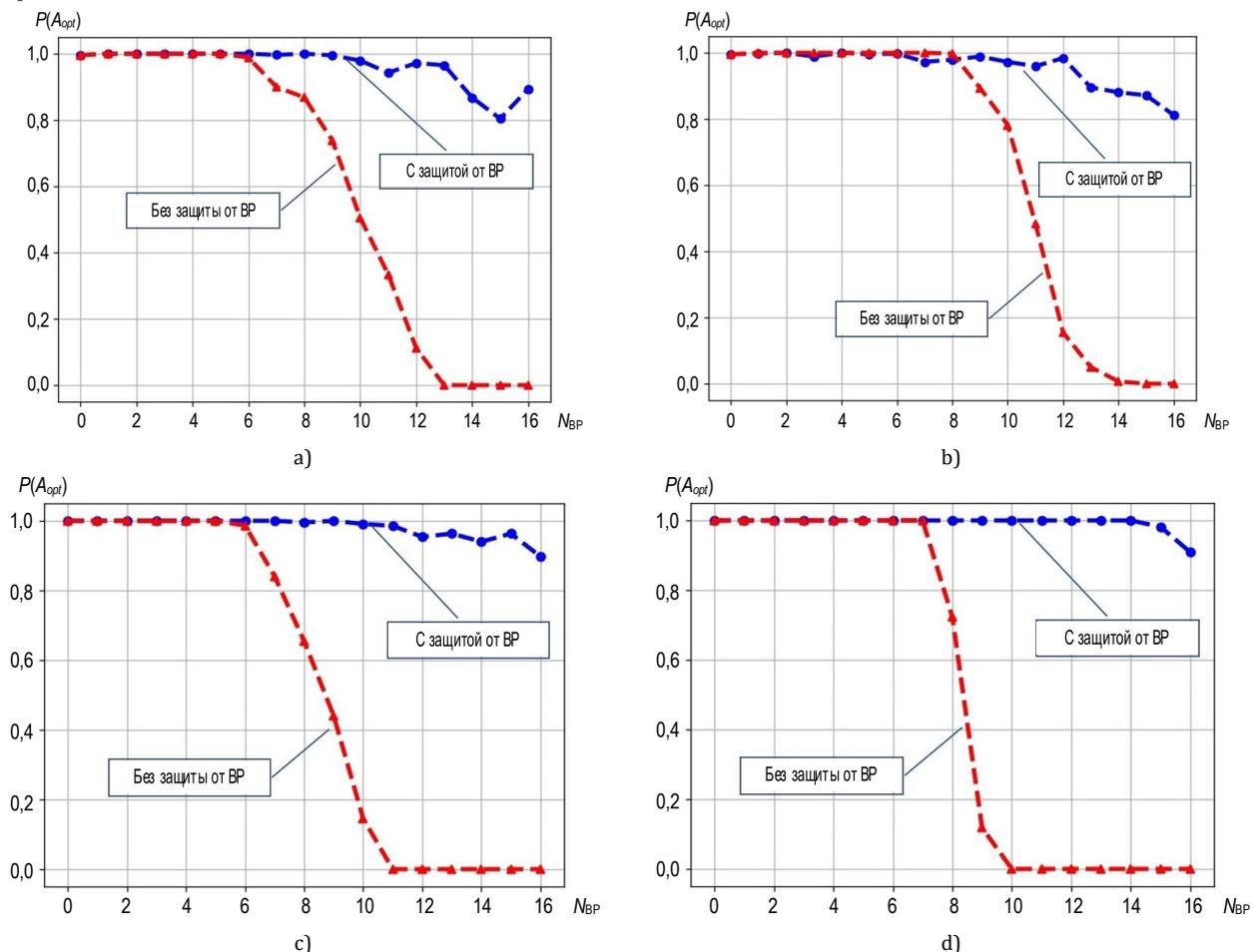


Рис. 8. Оценка алгоритма при изменении концентрации ВР в рое с использованием алгоритма череспериодного вычитания и без него: а) $D_{CB} = 6, L = 5, Sc = 40\%$; б) $D_{CB} = 6, L = 5, Sc = 60\%$; в) $D_{CB} = 6, L = 10, Sc = 40\%$; д) $D_{CB} = 11, L = 10, Sc = 60\%$

Fig. 8. Algorithm Evaluation with Variable Concentration of Malicious Robots in Swarms, Which Uses and Does Not Use Through-Period Subtraction: а) $D_{CB} = 6, L = 5, Sc = 40\%$; б) $D_{CB} = 6, L = 5, Sc = 60\%$; в) $D_{CB} = 6, L = 10, Sc = 40\%$; д) $D_{CB} = 11, L = 10, Sc = 60\%$

Под сложностью сцены понималось процентное соотношение преобладающего цвета по отношению к остальным. Рассматривались две ситуации: простая – сцена содержит 60 % клеток желтого цвета, остальные цвета распределены равномерно по оставшимся 40 % клеткам; сложная – сцена содержит 40 % клеток желтого цвета, 60 % клеток окрашены равномерно в 4 цвета.

В начале эксперимента генерировалась сцена заданной сложности со случайным расположением цветов, и роботы случайным образом размещались внутри арены. Номера ВР-роботов выбирались датчиком случайных чисел. Траектория движения каждого робота представляется ломаной линией – в своей активной фазе робот чередует движение в произвольно выбранном направлении либо вращение на месте, направление которых также выбирается случайным образом. Робот способен принимать извещения только от тех роботов, которые находятся на расстоянии, не превышающем заданную дальность радиосвязи.

Все роботы при обследовании сцены действовали по единым алгоритмам. Алгоритм, представленный на рисунке 3, использовался для роботов в активной фазе, на рисунке 7 – в пассивной. Отличие программного обеспечения ВР от «незараженных» роботов состояло в том, что все ВР в своей активной фазе выбирали единую альтернативу $A^* = A_2$ – «цвет зеленый». Для сравнения также осуществлялся расчет действий роя без использования алгоритма череспериодного вычитания.

На рисунке 8 представлены результаты экспериментов, когда расчет вероятности $P(A_{opt})$ осуществлялся при увеличении количества ВР в рое; приведены значения, усредненные по 100 сериям экспериментов. Из рисунка видно, что если роботы используют алгоритмы, не имеющие механизмов защиты от атак ВР, то для сложной сцены ($Sc = 40\%$) ВР с КСП, количество которых превышает 30% от числа роботов в группе, это приводит к резкому снижению вероятности $P(A_{opt})$ (см. ри-

сунки 8а и 8с). Достижение концентрации ВР 50% приводит к фатальным результатам – рой гарантированно не сможет определить преимущественный цвет сцены. Для простой сцены ($Sc = 60\%$) ситуация незначительно лучше.

Таким образом, в соответствии с поставленной целью, можно утверждать, что защищенность роя роботов от атаки «51 процент» с использованием алгоритма череспериодного вычитания возрастает до 80%. Если роботы используют предложенный алгоритм череспериодного вычитания, то даже при значительном преобладании ВР с КСП рой может выполнить поставленную задачу с вероятностью $P(A_i = A_{opt}) > 0,8$. Причем увеличение длины кортежа способствует большей стабильности результатов обследования сцены (см. рисунок 8d).

На рисунке 9 показана зависимость вероятности выбора верной альтернативы от дальности радиосвязи.

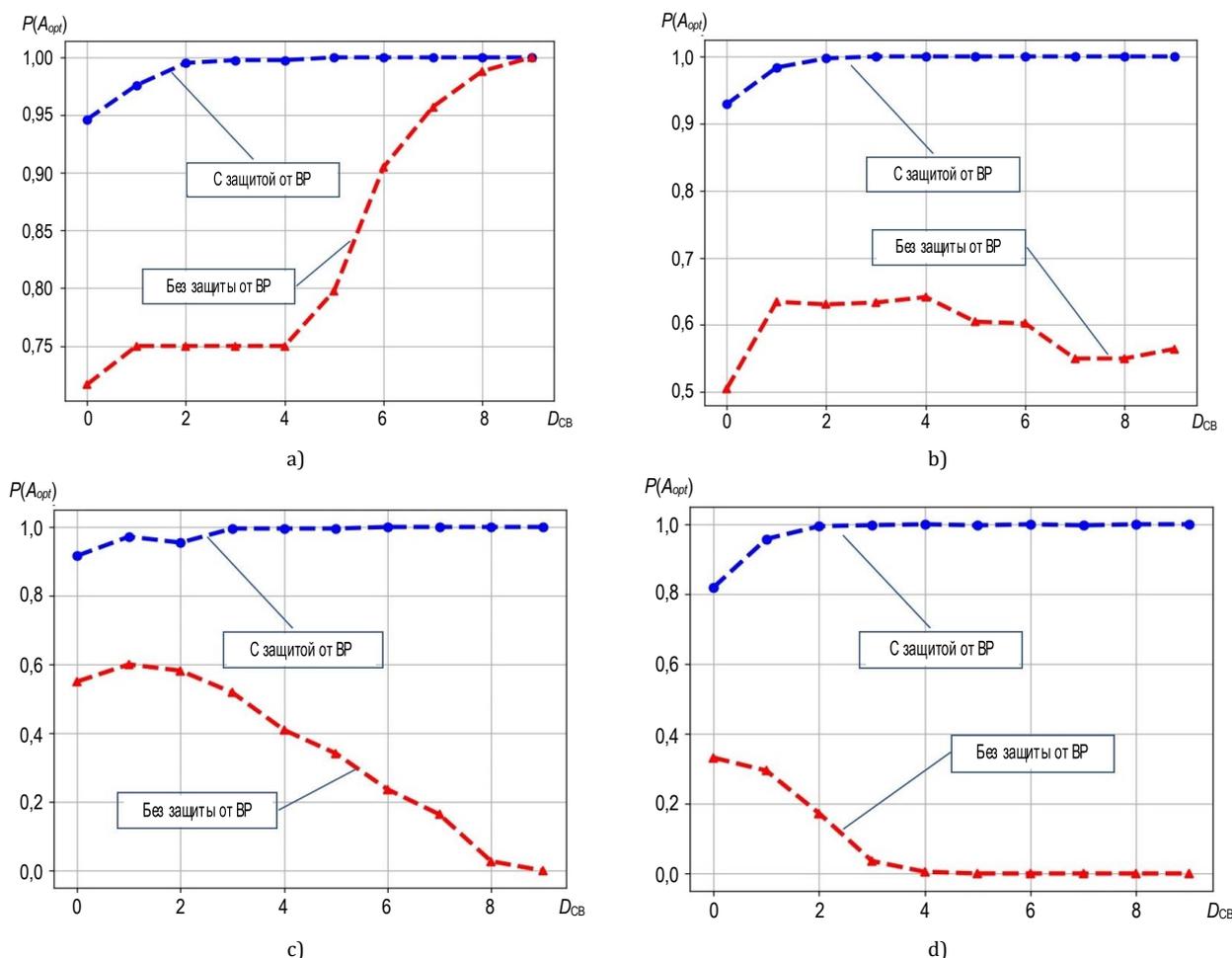


Рис. 9. Оценка алгоритма при изменении дальности радиосвязи между роботами в группе:
 а) $N_{BP} = 5, L = 10, Sc = 60\%$; б) $N_{BP} = 5, L = 10, Sc = 40\%$; в) $N_{BP} = 8, L = 10, Sc = 60\%$; д) $N_{BP} = 8, L = 10, Sc = 40\%$
 Fig. 9. Algorithm Evaluation with Variable Communication Range in Robot Group:
 а) $N_{BP} = 5, L = 10, Sc = 60\%$; б) $N_{BP} = 5, L = 10, Sc = 40\%$; в) $N_{BP} = 8, L = 10, Sc = 60\%$; д) $N_{BP} = 8, L = 10, Sc = 40\%$

При небольшом количестве ВР и простой сцене увеличение дальности радиосвязи, а значит – и количества роботов, принимающих участие в достижении консенсуса, приводит к положительным результатам даже без принятия мер противодействия ВР (см. рисунок 9а). Однако при сложной сцене или при увеличении количества ВР эффективность такого алгоритма существенно снижается (см. рисунки 9b–9d).

При использовании алгоритма череспериодной компенсации увеличение дальности радиосвязи положительно сказывается на достижении консенсуса. Очевидно, это связано с тем, что увеличение дальности радиосвязи приводит к повышению осведомленности каждого отдельного робота об исследуемой сцене.

Заключение

Предложенный алгоритм выявления ВР с КСП показал высокие результаты при использовании в рассмотренном проблемном сценарии коллективного восприятия. Роботы смогли исследовать окружающую среду, оценить частоту определенных функций и коллективно определить, какая функция встречается чаще всего даже при высокой концентрации в рое ВР. В отличие от механизмов выявления ВР, основанных на моделях доверия и/или репутации, каждый робот в группе

получает однозначно интерпретируемую оценку «полезности» своих соседей.

В отличие от известных алгоритмов, эта оценка, получаемая путем реализации эвристического алгоритма череспериодного вычитания, не требует дополнительных организационных мер, внедрения дополнительных информационных объектов и вычислительных ресурсов для контроля за ситуацией, так как алгоритм реализуется бортовыми вычислительными устройствами каждого робота.

В качестве ограничения, принятого авторами статьи, можно указать следующее. В статье не рассматривалась ситуация, когда ВР использовали бы рефлексию второго порядка, что предполагает осознанное противодействие со стороны ВР алгоритмам противодействия этим ВР роботов группы [21]. Практическая реализация рефлексии второго порядка может заключаться в том, что вредоносные роботы будут прибегать к сочетанию КСП со стратегиями ССП или ОСП. Очевидно, что это усложнит работу анализатора (см. рисунок 7), и вынудит использовать более сложные теории и представления знаний о социумах роботов [22, 23]. Однако можно утверждать, что эффективность атаки ВР при отказе от КСП также будет снижена.

Задача информационного противоборства в социуме роботов представляет все более возрастающий интерес, и может быть рассмотрена в дальнейших исследованиях авторов.

Список источников

1. Sailor M.J., Link J.R. Smart dust: nanostructured devices in a grain of sand // *Chemical Communications*. 2005. Iss. 11. P. 1375.
2. Higgins F., Tomlinson A., Martin K.M. Threats to the Swarm: Security Considerations for Swarm Robotics // *International Journal on Advances in Security*. 2009. Vol. 2. Iss. 2&3. PP. 288–297.
3. Page J., Zaslavsky A., Indrawan M. A Buddy model of security for mobile agent communities operating in pervasive scenarios // *Proceeding of the Australasian Information Security Workshop (AISW 2004), the Australasian Workshop on Data Mining and Web Intelligence (DMWI 2004), the Australasian Workshop on Software Internationalisation (AWSI 2004)*, Dunedin, New Zealand, January 2004. Sydney: Australian Computer Society, 2004. Vol. 54. PP. 17–25.
4. Schillo M., Funk P., Rovatsos M. Using trust for detecting deceitful agents in artificial societies // *Applied Artificial Intelligence*. 2000. Vol. 14. Iss. 8. PP. 825–848. DOI:10.1080/08839510050127579
5. Golbeck J., Parsia B., Hendler J. Trust Networks on the Semantic Web // *Proceeding of the 7th International Workshop on Cooperative Information Agents (CIA 2003, Helsinki, Finland, 27–29 August 2003)*. Lecture Notes in Computer Science. Berlin Heidelberg: Springer-Verlag, 2003. Vol. 2782. PP. 238–249.
6. Garcia-Morchon O., Kuptsov D., Gurtov A., Wehrle K. Cooperative security in distributed networks // *Computer Communications*. 2013. Vol. 36. Iss. 12. PP. 1284–1297. DOI:10.1016/j.comcom.2013.04.007
7. Strobel V., Castelló Ferrer E., Dorigo M. Blockchain Technology Secures Robot Swarms: A Comparison of Consensus Protocols and Their Resilience to Byzantine Robots // *Frontiers in Robotics and AI*. 2020. Vol. 7. P. 54. DOI:10.3389/frobt.2020.00054
8. Fagiolini A., Pellinacci M., Valenti G., Dini G., Bicchi A. Consensus-based Distributed Intrusion Detection for Multi-Robot Systems // *Proceeding of the International Conference on Robotics and Automation (ICRA 2008, Pasadena, USA, 19–23 May 2008)*. IEEE, 2008. DOI:10.1109/ROBOT.2008.4543196
9. Бешта А.А., Кирпо М.А. Построение модели доверия к объектам автоматизированной информационной системы для предотвращения деструктивных воздействий на систему // *Известия Томского политехнического университета*. 2013. Т. 322. № 5. С. 104–108. EDN:QOXUKV
10. Зикратов И.А., Зикратова Т.В. Использование поведенческих моделей для исследования социумов роботов // *Информация и космос*. 2022. № 4. С. 170–174. EDN:DQASLC

11. Basan A., Basan E., Makarevich O. Analysis of ways to secure group control for autonomous mobile robots // Proceedings of the 10th International Conference on Security of Information and Networks (Jaipur, India, 13–15 October 2017). New York: Association for Computing Machinery, 2017. PP. 134–139. DOI:10.1145/3136825.3136879
12. Strobel V., Castelló Ferrer E., Dorigo M. Managing Byzantine Robots via Blockchain Technology in a Swarm Robotics Collective Decision Making Scenario: Robotics track // Proceedings of the International Conference on Autonomous Agents and Multiagent Systems (IntelliSys 2016). Lecture Notes in Networks and Systems. Vol. 16. Cham: Springer, 2018. PP. 541–549.
13. Sargeant I., Tomlinson A. Review of Potential Attacks on Robotic Swarms // Proceedings of the International Conference on Autonomous Agents and Multiagent Systems (IntelliSys 2016). Lecture Notes in Networks and Systems. Vol. 16. Cham: Springer, 2018. PP. 628–646. DOI:10.1007/978-3-319-56991-8_46
14. Рябцев С.С. Метод выявления вредоносных роботов на основе данных процесса коллективного принятия решений в роевых робототехнических системах // Системы управления, связи и безопасности. 2022. № 3. С. 105–137. DOI:10.24412/2410-9916-2022-3-105-137. EDN:SVSCHG
15. Юрьева Р.А., Комаров И.И., Вискнин И.И. Иммунологические принципы принятия решения в мультиагентных робототехнических системах // Глобальный научный потенциал. 2015. № 5(50). С. 87–91. EDN:UKOVSB
16. Юрьева Р.А., Комаров И.И., Масленников О.С. Разработка метода обнаружения и идентификации скрытого деструктивного воздействия на мультиагентные робототехнические системы // Программные системы и вычислительные методы. 2016. № 4. С. 375–382. DOI:10.7256/2305-6061.2016.4.21128. EDN:XIAJDB
17. Valentini G., Brambilla D., Hamann H., Dorigo M. Collective Perception of Environmental Features in a Robot Swarm // Proceedings of the International Conference on Swarm Intelligence. Lecture Notes in Computer Science. Vol. 9882. Cham: Springer, 2016. PP. 65–76. DOI:10.1007/978-3-319-44427-7_6
18. Каляев И.А., Гайдук А.Р., Капустян С.Г. Модели и алгоритмы коллективного управления в группах роботов. М.: ФИЗМАТЛИТ, 2009. 280 с. EDN:MUWSIT
19. Зикратова Т.В. Метод группового управления в мультиагентных робототехнических системах в условиях воздействия дестабилизирующих факторов // Труды учебных заведений связи. 2021;7(3):92–100. DOI:10.31854/1813-324X-2021-7-3-92-100. EDN:JFMYBF
20. Zikratov I.A., Lebedev I.S., Gurtov A.V., Kuzmich E.V. Securing swarm intellect robots with a police office model // Proceedings of the 8th IEEE International Conference on Application of Information and Communication Technologies (AICT, Astana, Kazakhstan, 15–17 October 2014). IEEE, 2014. DOI:10.1109/ICAICT.2014.7035906
21. Лефевр В.А., Смолян Г.Л. Алгебра конфликта. М., 1968. 51 с.
22. Городецкий В.И. Поведенческие модели кибер-физических систем и групповое управление: основные понятия // Известия ЮФУ. Технические науки. 2019. № 1(203). С. 144–162. DOI:10.23683/2311-3103-2019-1-144-162. EDN:LYUZBR
23. Карпов В.Э. Социальные сообщества роботов: от реактивных к когнитивным агентам // Мягкие измерения и вычисления. 2019. № 2(15). С. 61–78. EDN:SEFEFV

References

1. Sailor M.J., Link J.R. Smart dust: nanostructured devices in a grain of sand. *Chemical Communications*. 2005;11:1375.
2. Higgins F., Tomlinson A., Martin K.M. Threats to the Swarm: Security Considerations for Swarm Robotics. *International Journal on Advances in Security*. 2009;2(2&3):288–297.
3. Page J., Zaslavsky A., Indrawan M. A Buddy model of security for mobile agent communities operating in pervasive scenarios. *Proceeding of the Australasian Information Security Workshop (AISW 2004), the Australasian Workshop on Data Mining and Web Intelligence (DMWI 2004), the Australasian Workshop on Software Internationalisation (AWSI 2004), January 2004, Dunedin, New Zealand, vol.54*. Sydney: Australian Computer Society; 2004. p.17–25.
4. Schillo M., Funk P., Rovatsos M. Using trust for detecting deceitful agents in artificial societies. *Applied Artificial Intelligence*. 2000;14(8):825–848. DOI:10.1080/08839510050127579
5. Golbeck J., Parsia B., Hendler J. Trust Networks on the Semantic Web. *Proceeding of the 7th International Workshop on Cooperative Information Agents, CIA 2003, 27–29 August 2003, Helsinki, Finland. Lecture Notes in Computer Science, vol.2782*. Berlin Heidelberg: Springer-Verlag; 2003. p.238–249.
6. Garcia-Morchon O., Kuptsov D., Gurtov A., Wehrle K. Cooperative security in distributed networks. *Computer Communications*. 2013;36(12):1284–1297. DOI:10.1016/j.comcom.2013.04.007
7. Strobel V., Castelló Ferrer E., Dorigo M. Blockchain Technology Secures Robot Swarms: A Comparison of Consensus Protocols and Their Resilience to Byzantine Robots. *Frontiers in Robotics and AI*. 2020;7:54. DOI:10.3389/frobt.2020.00054
8. Fagiolini A., Pellinacci M., Valenti G., Dini G., Bicchi A. Consensus-based Distributed Intrusion Detection for Multi-Robot Systems. *Proceeding of the International Conference on Robotics and Automation, ICRA 2008, 19–23 May 2008, Pasadena, USA*. IEEE; 2008. DOI:10.1109/ROBOT.2008.4543196
9. Beshta A.A., Kirpo M.A. Automated Information System Objects Trust Model Design For Preventing Destructive Effects On The System. *Bulletin of the Tomsk Polytechnic University*. 2013;322(5):104–108. (in Russ.) EDN:QOXUKV
10. Zikratov I., Zikratova T. Using Behavioral Models To Study Robot Societies // Information and Space. 2022;4:170–174. (in Russ.) EDN:DQASLC
11. Basan A., Basan E., Makarevich O. Analysis of ways to secure group control for autonomous mobile robots. *Proceedings of the 10th International Conference on Security of Information and Networks, 13–15 October 2017, Jaipur, India*. New York: Association for Computing Machinery; 2017. p.134–139. DOI:10.1145/3136825.3136879
12. Strobel V., Castelló Ferrer E., Dorigo M. Managing Byzantine Robots via Blockchain Technology in a Swarm Robotics Collective Decision Making Scenario: Robotics track. *Proceedings of the International Conference on Autonomous Agents and Multiagent Systems (IntelliSys 2016). Lecture Notes in Networks and Systems, vol.16*. Cham: Springer; 2018. p.541–549.

13. Sargeant I., Tomlinson A. Review of Potential Attacks on Robotic Swarms. *Proceedings of the International Conference on Autonomous Agents and Multiagent Systems (IntelliSys 2016). Lecture Notes in Networks and Systems, vol.16*. Cham: Springer; 2018. p.628–646. DOI:10.1007/978-3-319-56991-8_46.
14. Ryabtsev S.S. A method for detecting Byzantine robots based on data from the collective decision-making process in swarm robotic systems. *Systems of Control, Communication and Security*. 2022;3:105–137. (in Russ.) DOI:10.24412/2410-9916-2022-3-105-137. EDN:SVSCHG
15. Yuryeva R.A., Komarov I.I., Viksnin I.I. Immunological Principles Of Decision-Making In Multiagent Robotic Systems. *Global Scientific Potential*. 2015;5(50):87–91. (in Russ.) EDN:UKOVSB
16. Yuryeva R.A., Komarov I.I., Maslennikov O.S. Development Of A Method For Detecting And Identifying Hidden Destructive Effects On Multi-Agent Robotic Systems. *Software Systems and Computational Methods*. 2016;4:375–382. (in Russ.) DOI:10.7256/2305-6061.2016.4.21128. EDN:XIAJDB
17. Valentini G., Brambilla D., Hamann H., Dorigo M. Collective Perception of Environmental Features in a Robot Swarm. *Proceedings of the International Conference on Swarm Intelligence. Lecture Notes in Computer Science, vol.9882*. Cham: Springer; 2016. p.65–76. DOI:10.1007/978-3-319-44427-7_6
18. Kalyaev I.A., Gaiduk A.R., Kapustyan S.G. *Models and algorithms of collective control in robot groups*. Moscow: FIZMATLIT Publ.; 2009. 280 p. (in Russ.) EDN:MUWSIT
19. Zikratova T. The Method of Group Control In Multi-Agent Robotic Systems Under The Influence Of Destabilizing Factors. *Proceedings of Telecommunication Universities*. 2021;7(3):92–100. (in Russ.) DOI:10.31854/1813-324X-2021-7-3-92-100. EDN:JFMYBF
20. Zikratov I.A., Lebedev I.S., Gurtov A.V., Kuzmich E.V. Securing swarm intellect robots with a police office model. *Proceedings of the 8th IEEE International Conference on Application of Information and Communication Technologies, AICT, 15–17 October 2014, Astana, Kazakhstan*. IEEE; 2014. DOI:10.1109/ICAICT.2014.7035906
21. Lefevr V.A., Smolyan G.L. *Algebra of Conflict*. Moscow, 1968. 51 p. (in Russ.)
22. Gorodetsky V.I. Behavioral Model For Cyber-Physical System And Group Control: The Basic Concepts. *Izvestiya SFedU. Engineering Sciences*. 2019;1(203):144–162. (in Russ.) DOI:10.23683/2311-3103-2019-1-144-162. EDN:LYUZBR
23. Karpov V.E. Social communities of robots: from reactive to cognitive agents. *Soft Measurements and Computing*. 2019;2(15):61–78. (in Russ.) EDN:SEFEFV

Статья поступила в редакцию 17.04.2024; одобрена после рецензирования 14.05.2024; принята к публикации 04.06.2024.

The article was submitted 17.04.2024; approved after reviewing 14.05.2024; accepted for publication 04.06.2024.

Информация об авторах:

**ЗИКРАТОВ
Игорь Алексеевич**

доктор технических наук, профессор, профессор кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
 <https://orcid.org/0000-0001-9054-800X>

**ЗИКРАТОВА
Татьяна Викторовна**

преподаватель кафедры информационных технологий Военно-морского политехнического института ВУНЦ ВМФ «Военно-морская академия имени Адмирала Флота Советского Союза Н.Г. Кузнецова»
 <https://orcid.org/0000-0001-8365-658X>

**НОВИКОВ
Егор Анатольевич**

аспирант кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
 <https://orcid.org/0000-0003-3448-3015>

Авторы сообщают об отсутствии конфликтов интересов.

The authors declare no conflicts of interests.

Научная статья

УДК 004.654

<https://doi.org/10.31854/1813-324X-2024-10-3-87-103>

Оптимизация распределения информационных ресурсов в едином информационном пространстве

Владимир Викторович Николаев¹✉, fortune-rus@yandex.ru

Игорь Борисович Саенко^{1,2}, ibsaen@mail.ru

¹Военная академия связи им. С.М. Буденного,
Санкт-Петербург, 194064, Российская Федерация

²Санкт-Петербургский Федеральный исследовательский центр Российской академии наук,
Санкт-Петербург, 199178, Российская Федерация

Аннотация

В статье решается **проблема** оптимального распределения информационных ресурсов по узлам хранения единого информационного пространства. **Актуальность** работы обусловлена противоречиями между требуемым уровнем своевременности в едином информационном пространстве и недостаточным уровнем работки научно-методического аппарата повышения указанного свойства для аналогичных систем.

Методы исследования основаны на использовании элементов теорий массового обслуживания, марковских цепей, эволюционных вычислений, а также статистики и общенаучных методов (анализ, синтез, сравнение, дедукция).

Целью работы является повышение своевременности обработки запросов должностными лицами к единому информационному пространству с учетом выполнения требования по устойчивости и безопасности.

Результаты. Цель достигнута благодаря разработке научно-методического обеспечения: модели обмена информационными ресурсами и методики оптимизации плана их распределения, а также научно-технических предложений по реализации, разработанных модели и методики. При создании модели использован концептуальный, аналитический и имитационный подходы, которые в совокупности позволяют рассчитать показатели своевременности, устойчивости и безопасности для любого плана распределения. Методика оптимизации плана распределения информационных ресурсов позволяет сформировать оптимальный план их распределения, удовлетворяющий заданным требованиям. Использование этих научных результатов в прикладной области позволило сформулировать научно-технические предложения по реализации и применению модели и методики. В заключение приводится экспериментальная оценка предложенного подхода, доказывающая его эффективность.

Новизна. Научные результаты позволяют осуществлять оценку показателей единого информационного пространства, а также поиск оптимального плана распределения информационных ресурсов как на этапе проектирования, так и на этапе реконфигурации системы.

Теоретическая значимость работы заключается в том, что она направлена на дальнейшее развитие теории построения единого информационного пространства в части оптимизации плана распределения информационных ресурсов, а **практическая** – в разработке технико-прикладного инструментария, повышающего показатели своевременности, безопасности и устойчивости единого информационного пространства.

Ключевые слова: единое информационное пространство, информационный ресурс, имитационное моделирование, генетический алгоритм

Ссылка для цитирования: Николаев В.В., Саенко И.Б. Оптимизация распределения информационных ресурсов в едином информационном пространстве // Труды учебных заведений связи. 2024. Т. 10. № 3. С. 87–103. DOI:10.31854/1813-324X-2024-10-3-87-103. EDN:UFROMW

Original research

<https://doi.org/10.31854/1813-324X-2024-10-3-87-103>

Optimization of Information Resources Distribution in Common Information Space

Vladimir V. Nikolaev¹✉, fortune-rus@yandex.ruIgor B. Saenko^{1,2}, ibsaen@mail.ru

¹Military Academy of Communications,
St. Petersburg, 194064, Russian Federation

²Saint Petersburg Federal Research Center of the Russian Academy of Science,
St. Petersburg, 199178, Russian Federation

Annotation

The article solves the problem of optimal distribution of information resources across the storage nodes of a common information space. The **relevance** of the work is due to the contradictions between the required level of timeliness in a common information space and the insufficient level of development of a scientific and methodological apparatus for improving this property for similar systems. The research **methods** are based on the use of elements of queuing theories, Markov chains, evolutionary calculations, as well as statistics and general scientific methods (analysis, synthesis, comparison, deduction). The **purpose** of the work is to increase the timeliness of processing requests by officials to a common information space, taking into account the fulfillment of the requirements for sustainability and safety. **Results.** The goal was achieved through the development of scientific and methodological support: a model for the exchange of information resources and a methodology for optimizing the information resource allocation plan, as well as scientific and technical proposals for implementation, developed models and methods. When creating the model, conceptual, analytical and simulation approaches were used, which together make it possible to calculate indicators of timeliness, sustainability and safety for any distribution plan. The methodology for optimizing the information resource allocation plan allows you to create an optimal information resource allocation plan that meets the specified requirements. The use of these scientific results in the applied field made it possible to formulate an applied result with practical significance - scientific and technical proposals. In conclusion, an experimental assessment of the proposed approach is presented, proving its effectiveness. **Novelty.** The scientific results make it possible to evaluate the indicators of the common information space, as well as to search for an optimal plan for the distribution of information resources both at the design stage and at the stage of system reconfiguration. The **theoretical significance** of the work lies in the fact that it is aimed at further developing the theory of building a common information space in terms of optimizing the information resource allocation plan, and the **practical significance** lies in the development of technical and applied tools that improve the timeliness, security and sustainability of a common information space.

Keywords: common information space, information resource, simulation modeling, genetic algorithm

For citation: Nikolaev V.V., Saenko I.B. Optimization of Information Resources Distribution in Common Information Space. *Proceedings of Telecommunication Universities*. 2024;10(3):87–103. (in Russ.) DOI:10.31854/1813-324X-2024-10-3-87-103. EDN:UFROMW

Введение

На сегодняшний день военно-политическую обстановку вокруг Российской Федерации можно охарактеризовать как сложную, изменчивую и напряженную. Ведущие страны мира стараются оказывать давление на нашу страну во всех областях, осуществляют санкционное сдерживание и препятствуют реализации политики нашего государства. В связи с этим ключевым фактором для достижения

превосходства во всех сферах является информация, рассматриваемая, с одной стороны, как исходные данные для принятия управленческих решений, а с другой стороны – используемая для осуществления кибервоздействий на инфраструктурные объекты и систему управления организации. Система управления является важнейшим элементом поддержания организации на требуемом уровне готовности к решению задач, а ее фундаментальной составляющей

является автоматизированная система управления, которая формируется в настоящее время путем объединения существующих и разрабатываемых локальных автоматизированных систем (ЛАС) в единое информационное поле. При этом объединение ЛАС подразумевает их взаимодействие, которое возможно только при условии совместимости баз данных при их интеграции на объектах автоматизации с целью создания единого информационного пространства (ЕИП) организации.

Целью настоящей работы является разработка и экспериментальная оценка предложенного подхода к оптимизации распределения информацион-

ных ресурсов (ИР), из которых состоит ЕИП, по местам возможного хранения с учетом требований по своевременности, устойчивости и безопасности.

Классификация

Согласно концептуальным документам, в широком смысле ЕИП можно определить, как упорядоченную совокупность всей информации, имеющейся в организации, а в узком смысле – как совокупность ИР, разработанных и упорядоченных по единым правилам формирования, хранения и распространения [1, 2].

В ЕИП интегрируются различные ИР. Исходя из их многообразия, можно предложить классификацию ИР, представленную на рисунке 1.

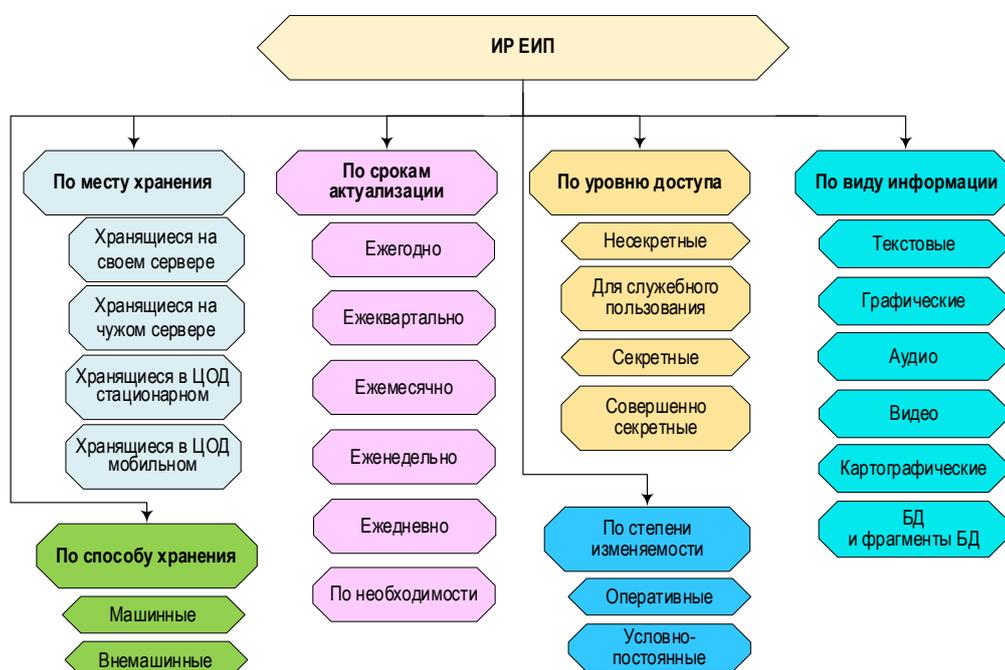


Рис. 1. Классификация ИР

Fig. 1. Information Resources Classification

Известные подходы к рациональному использованию ИР, как правило, не имеют количественного обоснования и не связаны с необходимостью удовлетворять те или иные критерии [3]. Поэтому в настоящей статье будет предложен подход к оптимальному распределению ИР в ЕИП, который направлен на удовлетворение основных требований, предъявляемых к ЕИП. К числу таких относятся требования по своевременности, устойчивости и безопасности функционирования ЕИП.

Распределение

Рассмотрим классификацию (см. рисунок 1) «по месту хранения» [4]. Она подразумевает под собой возможность совмещения двух подходов к хранению информации – централизованного и децентра-

лизованного. Сравнение этих подходов показывает, что ни один из них в отдельности не является оптимальным. Поэтому целесообразным представляется применение смешанного способа хранения ИР, вариант которого представлен на рисунке 2, где узел хранения (УХ) 1 – это стационарный центр обработки данных (ЦОД), УХ 2 – мобильный ЦОД, а остальные УХ – файловые сервера пользователей ЕИП [5].

В связи с этим важной задачей для эффективного функционирования ЕИП является оптимальное распределение ИР по УХ. Для решения данной задачи должностными лицами организации, ответственной за ведение фонда ИР, формируется план распределения ИР. Структура плана изображена на рисунке 3.

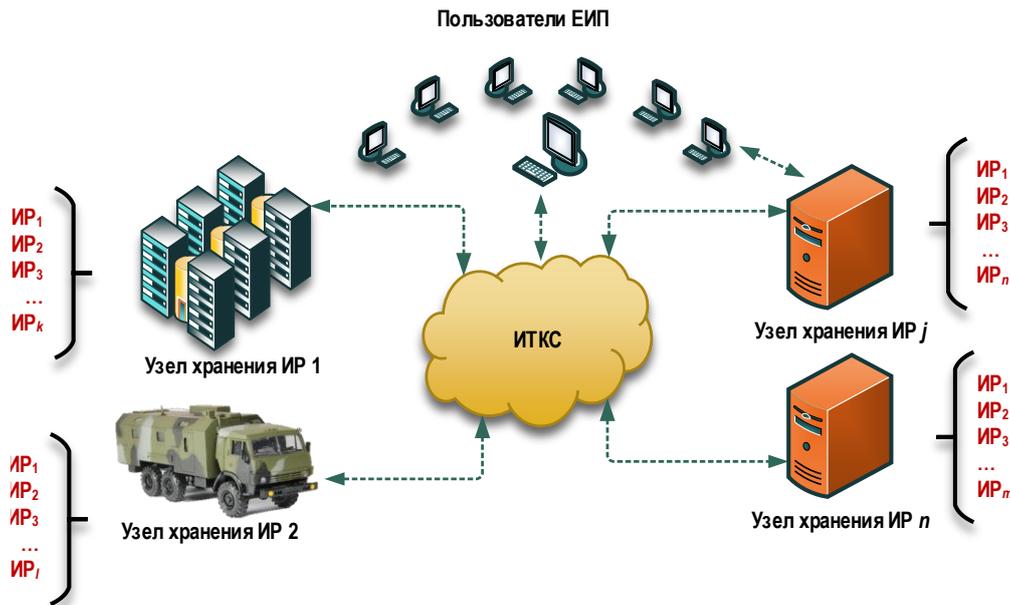


Рис. 2. Смешанный способ хранения ИР в ЕИП

Fig. 2. A Mixed Way of Storing Information Resources in a Common Information Space

	U_1	U_2	...	U_j	...	U_n
R_1	x_{11}	x_{12}	...	x_{1j}	...	x_{1n}
R_2	x_{21}	x_{22}	...	x_{2j}	...	x_{2n}
...
R_i	x_{i1}	x_{i2}	...	x_{ij}	...	x_{in}
...
R_m	x_{m1}	x_{m2}	...	x_{mj}	...	x_{mn}

R_i – i -й ИР, $i = \overline{1, m}$;
 m – множество ИР в ЕИП;
 U_j – j -й узел хранения, $j = \overline{1, n}$
 n – множество узлов хранения ИР

$x_{ij} = \begin{cases} 1, & \text{если } R_i \in U_j \\ 0, & \text{если } R_i \notin U_j \end{cases}$

Рис. 3. План распределения ИР в ЕИП

Fig. 3. Information Resources Allocation Plan in a Common Information Space

Таким образом, мы подходим к проблеме распределения ИР по УХ, а именно такого размещения, чтобы оно было оптимальным с точки зрения обеспечения показателей своевременности, устойчивости и безопасности ЕИП.

Постановка задачи

Исходные данные

Требования, предъявляемые к ЕИП по своевременности, устойчивости и безопасности:
 $G(V, H)$ – сетевая структура ЕИП;
 $U = \{u_j\}$ – множество УХ ЕИП, $j = \overline{1, n}$ (n – количество УХ в ЕИП);
 $C = \{c_{ji}\}$ – матрица коэффициентов пропускной

способности составного канала связи между узлами u_j и u_i ;

$C_{лвс}$ – пропускная способность каналов связи внутри узла;

$C_{серв}$ – скорость обработки информации в сервере;

λ – интенсивность отказа УХ;

μ – интенсивность восстановления УХ;

$P = \{p_1, p_2, p_3, \dots\}$ – вероятности несанкционированного доступа (НСД) к серверу ИР, центру обработки данных стационарному (ЦОДст) и центру обработки данных мобильному (ЦОДм);

$PR = \{PR_{li}\}$ – вероятность формирования запросов с узла U_l к ИР R_i ;

v_0 – средний объем запроса на доступ к ИР (служебного запроса сервера к другому серверу);

$R = \{r_i\}$ – множество всех ИР, $i = \overline{1, m}$ (m – количество различных ИР в ЕИП);

$V = \{v_i\}$ – множество объемов всех ИР;

$\Lambda = \{\lambda_j\}$ – множество интенсивностей запросов к ИР;

$X_d = \{x_{ij}\}$ – действующий на текущий момент план распределения ИР.

Переменные: план распределения ИР $X = \{x_{ij}\}$.

Допущения и ограничения

$\sum_{i=1}^m x_{ij} \geq 1$ – на каждом узле должен содержаться хотя бы один ИР.

$\sum_{j=1}^n x_{ij} \geq 1$ – все ИР должны быть гарантированно распределены.

Требуется разработать

1) Модель обмена ИР в ЕИП, сочетающая централизованный и децентрализованный способ их распределения, которая позволяет рассчитать показатели эффективности ЕИП.

2) Методику, учитывающую критерии по своевременности, устойчивости и безопасности, которая обеспечивает оптимальное распределение ИР по узлам ЕИП.

3) Научно-технические предложения по реализации и применению модели обмена и методики оптимизации распределения ИР в ЕИП.

Концептуальная модель обмена

Рассмотрим инфотелекоммуникационную сеть (ИТКС). ИТКС представляет собой сложную систему, соединяющую множество узлов, каждый из которых имеет локальную вычислительную сеть (ЛВС). Эти локальные сети объединяют пользователей ЕИП, предоставляя им доступ к сети и ее ресурсам через выделенные каналы связи. Узлы ИТКС могут быть расположены по-разному, образуя произвольную топологию сети, вариант которой представлен на рисунке 4. Топология может включать звездообразные, кольцевые и сетчатые

структуры, либо их комбинации. Эта гибкость позволяет сети адаптироваться к различным требованиям по масштабируемости и отказоустойчивости. В каждом узле сети организованы ЛВС, которые служат для объединения пользователей и различных устройств. ЛВС могут включать в себя не только стационарные компьютеры, но и мобильные устройства, серверы и специализированные системы, такие как ЛАС. Пользователи ЛВС получают доступ к ЕИП посредством каналов связи, которые могут быть проводными (Ethernet, оптоволокно) или беспроводными (Wi-Fi, мобильные сети). Каждый канал связи обеспечивает безопасный и надежный обмен данными между пользователями и другими узлами сети. Пользователями ЕИП могут выступать различные гетерогенные устройства, в том числе автоматизированные системы управления. ИР распределены по узлам ЕИП, что позволяет эффективнее использовать вычислительные и сетевые ресурсы [6].

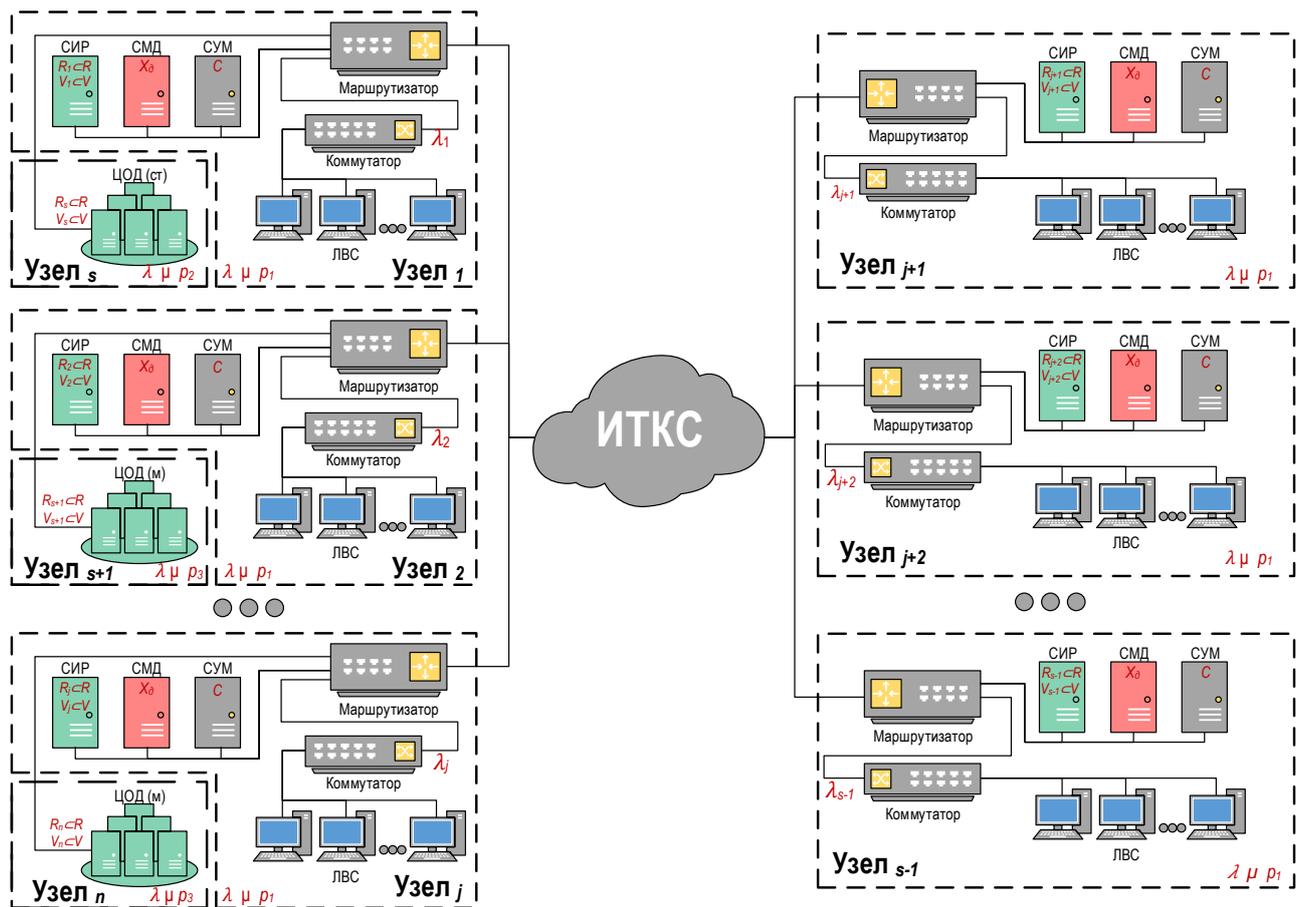


Рис. 4. Детализированная структурная модель обмена ИР в ЕИП

Fig. 4. A Detailed Structural Model for the Exchange of Information Resources in a Common Information Space

Структура узлов включает следующие компоненты: сервер ИР; сервер метаданных (СМД); сервер управления маршрутизацией (СУМ); ЦОДст или

ЦОДм. Сервер ИР осуществляет хранение ИР. СМД содержит план распределения ИР по узлам ЕИП. СУМ обеспечивает взаимодействие пользователей с ЕИП и выполняет следующие основные задачи:

- обработка входящих запросов от пользователей;
- определение узлов ЕИП, ответственных за обработку конкретных запросов пользователей;
- отправка запроса на выбранный узел;
- получение ИР от узлов в ответ на запросы пользователей;
- доставка ИР пользователю, инициировавшему запрос.

Такая архитектура позволяет эффективно управлять распределением и маршрутизацией запросов, обеспечивая оптимальное взаимодействие пользователей с ресурсами ЕИП. Каждый запрос нацелен на доступ к определенному ИР. Алгоритм прохождения пользовательского запроса представлен на рисунке 5.

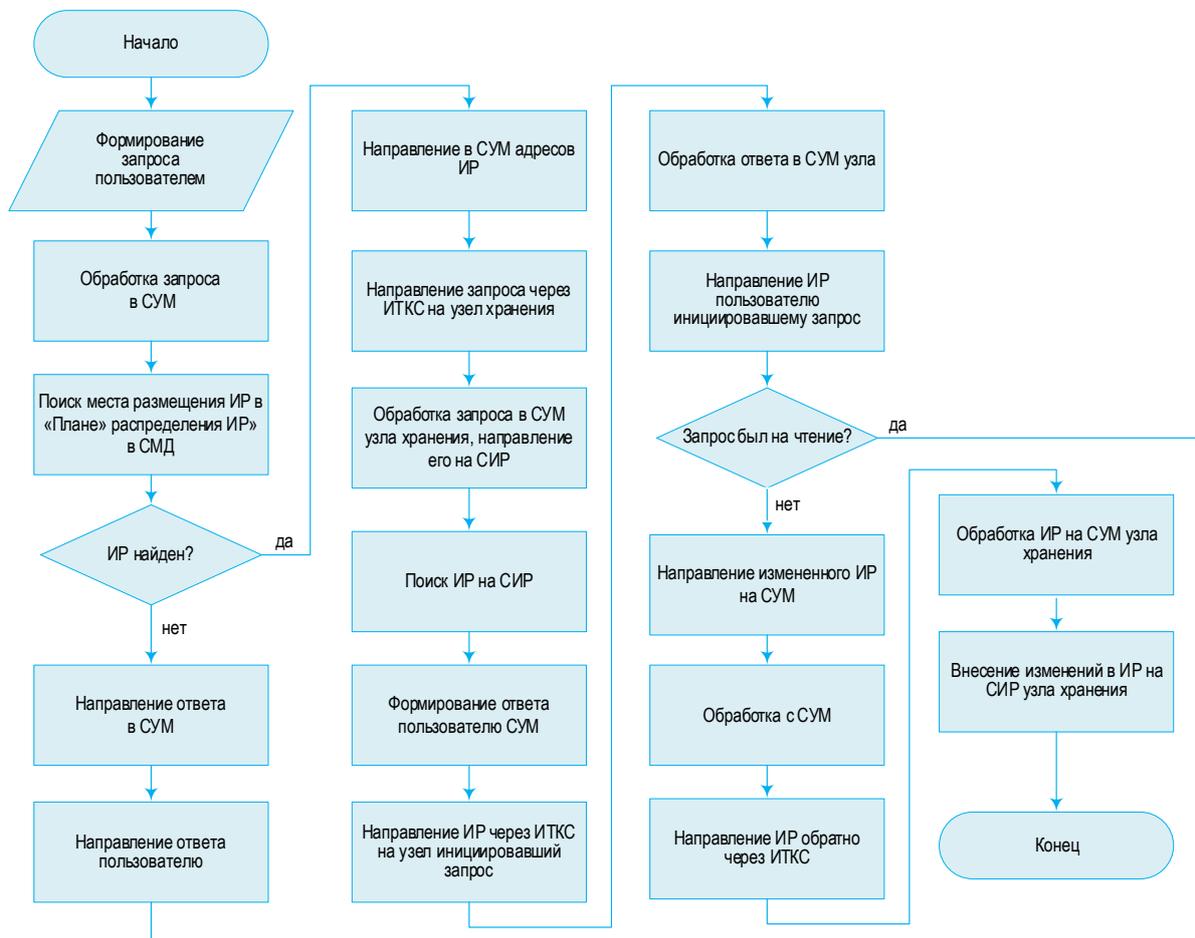


Рис. 5. Алгоритм прохождения пользовательского запроса

Fig. 5. The Algorithm for Passing a User Request

Рассмотрим СеМО, в которую поступает пуассоновский поток заявок. Это означает, что интервал времени между прибытием заявок распределен по экспоненциальному закону с плотностью вероятности $f(t) = \lambda e^{-\lambda t}$, где λ – интенсивность потока

Внесем в СеМО некоторые упрощающие допущения [7]:

1) отсутствие отказов: мы предполагаем, что ни один из компонентов системы не выходит из строя, обеспечивая стабильную и бесперебойную работу системы;

2) нет приоритезации трафика: все запросы обрабатываются в порядке их поступления, без выделения приоритетов для различных типов запросов;

3) диспетчеризация типа FIFO (аббр. от англ. First In, First Out): запросы обрабатываются по принципу очереди – первым поступил, первым обслужен;

4) отсутствие проблем столкновений и сегментации сообщений: мы учитываем, что используемые протоколы связи эффективно минимизируют вероятность возникновения коллизий и иных проблем при передаче данных.

формирование запросов пользователями в информационных системах часто соответствует пуассоновскому процессу с высокой степенью точности. Это обусловлено случайным характером поступления запросов и независимостью каждого поступления от предыдущих. Более того, пуассоновский поток заявок существенно упрощает математическое моделирование и аналитическое решение задач СМО, позволяет относительно легко вычислять такие характеристики системы, как среднее время

ожидания, среднее число заявок в системе, вероятность отказа и другие параметры эффективности [8].

Эти допущения помогут упростить нашу модель и сосредоточиться на ключевых аспектах функционирования системы без учета множества вариативных и зачастую маловероятных факторов, что позволит более четко понять структуру и работу ЕИП. Описанную модель можно представить в виде СеМО, приведенной на рисунке 6 [9].

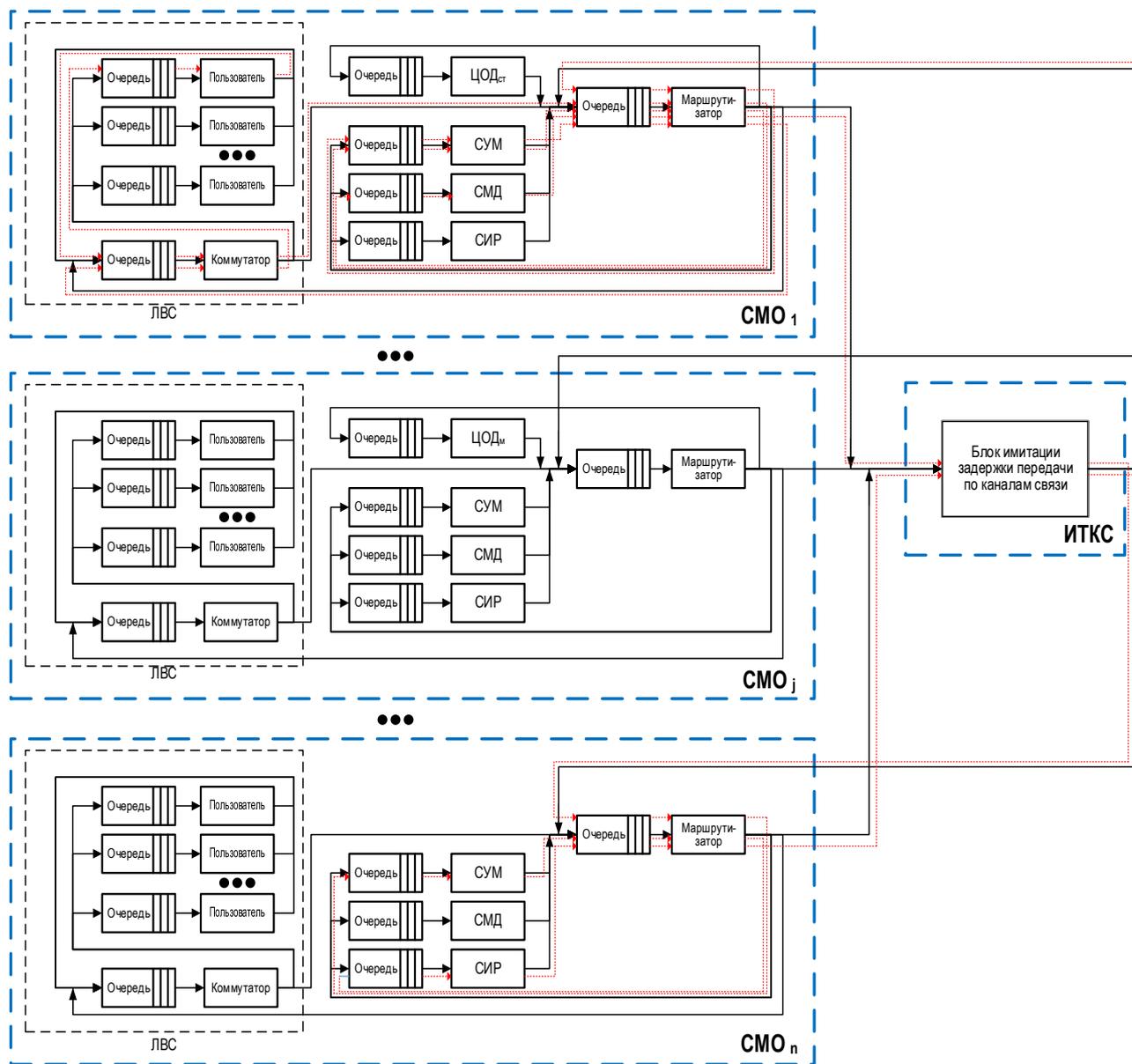


Рис. 6. Модель обмена ИР в ЕИП в терминах теории массового обслуживания

Fig. 6. A Model for the Exchange of Information Resources in a Common Information Space in Terms of Queuing Theory

Для определения времени выполнения запроса конкретного пользователя имеет смысл использовать декомпозиционный подход. Для этого вводятся следующие временные характеристики:

1) время ожидания предоставления ресурсов канала – это время, которое запрос проводит в ожидании доступа к коммуникационным ресурсам, таким как пропускная способность канала связи;

например, если канал перегружен, запрос будет ожидать свободного места для передачи данных;

2) время передачи по каналу связи запросов (квитанций) к маршрутизатору узла и обработки в нем служебной информации – включает в себя время, необходимое для передачи данных от источника к маршрутизатору через канал связи, а также время, которое маршрутизатор тратит на обработку служебной информации (например, заголовков пакетов, маршрутизацию и т. д.);

3) время ожидания запроса в буферной памяти СУМ (сервер ИР, СМД) – время, которое запрос ожидает в очереди (буфере) перед тем, как будет обработан сервером; это ожидание может быть связано с текущей загруженностью системы;

4) время обработки запроса пользователя в СУМ (сервер ИР, СМД) – время, необходимое для непосредственной обработки запроса системой. Оно включает в себя операции чтения и записи данных и т. д.

5) время передачи запроса через ИТКС – это время передачи запроса через ИТКС до конечного пункта назначения (например, сервер ИР) и обратно до пользователя; в это время также включается задержка сети (латентность) и возможные повторные передачи данных при потере пакетов.

Все эти временные составляющие суммируются для определения полного времени выполнения запроса конкретного пользователя.

Аналитическая модель обмена информационными ресурсами

Целью построения модели является определение показателей таких свойств ЕИП, как своевременность, устойчивость и безопасность. Своевременность важна, потому что пользователи должны иметь возможность получать требуемую информацию в нужный момент времени, чтобы принимать обоснованные решения и выполнять задачи. Например, в случае критически важных ситуаций своевременный доступ к информации может быть решающим фактором. Устойчивость информационного пространства гарантирует непрерывный доступ к информационным ресурсам вне зависимости от времени, внешних воздействий или технических проблем. Это важно для обеспечения бесперебойной работы систем, особенно в случае, когда доступ к информации критичен для выполнения определенных функций или процессов. Безопасность информационного пространства необходима для защиты от НСД, взломов, утечек данных и других угроз. Это особенно важно с учетом существующих киберугроз и утечек информации, которые могут нанести значительный ущерб.

Таким образом, своевременность, устойчивость и безопасность являются фундаментальными

свойствами ЕИП, необходимыми для его эффективного функционирования и обеспечения потребностей пользователей.

Остановимся более подробно на выбранных свойствах и их показателях [10–12].

Своевременность – основное свойство, показывающее способность обеспечить получение пользователем требуемого ИР по запросу в заданное время. Показателем своевременности может служить вероятность того, что среднее время реакции системы (T_p) на запросы пользователей не больше допустимого ($T_p^{доп}$).

Введенные в предыдущем разделе временные характеристики позволяют определить время TP_{lk} выполнения запроса из узла U_l на узел U_k :

$$\begin{aligned} TP_{lk} = & TOK_1^{КОМ} + TPO_1^{КОМ} + TOK_1^M + TPO_1^M + \\ & + TOP_1^{СУМ} + TOB_1^{СУМ} + TOK_2^M + TPO_2^M + TOP^{СМД} + \\ & + TOB^{СМД} + TOK_3^M + TPO_3^M + TOP_2^{СУМ} + TOB_2^{СУМ} + \\ & + TOK_4^M + TPO_4^M + TOK_1^{ИТКС} + TPO_1^{ИТКС} + \\ & + TOP_3^{СУМ} + TOB_3^{СУМ} + TOK_5^M + TPO_5^M + s_{r1} \times \\ & \times (TOP^{СИР} + TOB^{СИР}) + s_{r2} * (TOP^{ЦОД} + TOB^{ЦОД}) + \\ & + TOK_6^M + TPO_6^M + TOP_4^{СУМ} + TOB_4^{СУМ} + TOK_7^M + \\ & + TPO_7^M + TOK_2^{ИТКС} + TPO_2^{ИТКС} + TOP_5^{СУМ} + \\ & + TOB_5^{СУМ} + TOK_8^M + TPO_8^M + TOK_2^{КОМ} + TPO_2^{КОМ}, \end{aligned} \quad (1)$$

где s_{r1} и s_{r2} – элементы матрицы $s = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$; СИР – сервер ИР. Если ИР размещен на сервере ИР, то $r = 1$, если в ЦОД, то $r = 2$.

Обозначим вероятность формирования запроса с узла U_l на узел U_k как PQ_{lk} , $l = \overline{1, n}$, $k = \overline{1, n}$. Тогда время TP_l выполнения запросов с узла U_l можно определить по формуле:

$$TP_l = \sum_{k=1}^n PQ_{lk} * TP_{lk}. \quad (2)$$

Время TP реакции системы на запросы пользователей вычисляется по формуле:

$$TP = \sum_{l=1}^n \lambda_l * TP_l / \sum_{l=1}^n \lambda_l. \quad (3)$$

Для определения времени выполнения запросов с узла U_l необходимо учитывать вероятности формирования запроса с узла U_l на другие узлы:

$$PQ_{li} = \sum_{i=1}^m PR_{li} * x_{ik}, \quad (4)$$

где PR_{li} – вероятность формирования запросов с узла U_l к ИР R_i ; x_{ik} – элемент матрицы плана распределения ИР в ЕИП ($x_{ik} = 1$, если ИР R_i находится на узле U_k , иначе $x_{ik} = 0$).

Время ожидания обслуживания заявок с γ входными потоками и диспетчеризацией FIFO и при отсутствии приоритетов вычисляется по следующей формуле:

$$t_0 = \sum_{i=1}^{\gamma} \lambda_i \bar{x}_i^2 * \left(2 \left(1 - \sum_{i=1}^{\gamma} \lambda_i \omega_i \right) \right), \quad (5)$$

где λ_i – интенсивность i -го потока заявок; \bar{x}_i^2 – второй момент обслуживания заявок; ω_i – среднее время обслуживания заявок.

В нашем случае поток заявок один, поэтому приведенную формулу можно упростить до следующего вида:

$$t_0 = \frac{\lambda_i \bar{x}_i^2}{2 \left(1 - \sum_{i=1}^{\gamma} \lambda_i \omega_i \right)}. \quad (6)$$

Определим *среднее время обслуживания запросов* для нескольких случаев:

– среднее время обслуживания запросов в каналах внутри узла:

$$W_{\text{лвс}}^{\text{запр}} = \frac{v_0}{c_{\text{лвс}}}, \quad (7)$$

– среднее время обслуживания запросов на серверах (в ЦОД):

$$W_{\text{лвс}}^{\text{запр}} = \frac{v_0}{c_{\text{серв}}}, \quad (8)$$

– среднее время обслуживания запросов при передаче через ИТКС:

$$W_{\text{лвс}}^{\text{запр}} = v_0 c_{\text{лк}}, \quad (9)$$

где v_0 – средний объем запроса на доступ к ИР (служебного запроса к серверу); $c_{\text{лвс}}$ – скорость передачи информации внутри узла; $c_{\text{серв}}$ – скорость обработки информации на серверах; $c_{\text{лк}}$ – коэффициент пропускной способности составного канала при передаче информации через ИТКС.

Определим *среднее время обслуживания ИР* для нескольких случаев:

– среднее время обслуживания ИР в каналах внутри узла:

$$W_{\text{лвс}}^{\text{ИР}} = \frac{v_i}{c_{\text{лвс}}}, \quad (10)$$

– среднее время обслуживания ИР на серверах (в ЦОД):

$$W_{\text{лвс}}^{\text{ИР}} = \frac{v_i}{c_{\text{серв}}}, \quad (11)$$

– среднее время обслуживания ИР при передаче через ИТКС:

$$W_{\text{лвс}}^{\text{ИР}} = v_i c_{\text{лк}}, \quad (12)$$

где v_i – объем ИР R_i .

При экспоненциальном законе распределения вторые моменты времени обслуживания равны $\bar{x}^2 = 2\omega^2$, а при постоянном времени обслуживания $\bar{x}^2 = \omega^2$. Время передачи запроса будем считать постоянным, в то время как длительность передачи данных, возвращаемых запросом, распределено по экспоненциальному закону. Тогда выражение для расчета времени TR_{lk} выполнения запроса из узла U_i на узел U_k принимает следующий вид:

$$TR_{lk} = 6\text{ТОК}_{\text{лвс}}^{\text{запр}} + 4\text{ТОК}_{\text{лвс}}^{\text{ИР}} + \text{ТОК}_{\text{иткс}}^{\text{запр}} + \text{ТОК}_{\text{иткс}}^{\text{ИР}} + 4\text{ТОК}_{\text{серв}}^{\text{запр}} + 4\text{ТОК}_{\text{серв}}^{\text{ИР}} + 6W_{\text{лвс}}^{\text{запр}} + W_{\text{иткс}}^{\text{запр}} + 4W_{\text{лвс}}^{\text{ИР}} + W_{\text{иткс}}^{\text{ИР}} + 6W_{\text{серв}}^{\text{запр}} + 2W_{\text{серв}}^{\text{ИР}}. \quad (13)$$

Под безопасностью ЕИП понимается свойство, характеризующее его способность противостоять получению НСД к ИР. Показателем безопасности является вероятность защищенности ЕИП от НСД к ИР за заданный период времени $T_{\text{зад}}$ ($P_{\text{защ}}(T_{\text{зад}})$). Он рассчитывается по следующим формулам:

$$P_{\text{защ}} = 1 - P_{\text{НСД}}, \quad (14)$$

где $P_{\text{НСД}}$ – вероятность совершения НСД в ЕИП:

$$P_{\text{НСД}} = \min_{1 \leq i \leq n} p_i^{\text{НСД}}, \quad (15)$$

где n – количество ИР в ЕИП; $p_i^{\text{НСД}}$ – вероятность совершения НСД к i -му ИР, учитывающая наличие дубликатов ИР на других УХ:

$$p_i^{\text{НСД}} = 1 - \prod_{k \in [1, n_1]} (1 - p_{\text{сир}}^{\text{НСД}} x_{ik}) \times \prod_{k \in [n_1+1, n_1+n_2]} (1 - p_{\text{ЦОДм}}^{\text{НСД}} x_{ik}) \times \prod_{k \in [n-n_3+1, n]} (1 - p_{\text{ЦОДст}}^{\text{НСД}} x_{ik}), \quad (16)$$

где $p_{\text{сир}}^{\text{НСД}}$, $p_{\text{ЦОДм}}^{\text{НСД}}$, $p_{\text{ЦОДст}}^{\text{НСД}}$ – вероятность НСД к серверу ИР, мобильному и стационарному ЦОД, соответственно; n_1 , n_2 , n_3 – количество серверов ИР, мобильных и стационарных ЦОД, соответственно; $n = n_1 + n_2 + n_3$.

Под устойчивостью ЕИП будем понимать его способность в каждый момент времени обеспечить доступ должностного лица к требуемому ИР. Показателем этого свойства может выступать коэффициент готовности ЕИП $K_{\text{ЕИП}}^{\text{ЕИП}}$. Данный показатель является комплексным, в него закладываются как надежные характеристики оборудования УХ, так и его живучесть.

В целом, чем больше мы имеем размещенных на узлах дубликатов, тем больше вероятность того, что должностное лицо, запросившее ИР, получит его в заданный интервал времени. Такую зависимость можно описать графом возможных состояний ЕИП, представленным на рисунке 7.

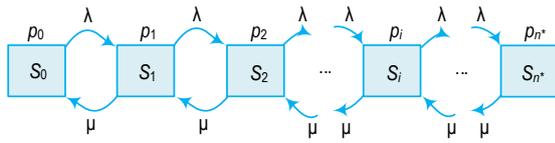


Рис. 7. Граф возможных состояний ЕИП для каждого из ИР
Fig. 7. Graph of Possible States of a Common Information Space for Each Information Resource

Состояние \$S_0\$ – когда все дубликаты ИР доступны, \$S_1\$ – когда один из дубликатов ИР недоступен, \$S_2\$ – когда два из дубликатов ИР недоступны и т. д.

Таким образом, коэффициент готовности можно определить следующими выражениями:

$$K_{r\text{ЕИП}} = \frac{\sum_{i=1}^n K_{r_i}}{n^*}, \tag{17}$$

где \$K_{r_i}\$ – коэффициент готовности для \$i\$-го ИР; \$n^*\$ – количество узлов, на которых размещен \$i\$-й ИР:

$$n^* = \sum_{k=1}^n x_{ik}. \tag{18}$$

Коэффициент готовности для \$i\$-го ИР вычисляется как сумма вероятностей всех состояний системы, кроме состояния «недоступны все узлы, хранящие ИР»:

$$K_{r_i} = \sum_{s=0}^{n^*-1} p_s. \tag{19}$$

Данные вероятности рассчитываются путем решения системы линейных уравнений, которые составляются для ЕИП, представленного в виде графа-схемы гибели-размножения:

$$\begin{cases} -\lambda p_0 + \mu p_1 = 0 \\ \lambda p_0 - (\lambda + \mu)p_1 + 2\mu p_2 = 0 \\ \dots \\ \lambda p_{s-1} - (\lambda + s\mu)p_s + (s+1)\mu p_{s+1} = 0 \\ \dots \\ \lambda p_{n^*-2} - (\lambda + (n^*-1)\mu)p_{n^*-1} + n^*\mu p_{n^*} = 0 \\ \sum_{s=0}^{n^*} p_s = 1 \end{cases} \tag{20}$$

где \$\lambda\$ – интенсивность перехода узла, хранящего ИР, из доступного состояния в недоступное; \$\mu\$ – интенсивность восстановления узла; \$p_0\$ – вероятность того, что все узлы хранящие ИР, доступны; \$p_s\$ – вероятность того, что \$s\$ узлов, хранящих ИР, недоступны; \$p_{n^*}\$ – вероятность того, что все узлы, хранящие ИР, недоступны.

Статистическая оценка адекватности модели обмена

Чтобы проверить адекватность модели обмена ИР в ЕИП, было принято решение воспользоваться

статистическими методами, а именно: построить уравнение регрессии [13] и оценить его при помощи критерия Фишера. Для этого были проанализированы результаты ряда экспериментов, проведенных на имитационной модели (выходной параметр \$y\$ – среднее время реакции системы).

Эксперименты проводились для следующей конфигурации:

- средняя интенсивность запросов в сутки: \$\lambda \in [10; 100]\$ (фактор \$z_1\$);
- количество узлов: \$n \in [10; 33]\$ (фактор \$z_2\$);
- количество информационных ресурсов: \$m \in [1000; 10000]\$ (фактор \$z_3\$);
- время моделирования: 30 суток.

Требуется определить степень влияния параметров \$z_1, z_2, z_3\$ на значение выходной переменной, для чего были поставлены эксперименты по плану полного факторного эксперимента (ПФЭ) \$2^k, k = 3\$ (таблица 1), число повторений каждого эксперимента – 3, т. е. значения выходных параметров – \$y_1, y_2, y_3\$.

ТАБЛИЦА 1. Исходная матрица планирования ПФЭ \$2^3\$
TABLE 1. The Initial Planning Matrix for a Complete Factorial Experiment

Номер опыта	Факторы			Результаты		
	\$z_1\$	\$z_2\$	\$z_3\$	\$y_1\$	\$y_2\$	\$y_3\$
1	+	+	+	14,8	16,8	12,8
2	-	+	+	17,2	14,0	15,6
3	+	-	+	24,6	18,0	18,6
4	-	-	+	11,6	11,6	11,4
5	+	+	-	37,6	34,0	30,4
6	-	+	-	16,8	16,8	12,0
7	+	-	--	23,6	14,0	18,8
8	-	-	-	21,0	15,6	16,2

- Работа выполняется по схеме:
- 1) кодируются переменные;
 - 2) достраиваются матрицы планирования в кодированных переменных с учетом парных взаимодействий и дополняются столбцом средних значений отклика;
 - 3) вычисляются коэффициенты уравнения регрессии;
 - 4) проверяются вычисленные коэффициенты на значимость, предварительно определяя дисперсию воспроизводимости, и получается уравнение регрессии в кодированных переменных;
 - 5) проверяется полученное уравнение на адекватность.

В результате было получено уравнение регрессии в кодированных переменных:

$$y = 18,49 + 3,51_{s_1} + 1,41_{s_2} - 2,91_{s_3} - 1,49_{s_{13}} - 1,79_{s_{23}} - 3,41_{s_{123}}. \tag{21}$$

Сравнивая табличное значение критерия Фишера с расчетным, был сделан вывод об адекватно-

сти уравнения регрессии, и, следовательно, об адекватности модели.

Методика оптимизации плана распределения с учетом критериев своевременности, устойчивости и безопасности

Предлагаемая методика предназначена для использования разработчиками и администраторами ЕИП на стадиях проектирования, эксплуатации и реорганизации ЕИП. Она представляет собой ин-

струмент, позволяющий на основании исходных данных оптимизировать план распределения ИР по критерию своевременности с учетом предъявляемых требований по устойчивости и безопасности ЕИП.

Методика состоит из четырех этапов. Ее общая структура представлена на рисунке 8. Ее особенность заключается в последовательном использовании генетического алгоритма [14] и имитационной модели.

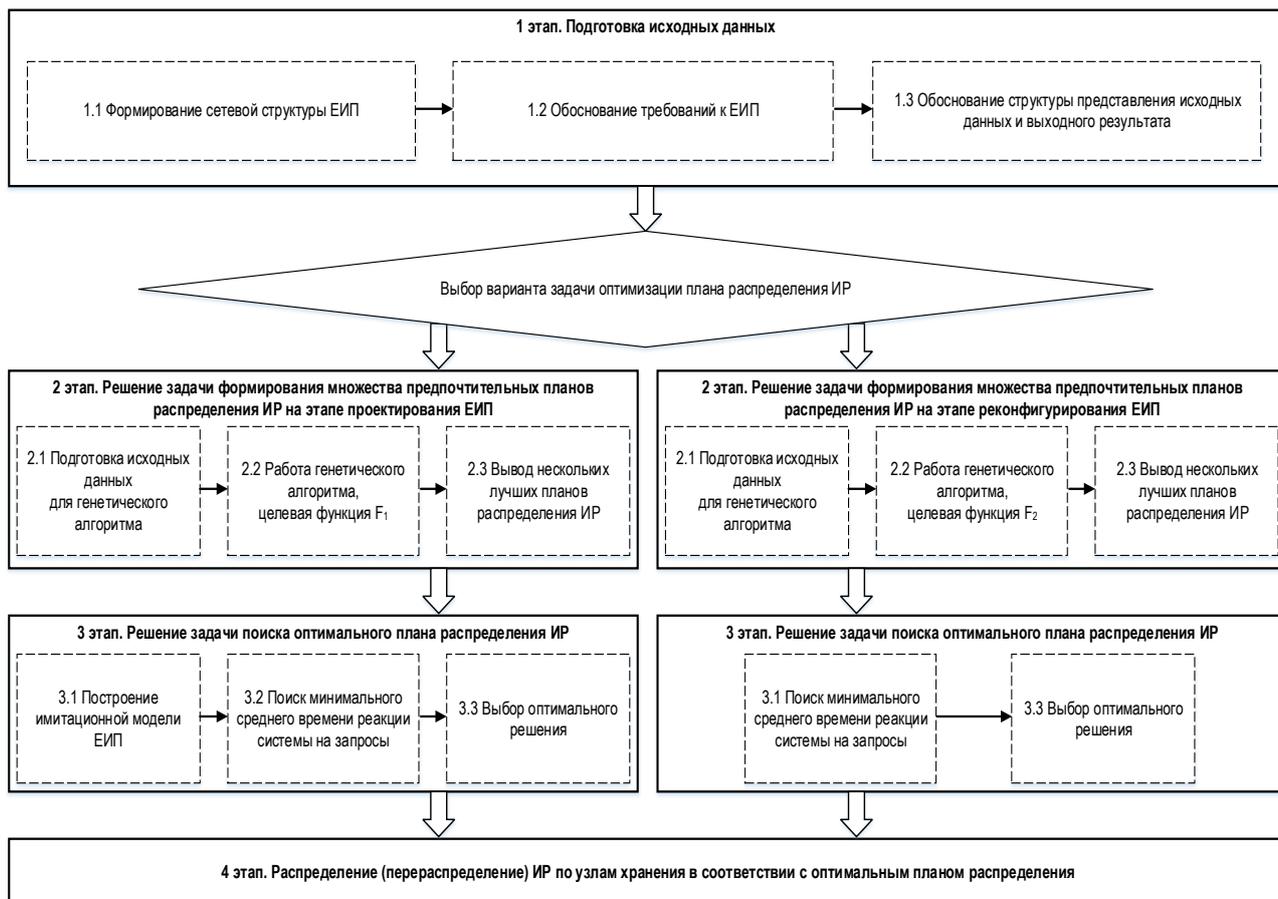


Рис. 8. Структура и взаимосвязь этапов методики оптимизации плана распределения ИР

Fig. 8. Structure and Interrelation of Methodology Stages for Optimization of the Information Resources Allocation Plan

На рисунке 9 представлена последовательность использования должностными лицами генетического алгоритма для решения задачи формирования множества предпочтительных планов распределения ИР. Новизна данного алгоритма заключается в комбинации его модификаций, таких как использование:

- многохромосомного подхода к построению особи, которой является вариант плана распределения ИР (рисунок 10);
- начального структурирования популяции с гарантированным распределением ИР по УХ;

- разбиения особей на группы с высоким значением функции пригодности с помощью алгоритма быстрой сортировки;
- адаптивной фильтрации, отсекающей особи с низким значением функции пригодности;
- универсального стохастического выбора числа точек скрещивания;
- элитизма, т. е. отбора нескольких наилучших особей в следующее поколение, минуя оператор селекции.

Задача формирования множества предпочтительных планов распределения ИР решается для двух случаев, при которых целевая функция генетического алгоритма отличается [15].

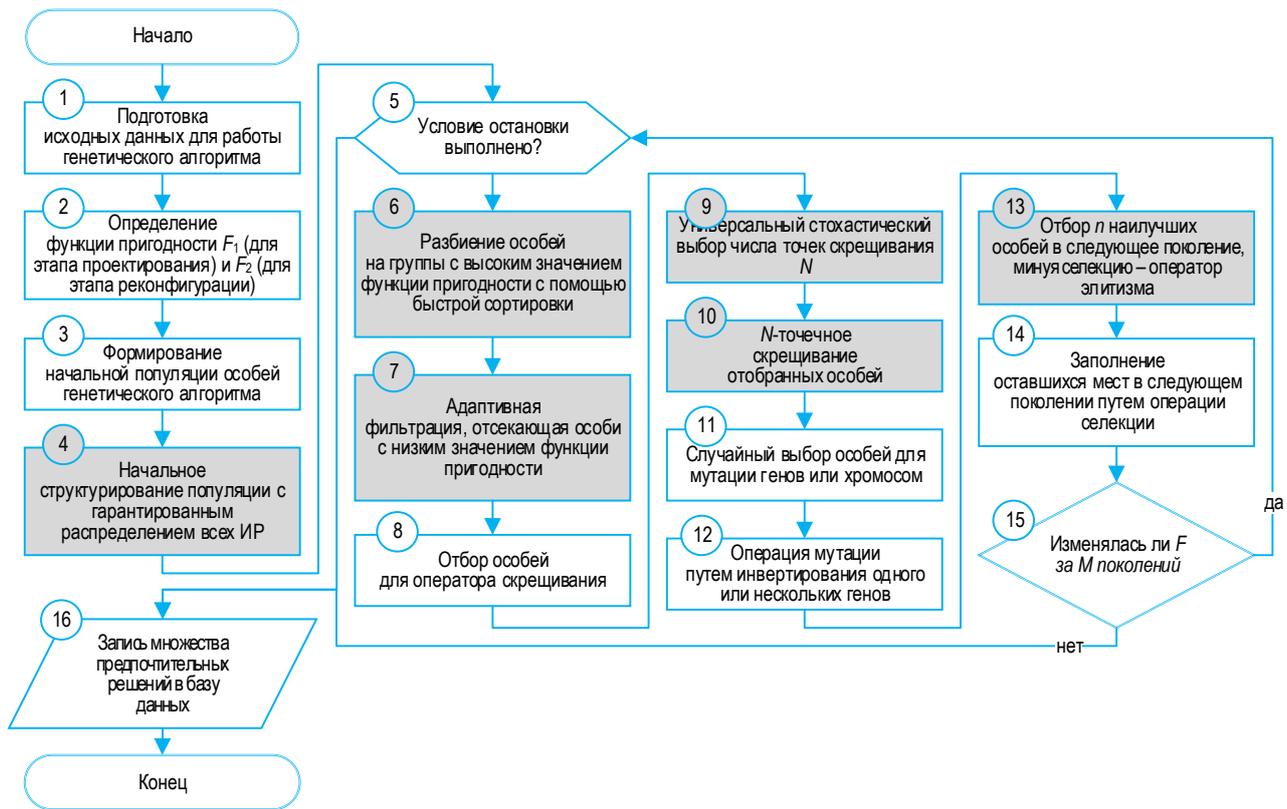


Рис. 9. Блок-схема алгоритма решения задачи формирования множества предпочтительных планов распределения ИР

Fig. 9. Block Diagram of the Algorithm for Solving the Set of Preferred Information Resources Allocation Plans Problem Forming

	U_1	U_2	...	U_j	...	U_n
R_1	0	1	...	1	...	0
R_2	1	0	...	0	...	1
...
R_i	1	1	...	0	...	1
...
R_m	1	1	...	1	...	0

– хромосома особи ГА
 – ген хромосомы

Рис. 10. Особь генетического алгоритма

Fig. 10. An Individual of the Genetic Algorithm

В первом случае (для этапа проектирования ЕИП) целевая функция принимает следующий вид:

$$F_1 = \gamma_1 f_1 + \gamma_2 f_2 + \gamma_3 f_3, \quad (22)$$

где $f_1 = f(P_{св}), f_2 = f(P_{защ}), f_3 = f(K_r)$ при условии, что $P_{св} \rightarrow \min, P_{защ} \geq P_{защ}^{треб}, K_r \geq K_r^{треб}$.

Во втором случае (для этапа реконфигурации ЕИП) целевая функция определяется выражением:

$$F_1 = \gamma_1 f_1 + \gamma_2 f_2 + \gamma_3 f_3 + \gamma_4 f_4, \quad (22)$$

где $f_1 = f(D), f_2 = f(P_{св}), f_3 = f(P_{защ}), f_4 = f(K_r)$ при условии, что $D \rightarrow \min, P_{св} \geq P_{св}^{треб}, P_{защ} \geq P_{защ}^{треб}, K_r \geq K_r^{треб}$.

В свою очередь, расстояние Хэмминга между текущим планом распределения ИР X_1 и новым X_2 рассчитывается следующим образом:

$$D(X_1, X_2) = \sum_{i=1}^m \sum_{k=1}^n |x_{ik_1} - x_{ik_2}|. \quad (24)$$

Оптимальный план распределения ИР находится на третьем этапе методики (рисунок 11) и реализуется при помощи использования имитационной модели, разработанной в среде имитационного моделирования AnyLogic.

При разработке имитационной модели [16] использован агентный подход и модульный принцип построения (рисунок 12). Как упоминалось выше, модель позволяет рассчитать показатели своевременности, безопасности и устойчивости для всех планов распределения ИР.

Запуск имитационной модели осуществлялся $N = 885104$ раз, тем самым обеспечивается требуемая точность $\epsilon = 0,01$ и достоверность $\alpha = 0,95$.

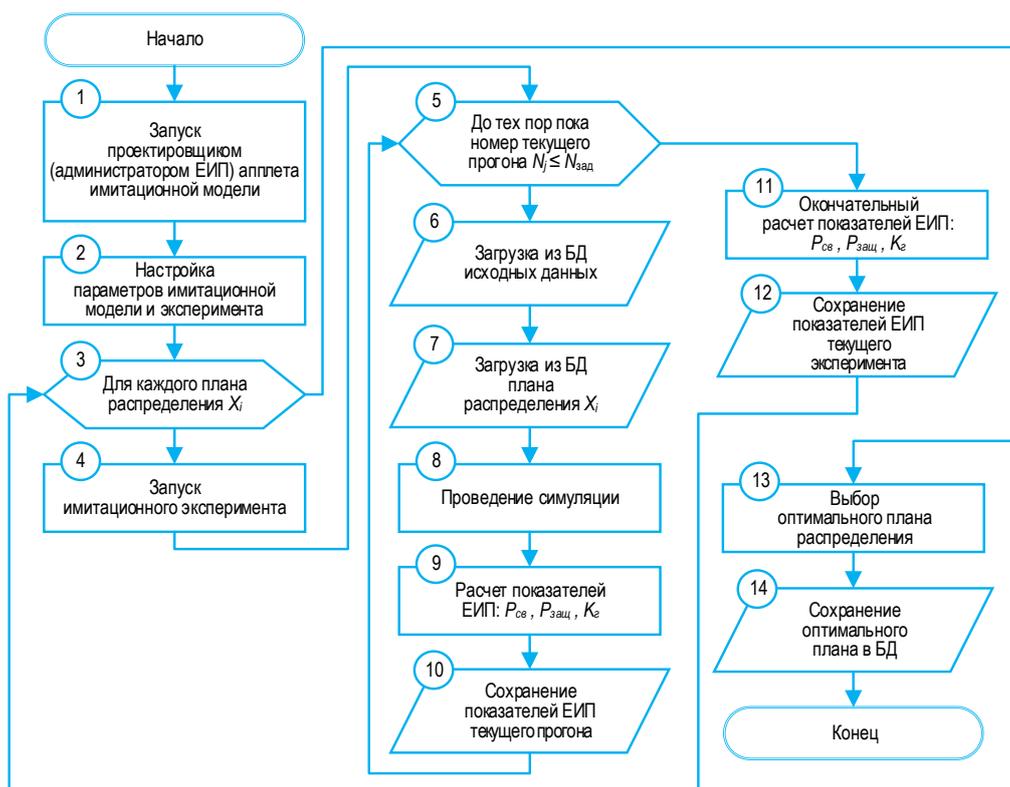


Рис. 11. Блок-схема алгоритма поиска оптимального плана распределения ИР в ЕИП

Fig. 11. Block Diagram of the Algorithm for Finding the Optimal Information Resources Allocation Plan

Количество прогонов было рассчитано по формуле [17]:

$$DN = t_{\alpha}^2 \frac{\sigma_{\alpha}^2}{\epsilon^2}, \tag{25}$$

где t_{α} – значение аргумента функции Лапласа для значения достоверности α ; σ_{α}^2 – дисперсия, рассчитанная в ходе проведения регрессионного анализа.

Предложения по построению системы планирования распределения ИР

Приведенная методика оптимизации распределения ИР в ЕИП используется для построения системы планирования распределения ИР (далее – Система). Данная система будет работать на двух этапах – на этапе проектирования ЕИП ее будут использовать разработчики и проектировщики, а на этапе реконфигурации ею будут пользоваться администраторы ЕИП. Как и любая автоматизированная система, она обладает присущими ей видами обеспечения (рисунок 13): техническим, информационным, лингвистическим, математическим, программным и кадровым [18]. Лингвистическое и кадровое обеспечение в данной статье рассматриваться не будут.

Техническое обеспечение Системы представляет собой совокупность технических средств реализации процессов преобразования информации, к ко-

торым относятся средства обработки, ввода-вывода, передачи и хранения. Остановимся более подробно на средствах обработки и хранения, так как именно они представляют особую значимость для процесса распределения ИР. Основу средств хранения составляют ЦОД и сервера, предназначенные для хранения ИР в ЕИП. Технические характеристики ЦОД и серверов хранения известны и более, чем достаточны для функционирования ЕИП. К средствам обработки относятся ПЭВМ разработчика и администратора. ПЭВМ должны отвечать современным требованиям к компьютерным системам, должны быть достаточно производительны для максимального снижения времени работы специального программного обеспечения (ПО), о котором речь пойдет далее. Варианты аппаратной конфигурации ПЭВМ разработчика и администратора представлены на рисунке 12.

Информационное обеспечение для Системы представляет собой комбинацию различных элементов, таких как описание информационных баз, системы классификации и кодирования данных, унифицированные системы документов и нормативно-справочные базы, необходимые для обеспечения ее эффективного функционирования.

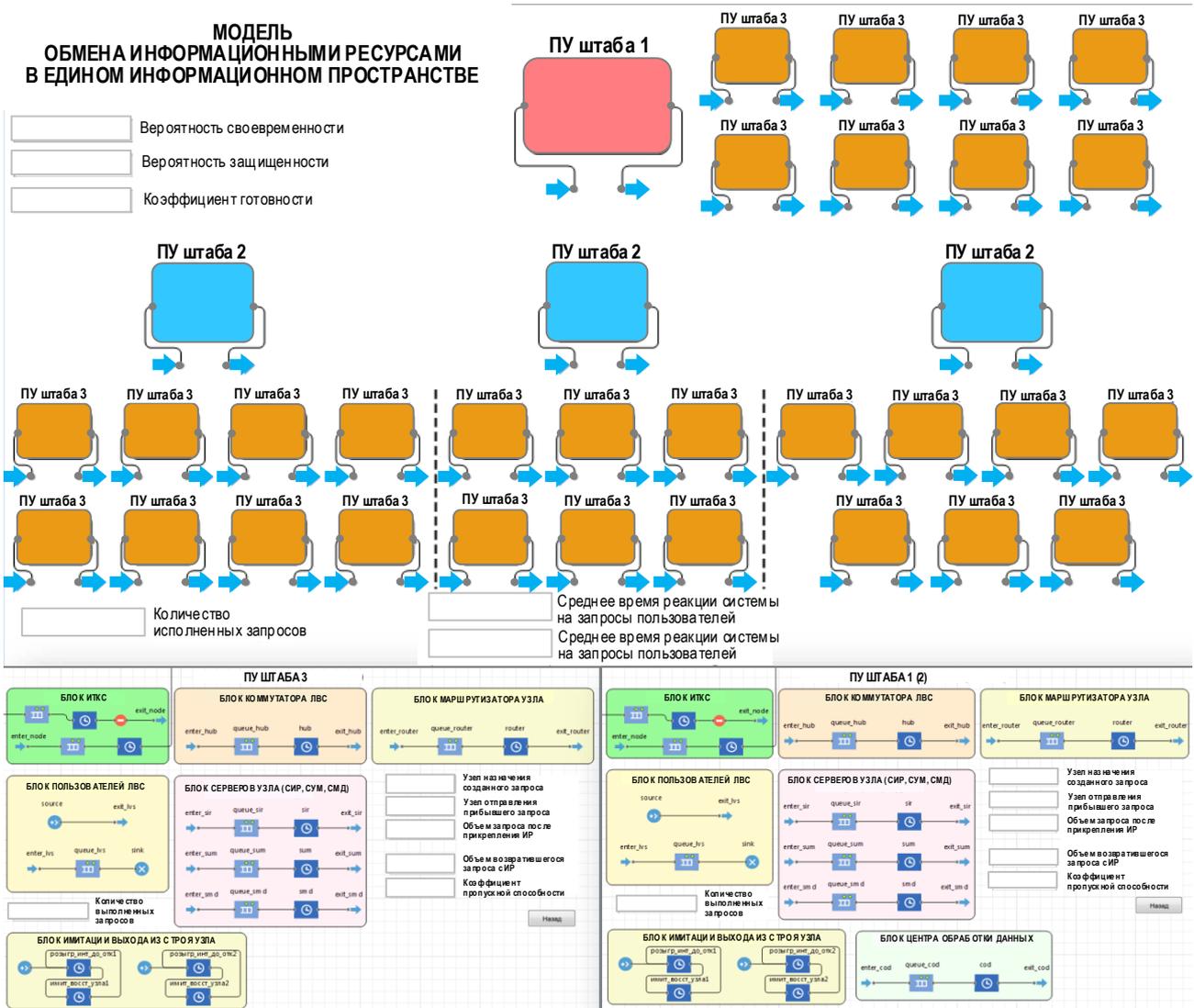


Рис. 12. Имитационная модель обмена информационными ресурсами в ЕИП
Fig. 12. Simulation Model of Information Resource Exchange in a Common Information Space

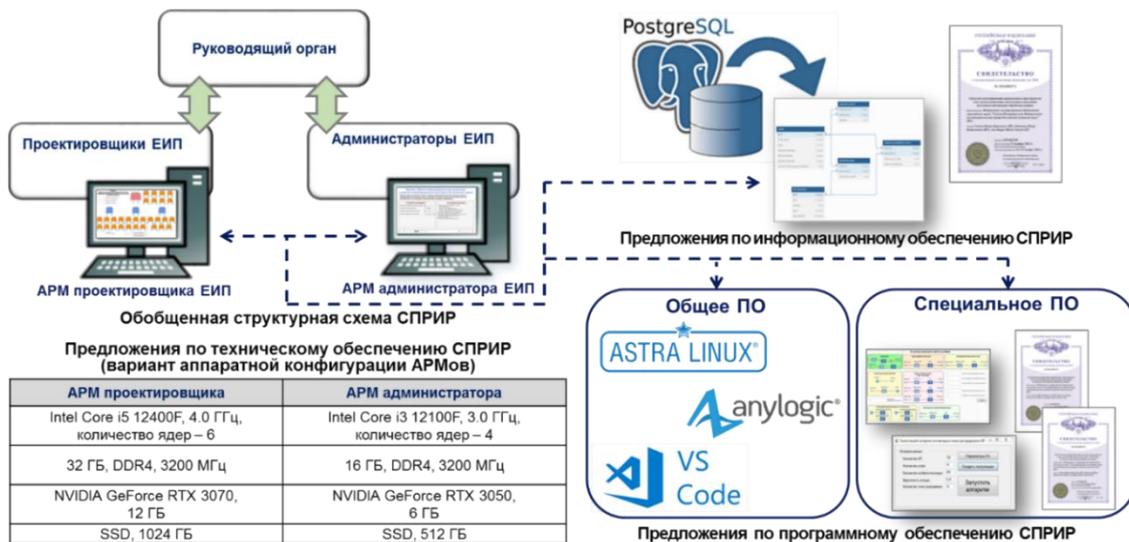


Рис. 13. Система планирования распределения ИР
Fig. 13. Information Resource Allocation Planning System

Учитывая, что персональные компьютеры, включенные в Систему, работают под управлением операционной системы AstraLinux, рекомендуется применять СУБД PostgreSQL для хранения исходных данных и выходного результата методики. Математическое обеспечение Системы включает в себя модели, методы и алгоритмы для преобразования информации, используемые в ее работе. Эти математические компоненты делятся на две категории: общее и специальное математическое обеспечение [19].

ПО Системы включает в себя набор программных продуктов и документацию, которые используются для ее отладки, тестирования и эксплуатации. В зависимости от выполняемых функций его можно разделить на две основные категории: общее и специальное [20].

Общее ПО обеспечивает базовые функции для работы системы и возможность взаимодействия с аппаратным обеспечением, предназначено для организации функционирования ЭВМ и делится на ПО ЭВМ и общесистемное ПО. К ПО ЭВМ относят операционную систему, программы технического обслуживания, сервисные программы. Основное требование – использование ПО отечественной разработки, а именно: операционной системы AstraLinux. К общесистемному ПО, помимо стандартного предустановленного ПО, следует отнести платформу для имитационного моделирования, предназначенную для разработки и использования разработанной модели обмена ИР в ЕИП. В качестве варианта – можно использовать среду имитационного моделирования AnyLogic. Также в эту группу можно отнести средства, необходимые разработчику для программирования на языке Python и библиотеки, работающие с генетическими алгоритмами, например, фреймворк DEAP.

Специальное ПО – это специализированные программные продукты, предназначенные для решения конкретных задач в рамках системы. К специальному ПО применительно к приведенным предложениям можно отнести программы решения специализированных задач, а именно: апплет имитационной модели обмена ИР в ЕИП, а также программу, реализующую методику оптимизации распределения ИР в ЕИП, реализованную на языке программирования Python и основанную на применении генетического алгоритма.

Экспериментальная оценка предложенного подхода

Чтобы оценить предложенный подход, были проведены контрольные вычислительные эксперименты для различных вариантов планов распределения ИР – централизованного, децентрализован-

ного и смешанного оптимального (таблица 2). Количество распределяемых ИР во всех случаях было равно 1000. Количество узлов ЕИП, которые являлись местами хранения ИР, было равно 23 или 37.

ТАБЛИЦА 2. Результаты контрольных замеров

TABLE 2. The Results of Control Measurements

Кол-во узлов	Варианты распределения ИР	Показатели вариантов распределения ИР		
		$P_{св}$	$P_{зщ}$	$K_{г}$
23	Централизованный	0,851	0,889	0,869
	Децентрализованный	0,880	0,893	0,914
	Смешанный (оптимальный)	0,984	0,974	0,980
37	Централизованный	0,834	0,823	0,869
	Децентрализованный	0,854	0,873	0,896
	Смешанный (оптимальный)	0,979	0,978	0,963

Из таблицы 2 видно, что смешанный оптимальный вариант распределения ИР при любых значениях количества узлов демонстрирует выполнение требований, определяющих необходимость быть больше или равным 0,9, по всем показателям – своевременности ($P_{св}$), безопасности ($P_{зщ}$) и устойчивости ($K_{г}$). В то же время для централизованного (когда все ИР хранятся в ЦОД) и децентрализованного (когда все ИР распределены по местам создания, а ЦОД – отсутствует) вариантов при любом количестве узлов эти требования практически никогда не выполняются (за исключением $K_{г}$ для децентрализованного варианта при 23 узлах).

Кроме того, видно, что с увеличением количества узлов своевременность, безопасность и устойчивость для централизованного и децентрализованного вариантов ухудшаются. В то же время для смешанных оптимальных вариантов хоть и наблюдаются небольшие уменьшения значений этих показателей, однако все они отвечают предъявляемым требованиям.

Заключение

В работе предложен подход к оптимизации плана распределения ИР в ЕИП по критериям своевременности, устойчивости и безопасности. Показано, что достичь такого оптимального распределения можно, применяя имитационную модель обмена ИР в ЕИП и методику оптимизации плана распределения ИР в ЕИП, основанную на использовании генетических алгоритмов. Кроме того, предложены решения по построению системы планирования распределения ИР в ЕИП, использование которой на этапах проектирования и реконфигурации ЕИП позволяет повысить показатели своевременности, с учетом требований по устойчивости и безопасности за счет оптимизации распределения ИР.

Список источников

1. Хахонова Н.Н. Место учета в системе единого информационного пространства организации // Финансовые исследования. 2015. № 1(46). С. 184–191. EDN:TTGAHD
2. Емельянова О.В. Структура информационно-аналитического пространства инновационной корпорации // Экономика, статистика и информатика. Вестник УМО. 2015. № 4. С. 174–178. EDN:ULFJQN
3. Саенко И.Б., Николаев В.В., Михайличенко А.В. Распределение информационных ресурсов в едином информационном пространстве, построенном с применением мобильных центров обработки данных // I научно-техническая конференция «Состояние и перспективы развития современной науки по направлению «ИТ-технологии» (Анапа, Российская Федерация, 24–25 марта 2022). Анапа: Военный инновационный технополис «ЭРА», 2022. Т. 3. С. 5–11. EDN:SZQYHX
4. Vishvanath R., Nasreen A. Survey on Recent Technology of Storage Area Network and Network Attached Storage Protocols // International journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering. 2014. Vol. 2. Iss. 8. PP. 1784–1789.
5. Куваев В.О., Ефимов В.В., Чечулин А.А., Лыжинкин К.В. Варианты построения единого информационного пространства для интеграции разнородных автоматизированных систем // Информация и космос. 2015. № 4. С. 83–87. EDN:VJFNDD
6. Николаев В.В. Модель обмена информационными ресурсами в едином информационном пространстве специального назначения // Известия Тульского государственного университета. Технические науки. 2024. № 2. С. 158–162. DOI:10.24412/2071-6168-2024-2-158-159. EDN:EXVFPV
7. Горобец В.В. Облачная модель транзакционной системы // Вестник компьютерных и информационных технологий. 2013. № 4(106). С. 19–24. EDN:PYCHUL
8. Кингман Дж. Пуассоновские процессы. М.: МЦНМО, 2007. 136 с.
9. Таха Х.А. Исследование операций. Пер. с англ. М.: Вильямс, 2016. 901 с.
10. Фабияновский И.Н. Обеспечение своевременности обмена информационными ресурсами на основе технологии распределенного реестра // Известия Тульского государственного университета. Технические науки. 2021. № 9. С. 184–194. DOI:10.24412/2071-6168-2021-9-184-194. EDN:ZLEFDL
11. ГОСТ Р 59341-2021. Системная инженерия. Защита информации в процессе управления информацией системы. М.: Стандартиформ, 2021.
12. Ревнивых А.В., Федотов А.М. Доступность ресурсов информационных систем // Вестник Новосибирского государственного университета. Серия: Информационные технологии. 2014. Т. 12. № 1. С. 55–63. EDN:SCLHLP
13. Любимова О.Н., Сиськов В.В. Построение и проверка регрессионных моделей при обработке результатов факторных экспериментов: для студентов, обучающихся по направлению «Прикладная механика». Практикум. Владивосток: Дальневост. федерал. ун-т, 2017. 36 с.
14. Simon D. Evolutionary Optimization Algorithms. John Wiley & Sons, 2013. 1002 p.
15. Богданов М.Д., Рудинский И.Д. Использование генетического алгоритма для решения задачи поиска оптимального пути // Вестник науки и образования Северо-Запада России. 2023. Т. 9. № 2. С. 76–88. EDN:UXLSLY
16. Белов А.Г., Моисеев С.А., Григорьев А.В. Методы имитационного моделирования // Труды международного симпозиума «Надежность и качество». 2014. Т. 1. С. 277–279. EDN:SPDJJF
17. Каталевский Д.Ю. Основы имитационного моделирования и системного анализа в управлении: учебное пособие. М.: Издательский дом «Дело» РАНХиГС, 2015. 496 с.
18. Куцый Н.В., Мальцев И.А., Цветков Д.Ю. Виды обеспечения автоматизированных систем управления // XI Международная научно-практическая конференция «Научный ответ на вызовы современности: технический и технологический аспекты» (октябрь, 2018). Уфа: Аэтерна, 2018. С. 9–11.
19. Легков К.Е., Емельянов А.В. Математическое обеспечение контуров автоматизированных систем управления информационными системами специального назначения при решении задач учета и мониторинга // Научные исследования в космических исследованиях земли. 2016. Т. 8. № S1. С. 37–43. EDN:YJWVUX
20. Кубасов И.А., Стрельников Ф.И. О перспективах перехода автоматизированных информационных систем на отечественное оборудование и программное обеспечение // Международная научно-практическая конференция «Стратегическое развитие системы МВД России: состояние, тенденции, перспективы» (Москва, Российская Федерация, 30 октября 2019 г.). М.: Академия управления Министерства внутренних дел Российской Федерации, 2019. С. 115–118. EDN:ZWAPMX

References

1. Khakhonova N.N. Place of accounting in the system of a single information space of an organization. *Financial Research*. 2015(46):184–191. (in Russ.) EDN:TTGAHD
2. Emelyanova O.V. The structure of the information and analytical space of the innovation corporation. *Economics, Statistics and Computer Science*. 2015;4:174–178. (in Russ.) EDN:ULFJQN
3. Saenko I.B., Nikolaev V.V., Mikhailichenko A.V. Distribution of information resources in a single information space built using mobile data processing centers. *Proceedings of the 1st Scientific and Technical Conference on State and Prospects for the Development of Modern Science in the Direction of "IT technologies", 24–25 March 2022, Anapa, Russian Federation, vol.3*. Anapa: Military Innovation Technopolis "ERA" Publ.; 2022. p.5–11. (in Russ.) EDN:SZQYHX
4. Vishvanath R, Nasreen A. Survey on Recent Technology of Storage Area Network and Network Attached Storage Protocols. *International journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering*. 2014;2(8): 1784–1789.

5. Kuvaev V.O., Efimov V.V., Chechulin A.A., Lyzhinkin K.V. Options for building a unified information space for the integration of diverse automated systems. *Information and Space*. 2015;4:83–87. (in Russ.) EDN:VJFNDD
6. Nikolaev V.V. The model of information resource exchange in a special purpose common information space. *Izvestiya Tula State University*. 2024;2:158–162. (in Russ.) DOI:10.24412/2071-6168-2024-2-158-159. EDN:EXVFPV
7. Gorobets V.V. Cloud model of on-line transaction processing system. *Herald of Computer and Information Technologies*. 2013;4(106):19–24. (in Russ.) EDN:PYCHUL
8. Kingman J. *Puassonovskie protsessy*. Translation from English. Moscow: MCN-MO Publ.; 2007. 136 p. (in Russ.)
9. Taha H.A. *Operations research: an introduction*. New Jersey: Paerson Education, 2003.
10. Fabianovski I.N. Providing timely exchange of information resources based on distributed register technology. *Izvestiya Tula State University*. 2021;9:184–194. (in Russ.) DOI:10.24412/2071-6168-2021-9-184-194. EDN:ZLEFDL
11. GOST R 59341-2021. *Systems Engineering. Protection of information in system information management process*. Moscow: Standartinform Publ.; 2021. (in Russ.)
12. Revnivykh A.V., Fedotov A.M. Availability of resources in information-processing systems. *Vestnik NSU. Series: Information Technologies*. 2014;12(1):55–63. (in Russ.) EDN:SCLHLP
13. Lyubimova O.N., Siskov V.V. *Construction and testing of regression models when processing the results of factorial experiments: for students studying in the direction of "Applied Mechanics"*. Vladivostok: Far Eastern Federal University Publ.; 2017. 36 p. (in Russ.)
14. Simon D. *Evolutionary Optimization Algorithms*. John Wiley & Sons; 2013. 1002 p.
15. Bogdanov M.D., Rudinsky I.D. Using a genetic algorithm to solve the problem of finding the optimal path. *Journal of Science and Education of North-West Russia*. 2023;9(2):76–88. (in Russ.) EDN:UXLSLY
16. Belov A.G., Moiseev S.A., Grigoriev A.V. Simulation modeling methods. *Proceedings of the International Symposium on Reliability and Quality, vol.1*. 2014. p.277–279. (in Russ.) EDN:SPDJFF
17. Katalevsky D.Yu. *Fundamentals of simulation modeling and system analysis in management*. Moscow: Delo RANKHiGS Publ.; 2015. 496 p. (in Russ.)
18. Kutsyi N.V., Maltsev I.A., Tsvetkov D.Yu. Types of support for automated control systems. *Proceedings of the XIth International Scientific and Practical Conference on Scientific Response to the Challenges of our Time: Technical and Technological Aspects, October 2018*. Ufa: Aeterna Publ.; 2018. p.9–11. (in Russ.)
19. Legkov K.E., Emelyanov A.V. Mathematical provision of automated control systems of information systems of special purpose in dealing with accounting and monitoring tasks. *H&ES Research*. 2016;8(S1):37–43. EDN:YJWVUX
20. Kubasov I.A., Strelnikov F.I. On the prospects for the transition of automated information systems to domestic equipment and software // *Proceedings of the International Scientific and Practical Conference on Strategic Development of the System of the Ministry of Internal Affairs of Russia: Status, Trends, and Prospects, 30 October 2019, Moscow, Russian Federation*. Moscow: Academy of Management of the Ministry of Internal Affairs of Russia Publ.; 2019. p.115-118. EDN:ZWAPMX

Статья поступила в редакцию 07.05.2024; одобрена после рецензирования 30.05.2024; принята к публикации 10.06.2024.

The article was submitted 07.05.2024; approved after reviewing 30.05.2024; accepted for publication 10.06.2024.

Информация об авторах:

НИКОЛАЕВ
Владимир Викторович

адъюнкт кафедры автоматизированных систем специального назначения
Военной академии связи имени Маршала Советского Союза С.М. Буденного
 <https://orcid.org/0009-0002-0823-6299>

САЕНКО
Игорь Борисович

доктор технических наук, профессор, профессор кафедры автоматизированных систем специального назначения Военной академии связи имени Маршала Советского Союза С.М. Буденного, главный научный сотрудник Санкт-Петербургского Федерального исследовательского центра Российской академии наук
 <https://orcid.org/0000-0002-9051-5272>

Авторы сообщают об отсутствии конфликтов интересов.

The authors declare no conflicts of interests.

Научная статья

УДК 519.61+539.1

<https://doi.org/10.31854/1813-324X-2024-10-3-104-115>

Оценка характеристик мультифрактального спектра фрактальной размерности сетевого трафика и компьютерных атак в IoT

- Олег Иванович Шелухин, sheluhin@mail.ru
- Сергей Юрьевич Рыбаков ✉, svolkov97@gmail.com
- Анна Вячеславовна Ванюшина, a.v.vaniushina@mtuci.ru

Московский технический университет связи и информатики,
Москва, 111024, Российская Федерация

Аннотация

Актуальность. Изменение фрактальной размерности сетевого трафика может служить индикатором атак или аномальной активности. Фрактальный анализ позволяет выявлять изменения временной структуры трафика и сигнализировать о возможных угрозах. Наблюдаемое в широких временных масштабах самоподобие указывает на мультифрактальную природу аномалий, что требует дальнейшего изучения. Таким образом, разработка методов для обнаружения и классификации кибератак с использованием мультифрактального анализа является актуальной задачей для повышения информационной безопасности.

Цель работы. Повышение эффективности обнаружения и классификации компьютерных атак в сетях IoT методами машинного обучения за счет расширения количества атрибутов, характеризующих параметры мультифрактального спектра фрактальной размерности.

Методы исследования: дискретный вейвлет анализ, мультифрактальный анализ, машинное обучение, программная реализация комбинированного метода многоклассовой классификации в совокупности с методами фрактального анализа.

Результаты. Разработана методология оценки характеристик мультифрактального спектра фрактальной размерности трафика с помощью последовательности текущих оценок фрактальной размерности в окне анализа фиксированной длины в зависимости от интервала разрешения (времени дискретизации). Приведены аналитические результаты экспериментальных оценок мультифрактального анализа обрабатываемых процессов в сетях IoT. Оценена информационная значимость дополнительных атрибутов компьютерных атак и нормального трафика для случая бинарной и многоклассовой классификации по индексу Джини для двух случаев: без добавления мультифрактального спектра фрактальной размерности и с добавлением мультифрактального спектра фрактальной размерности. Показано, что основная концентрация наиболее значимых атрибутов приходится на интервал дискретизации 500 мс...1,5 с

Новизна. Введено понятие мультифрактального спектра фрактальной размерности в виде последовательности текущих оценок фрактальной размерности в окне анализа фиксированной длины в зависимости от интервала разрешения.

Практическая значимость. Представленный метод оценки параметров мультифрактального спектра фрактальной размерности является универсальным и может быть применен в различных информационных системах.

Ключевые слова: фрактальная размерность, мультифрактальный анализ, алгоритмы, информационная значимость, компьютерные атаки, статистические характеристики, метрики

Ссылка для цитирования: Шелухин О.И., Рыбаков С.Ю., Ванюшина А.В. Оценка характеристик мультифрактального спектра фрактальной размерности сетевого трафика и компьютерных атак в IoT // Труды учебных заведений связи. 2024. Т. 10. № 3. С. 104–115. DOI:10.31854/1813-324X-2024-10-3-104-115. EDN:KIRCNK

Original research

<https://doi.org/10.31854/1813-324X-2024-10-3-104-115>

Estimation of the Multifractal Spectrum Characteristics of Fractal Dimension of Network Traffic and Computer Attacks in IoT

✉ **Oleg I. Sheluhin**, sheluhin@mail.ru
✉ **Sergey Y. Rybakov** ✉, svolkov97@gmail.com
✉ **Anna V. Vanyushina**, a.v.vaniushina@mtuci.ru

Moscow Technical University of Communications and Informatics,
Moscow, 111024, Russian Federation

Annotation

Relevance. Changes in the fractal dimension of network traffic can serve as an indicator of attacks or anomalous activity. Fractal analysis allows to identify changes in the temporal structure of traffic and signal possible threats. The self-similarity observed over wide time scales indicates the multifractal nature of the anomalies, which requires further study. Thus, the development of methods for detecting and classifying cyber attacks using multifractal analysis is an urgent task to improve information security.

The aim of the article. Increasing the efficiency of detection and classification of computer attacks in IoT networks using machine learning methods by expanding the number of attributes characterizing the parameters of the multifractal spectrum of fractal dimension.

Research methods: discrete wavelet analysis, multifractal analysis, machine learning, software implementation of a combined multiclass classification method in conjunction with fractal analysis methods.

Results. A methodology has been developed for assessing the characteristics of the multifractal spectrum of the fractal dimension of traffic using a sequence of current estimates of the fractal dimension in an analysis window of a fixed length depending on the resolution interval (sampling time). The analytical results of experimental assessments of multifractal analysis of processed processes in IoT networks are presented. The informational significance of additional attributes of computer attacks and normal traffic is assessed for the case of binary and multi-class classification using the Gini index for two cases: without adding a multifractal spectrum of fractal dimension and with the addition of a multifractal spectrum of fractal dimension. It has been shown that the main concentration of the most significant attributes falls on the sampling interval of 500 ms...1.5 s.

Novelty. The concept of a multifractal spectrum of fractal dimension is introduced in the form of a sequence of current estimates of the fractal dimension in an analysis window of a fixed length depending on the resolution interval.

Practical significance. The presented method for estimating the parameters of a multifractal spectrum of fractal dimension is universal and can be applied in various information systems.

Keywords: *fractal dimension, multifractal analysis, algorithms, information significance, computer attacks, statistical characteristics, metrics*

For citation: Sheluhin O.I., Rybakov S.Y., Vanyushina A.V. Estimation of the Multifractal Spectrum Characteristics of Fractal Dimension of Network Traffic and Computer Attacks in IoT. *Proceedings of Telecommunication Universities*. 2024;10(3):104–115. (in Russ.) DOI:10.31854/1813-324X-2024-10-3-104-115. EDN:KIRCNK

Постановка задачи

Многочисленные исследования статистических характеристик сетевого трафика, сетевых аномалий и компьютерных атак (КА) показывают нали-

чие у них свойств фрактальности или самоподобия, а также изменчивость показателей, характеризующих фрактальные свойства [1–3]. Для их оценки используются понятия фрактальной размерности (ФР) множества D по Хаусдорфу и пока-

затель Херста H , характеризующий степень самоподобия процесса, связанные между собой соотношением: $D = 2 - H$. В подавляющем большинстве работ в области телекоммуникаций [2–4] используется именно показатель Херста H , отличающийся от D на фиксированную величину. Поэтому в дальнейшем в качестве оценки ФР нормального трафика и КА будем использовать именно его.

Методы фрактального анализа широко используются для обнаружения атак и сетевых аномалий, в том числе в режиме реального времени путем мониторинга текущей ФР трафика компьютерных сетей [4]. Формализуя различие спектров трафика с аномалиями и без них, можно сравнивать фрактальные и корреляционные размерности, а также интервалы, характеризующие «ширину» спектра Лежандра для каждой из реализаций.

Информационные размерности сравниваемых реализаций различаются на небольшую постоянную величину и практически не зависят от количества уровней разложения. Это позволяет сделать вывод о том, что наличие в сигнале продолжительных атак и аномальной активности изменяет самоподобную природу трафика, и данное свойство можно использовать для выявления атак. Учитывая, что для оценки ФР трафика требуется, как правило, значительные интервалы времени и большие объемы данных, обнаружение КА с помощью фрактального анализа осуществлялось, как правило, независимо от других методов, позволяющих определить аномалии во временном ряду в режиме реального времени. Все это послужило поводом для поиска новых методов обнаружения и прогнозирования, к числу которых можно отнести комбинацию машинного обучения и фрактального анализа. Появились работы, в которых вопросы обнаружения и классификации КА стали интегрироваться с методами машинного обучения [4–7].

В работе [5] на примере базы данных KDD Cup1999 [7, 8] показано положительное влияние оценки самоподобных свойств сетевого трафика, характеризуемого средним значением показателя Херста на качество бинарной классификации. Авторы установили, что добавление в число атрибутов дополнительного параметра, характеризующего ФР атак, положительно влияет на эффективность бинарной классификации и справедливо для всех алгоритмов, представленных в исследовании.

В работах [5, 6] на примере набора данных UNSW-NB15 приведены результаты исследования влияния широкого спектра статистических характеристик ФР на качество бинарной классификации. Показано, что параметры ФР могут рассматриваться как дополнительные информационные признаки (атрибуты) КА. В качестве дополнительных при-

знаков предложено использовать широкий спектр статистических характеристик ФР, обрабатываемых последовательностей. Эффективность предлагаемого метода оценивается путем оценки качества бинарной классификации сетевых атак и нормального трафика. С помощью алгоритмов машинного обучения показано, что использование в качестве дополнительных информационных признаков статистических характеристик ФР позволяет повысить ее эффективность в среднем на 10 %.

В работах [8, 9] проанализирован алгоритм обнаружения КА на компьютерные сети, базирующийся на оценке самоподобия аномалий в сетевом трафике с использованием статистических методов. Алгоритм состоит из трех этапов, в рамках которых выполняется анализ свойства самоподобия для эталонного трафика, фрактальных свойств реального трафика и дополнительной обработки временных рядов статистическими методами на заключительном этапе. Программная реализация предложенного подхода подтвердила высокую эффективность проанализированного алгоритма.

В [10] предложено использовать для обнаружения аномальных выбросов в системах передачи данных метод машинного обучения, основанный на применении гибридной искусственной нейронной сети, состоящей из автокодировщика (autoencoder) и классификатора. Экспериментальная оценка предлагаемой методики подтвердила ее достаточную высокую эффективность.

В [11] представлен метод выявления аномалий сетевого трафика, основанный на утверждении о том, что последний является самоподобной структурой и моделируется фрактальным броуновским движением. В качестве инструментов при разработке метода были применены фрактальный анализ и математическая статистика. Проведен анализ существующих методов выявления сетевых аномалий на предмет их недостатков. Результатом работы является модифицированный метод выявления аномалий сетевого трафика. Данный метод относится к полуконтролируемой методике обнаружения аномалий, что позволяет процессу быть практически автономным от человеческого вмешательства. Алгоритм поиска аномалий, лежащий в основе метода, может применяться как для поиска входящих аномалий (сетевых атак), так и для поиска аномалий в исходящем трафике (DLP-системы).

В [12] на основании анализа обширных экспериментальных исследований показано, что существующие модели трафика в современных сетях связи должны отражать не только самоподобные свойства, но и другие характеристики этих потоков трафика, например, мультифрактальные (МФ). Кроме того, структура этих моделей должна учи-

тываться в алгоритме прогнозирования трафика, который выигрывает от более точного моделирования трафика.

В [13] МФ-свойства трафика магистральных сетей Интернета анализируются на основе вычисления функции МФ-спектра над временными рядами, сформированными из различных параметров трафика: IP-адресов и портов отправителя и получателя; временной метки; размера сетевого пакета; числа сетевых пакетов в потоке; типа сетевого протокола транспортного уровня; числа сетевых пакетов протоколов каждого типа; числа исходящих и входящих подключений для хоста и т. д. Данный список может быть расширен. Кроме того, выделенные значения в дальнейшем подвергаются статистической обработке для получения таких параметров, как среднее/максимальное/минимальное число пакетов, размер пакета и т. д. Все вышеописанные параметры необходимы для контроля поведения сетевого трафика; именно эти параметры формируют временные ряды, над которыми вычисляются МФ-эвристики.

В работах [14, 15] предложено использовать МФ-анализ для выявления в трафике магистральных сетей аномалий, свидетельствующих о сетевых неполадках или атаках. В качестве метрик безопасности применены значения характеристик МФ-спектра. Эффективность предложенного подхода подтверждена экспериментальными данными по обнаружению атак отказа в обслуживании.

Вместе с тем во всех указанных работах в качестве основных рассматривались традиционные асимптотические методы оценки ФР. Однако, используя методы текущей оценки ФР в скользящем окне в реальном масштабе времени, можно усовершенствовать рассмотренные алгоритмы.

В [16, 17] рассматривается метод обнаружения аномалий трафика на основе кратномасштабного МФ-анализа путем контроля за скачками ФР в режиме реального времени. Анализируемый метод базируется на текущей оценке МФ-свойств трафика с помощью скользящего окна и кратномасштабном вейвлет-анализе. Полученные численные данные позволяют сделать вывод, что использование ФР для различных составляющих МФ-спектра позволяют с высокой достоверностью зафиксировать наличие аномалии. Учет подобных составляющих МФ-спектра может быть реализован, например, путем построения многоканального алгоритма, каждый канал которого ориентирован на его соответствующую составляющую.

Информация о различии спектров ФР обрабатываемых процессов (если они доступны для обработки) при разном разрешении по времени может быть использована для модификации алгоритмов обнаружения/классификации КА метода-

ми машинного обучения и может привести к улучшению показателей классификации [18–21].

Целью работы являются экспериментальные оценки параметров МФ-спектра ФР компьютерных атак и нормального трафика и их информативная значимость, которые могут быть использованы как дополнительные информационные признаки при реализации алгоритмов классификации КА методами машинного обучения на примере сетей IoT.

Структура и характеристики экспериментального набора данных

В качестве примера, на котором иллюстрируется оценка МФ-характеристик анализируемого трафика, была рассмотрена база Kitsune (2019) [22–24], в которой собран набор данных сетевого трафика от устройств Интернета вещей (IoT, аббр. от англ. Internet of Things). Набор содержит информацию о различных типах атак, таких как разведка (Recon), человек посередине (MitM), отказ в обслуживании (DoS) и вредоносное ПО для ботнетов Mirai (Botnet Malware). В дальнейшем основное внимание уделено вредоносному ПО типа Mirai, которое заражает IoT-устройства и превращает их в сеть дистанционно управляемых ботов, называемых «зомби».

Информационные признаки (атрибуты) КА представляют собой инкрементальные (пошаговые) статистики поступающих данных. Так, если $S = \{x_1, x_2, \dots\}$ представляет собой неограниченный поток данных, где $x_i \in R$ – последовательность наблюдаемых размеров пакетов, то процедура обновления кортежа для вставки x_i в IS имеет вид:

$$IS \leftarrow (N + 1, L_{S_i} + x_i, SS_i + x_i^2),$$

а текущие статистики в любой момент времени:

$$\mu_{S_i} = \frac{1}{N} \sum_{i=1}^N x_i - \text{выборочное среднее};$$

$$\sigma_{S_i}^2 = \frac{1}{N} [\sum_{i=1}^N x_i^2 - \mu_{S_i}^2] - \text{дисперсия};$$

$$\sigma_S = \sqrt{\sigma_{S_i}^2} - \text{среднеквадратичное отклонение (СКО)}.$$

Помимо перечисленных статистик, при формировании атрибутов КА и нормального трафика список статистик, вычисляемых из инкрементальной статистики $IS_{i,\lambda}$, включает также коэффициенты ковариации $\text{cov}(x_i, x_j)$ и корреляции R_{ij} , дополнительные двумерные статистики:

$$M_{ij} = \sqrt{\mu_{S_i}^2 + \mu_{S_j}^2} \text{ и } Q_{ij} = \sqrt{(\sigma_{S_i}^2)^2 + (\sigma_{S_j}^2)^2}.$$

Используя перечисленные статистики в [22, 23], после предобработки сформирован набор из 23 признаков в пяти временных окнах $L = 5$: 100 мс, 500 мс, 1,5 с, 10 с и 1 мин с учетом коэффициента «старения» $\lambda = 5, 3, 1, 0,1$ и $0,01$.

В результате сформирован набор из 115 атрибутов (признаков), характеризующих перечисленные выше типы КА за указанные пять временных интервалов. Набор представлен в таблице 1, где атрибуты в первых 23 строках положены в основу алгоритмов обнаружения и классификации КА в сетях IoT [22, 23]. Однако результаты исследований, представленные в [24], показали, что нормальный трафик и КА в сетях IoT обладают специфическими фрактальными свойствами, что может быть дополнительно использовано для повышения эффективности обработки. В частности, показано, что скачки ФР трафика при возникновении атак могут быть использованы при создании алгоритмов обнаружения КА в сетях IoT, а численные характеристики ФР могут быть использованы в качестве дополнительных информационных признаков КА в задачах классификации методами машинного обучения.

ТАБЛИЦА 1. Набор атрибутов в данных Kitsune в разных временных окнах

TABLE 1. Set of Attributes in Kitsune Data in Different Time Windows

	№ атрибута	Атрибут
1	1, 24, 47, 70, 93	Длина комбинации MAC-IP в битах (μ)
2	2, 25, 48, 71, 94	Длина SrcIP в битах (μ)
3	3, 26, 49, 72, 95	Длина Channel в битах (μ)
4	4, 27, 50, 73, 96	Длина Socket в битах (μ)
5	5, 28, 51, 74, 97	Длина комбинации MAC-IP в битах (σ)
6	6, 29, 52, 75, 98	Длина SrcIP в битах (σ)
7	7, 30, 53, 76, 99	Длина Channel в битах (σ)
8	8, 31, 54, 77, 100	Длина Socket в битах (σ)
9	9, 32, 55, 78, 101	Длина Channel в битах (M_{ij})
10	10, 33, 56, 79, 102	Длина Socket в битах (M_{ij})
11	11, 34, 57, 80, 103	Длина Channel в битах (Q_{ij})
12	12, 35, 58, 81, 104	Длина Socket в битах (Q_{ij})
13	13, 36, 59, 82, 105	Длина Channel в битах ($Cov_{i,j}$)
14	14, 37, 60, 83, 106	Длина Socket в битах ($Cov_{i,j}$)
15	15, 38, 61, 84, 107	Длина Channel в битах (R_{ij})
16	16, 39, 62, 85, 108	Длина Socket в битах (R_{ij})
17	17, 40, 63, 86, 109	Количество пакетов MAC-IP (N)
18	18, 41, 64, 87, 110	Количество пакетов SrcIP в битах (N)
19	19, 42, 65, 88, 111	Количество пакетов Channel в битах (N)
20	20, 43, 66, 89, 112	Количество пакетов Socket в битах (N)
21	21, 44, 67, 90, 113	Межпакетные задержки исходящего трафика (N)
22	22, 45, 68, 91, 114	Межпакетные задержки исходящего трафика, Channel (μ)
23	23, 46, 69, 92, 115	Межпакетные задержки исходящего трафика, Channel (σ)
24	116, 117, 118, 119, 120	МФ-спектр ФР данных в окне разрешения $\{\hat{H}_{t_k}, i = \overline{1,5}\}$

Фрактальный анализ компьютерных атак на примере трафика IoT

Для оценки текущих значений ФР в режиме реального времени предлагается использовать оценки ФР (показателя \hat{H}) в скользящем окне, полученные методами дискретного вейвлет-анализа [17]. Рассмотрим процесс формирования оценки ФР на примере трафика IoT при воздействии атаки Mirai в скользящем окне размером $\Delta = 2000$ отсчетов, представленного на рисунке 1а. Будем считать наблюдаемый случайный процесс $\{X(t_i), i = \overline{1, I}\}$ дискретным. Произведем разложение трафика по вейвлет-коэффициентам в скользящем окне анализа размера Δ , смещение которого осуществляется с шагом $K \leq P$. В результате при смещении окна анализа слева направо оно «пробежит» m положений $M = P/K, m = \overline{1, M}$. В результате вейвлет-коэффициенты детализации вейвлет-разложения при m -м положении окна $d_{j,k}^m$ могут быть найдены в конце анализируемого интервала.

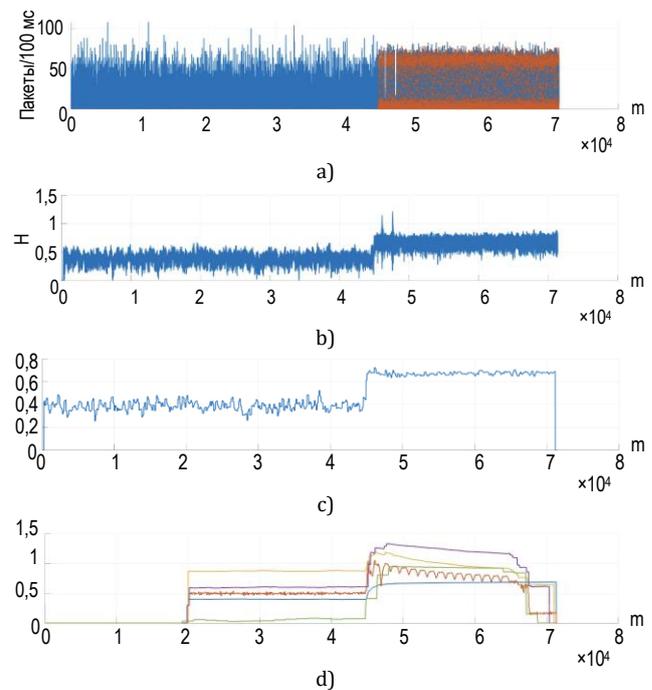


Рис. 1. Фрагмент трафика IoT при воздействии атаки Mirai (а) и оценка параметров его ФР в скользящем окне: \hat{H} с фильтрацией (б) и без фильтрации (с); МФ-спектра при $i = \overline{1,5}$ (д)

Fig. 1. A Fragment of IoT traffic under the Mirai Attack Influence (a) and Estimate of Its Fractal Dimension Parameters in a Sliding Window: \hat{H} with Filtering (b) and Without Filtering (c); Multifractal Spectrum at $i = \overline{1,5}$ (d)

Для нахождения текущей оценки параметра Херста \hat{H}_m при m -м положении окна анализа необходимо выполнить линейную регрессию на шкале j в диапазоне $[j_1, j_2]$, в соответствии с уравнением:

$$\log_2(\mu_{j,m}) = \log_2\left(\frac{1}{n_j} \sum_k |d_x^{(m)}(j, k)|^2\right) = (2\hat{H}_m - 1)j + \hat{c} = \alpha_m j + \hat{c}, \quad (1)$$

где $\hat{c} = \text{const}$.

Уравнение (1) описывает способ оценки показателя Херста \hat{H}_m для процессов с долговременной зависимостью в виде линейной функции вида $\hat{a}_m = (2\hat{H}_m - 1)$.

Оценка параметра Херста в m -м положении скользящего окна \hat{H}_m может быть получена путем оценки наклона графика функции $\log_2(\mu_{j,m})$ от j при каждом m -м положении окна анализа и имеет следующий вид [12]:

$$\hat{H}_m = \frac{1}{2} \left[\frac{\sum_{j=j_1}^{j_2} S_j j \eta_{j,m} - \sum_{j=j_1}^{j_2} S_j j \sum_{j=j_1}^{j_2} S_j j \eta_{j,m}}{\sum_{j=j_1}^{j_2} S_j \sum_{j=j_1}^{j_2} S_j j^2 - (\sum_{j=j_1}^{j_2} S_j j^2)} + 1 \right], \quad (2)$$

где $S = \sum_{j=j_1}^{j_2} 1/\sigma_j^2$, $S_1 = \sum_{j=j_1}^{j_2} j/\sigma_j^2$, $S_2 = \sum_{j=j_1}^{j_2} j^2/\sigma_j^2$ – весовые коэффициенты;

$$\sigma_j^2 = \frac{\xi\left(2, \frac{n_j}{2}\right)}{\ln^2 2} \sim \frac{2}{n_j \ln^2 2};$$

$$n_{j,m} = \log_2\left(\frac{1}{n_j} \sum_k |d_x^{(m)}(j, k)|^2\right).$$

Текущая оценка \hat{H}_m , полученная с помощью (2), в скользящем окне формируется с высокой дисперсией и резкими скачками показателя Херста, как это можно заметить на рисунке 1b. Для сглаживания резких выбросов и уменьшения дисперсии оценка \hat{H}_m в [6] предлагается воспользоваться процедурой трешолдинга (*от англ. Thresholding*, пороговое значение), с помощью которой осуществляется дополнительная фильтрация текущих оценок показателя Херста. В результате использования трешолдинга формула для текущей оценки \hat{H} с использованием дискретного вейвлет-преобразования приобретает следующий вид [6]:

$$\hat{H}(t_m) = \sum_{l=1}^{L_0} a_l^{(H)} \varphi_l^{(H)}(t_m) + \sum_{j=1}^J \sum_{l=1}^{L_j} T(d_{j,l}^{(H)}) \psi_{j,l}^{(H)}(t_m), \quad (3)$$

где $a_{j_0,l}^{(H)}, d_{j,l}^{(H)}$ – аппроксимирующие и детализирующие коэффициенты оценки показателя Херста при m -м положении окна фильтрации; $T(d_{j,l}^{(H)})$ – отфильтрованные с помощью преобразования трешолдинга; $T(\cdot)$ – детализирующие вейвлет-коэффициенты; $a_{j_0,l}^{(H)} = \langle \hat{H}(t_m), \varphi_l^{(H)} \rangle$ – масштабные

коэффициенты аппроксимации, равные скалярному произведению оценки показателя Херста $\hat{H}(t_m)$ и масштабной функции «самого грубого» масштаба j , смещенной на l единиц масштаба вправо от начала координат; $d_{j,l}^{(H)} = \langle \hat{H}(t_m), \psi_{j,l}^{(H)} \rangle$ – вейвлет-коэффициенты детализации масштаба j , равные скалярному произведению оценки показателя Херста $\hat{H}(t_m)$ и вейвлета масштаба j , смещенного на l единиц масштаба вправо от начала координат при $L_0 = 2^{J_{\max}}$, ($L_0 \leq L$), а $J_{\max} = \lfloor \log_2 L \rfloor$ – максимальное число масштабов разложения; $\lfloor \log_2 L \rfloor$ – целая часть числа.

Результаты сглаживания можно видеть на рисунке 1с.

При гауссовских и квазидекоррелированных вейвлет-коэффициентах дисперсия оценки \hat{H} может быть оценена соотношением [17]:

$$\sigma_{\hat{H}}^2 = \text{var} \hat{H}(j_1, j_2) = \frac{2}{n_{j_1} \ln^2 2} \frac{1 - 2^J}{1 - 2^{-(J+1)(J^2+4)+2-2J}}, \quad (4)$$

где $J = j_2 - j_1$ – число октав, вовлеченных в линейное сглаживание; $n_{j_1} = 2^{-j_1} N_0$ – число доступных коэффициентов в рамке j_1 .

Из формулы (4) в гауссовском и асимптотическом приближении можно получить доверительный интервал:

$$\hat{H} - \sigma_{\hat{H}} z_{\beta} \leq H \leq \hat{H} + \sigma_{\hat{H}} z_{\beta},$$

где z_{β} представляет $1 - \beta$ квантиль стандартного Гауссовского распределения, то есть $P(z \geq z_{\beta}) = \beta$. Все результаты, представленные ниже, и при числовом моделировании, и при фактическом анализе данных, были подсчитаны при $\beta = 0,025$ (т. е. 95 % доверительный интервал).

Предложенная модификация алгоритма оценки ФР (3) основана на использовании дополнительной фильтрации показателя Херста \hat{H} внутри скользящего окна. Как показано в [6], для получения достоверной оценки показателя Херста целесообразно использовать вейвлеты Хаара, поскольку в этом случае наблюдается самая низкая дисперсия оценки ФР.

Оценка параметров мультифрактального спектра фрактальной размерности

Учитывая, что свойство самоподобия наблюдается в широких временных масштабах (например, при различном временном разрешении на уровне бит, пакетов, потоков и т. д.), наличие в сигнале продолжительных атак и аномальной активности изменяет самоподобную природу трафика, приводит к МФ-структуре обрабатываемых процессов [21], что может быть использовано, например, для повышения эффективности классификации КА методами машинного обучения.

С целью исследования этого феномена уточним понятие мультифрактального спектра фрактальной размерности. Под МФ-спектром ФР будем понимать последовательность текущих оценок ФР $\widehat{H}_{t_{D_i}}$ в окне анализа Δ фиксированной длины в зависимости от интервала разрешения (времени дискретизации t_D):

$$\{\widehat{H}_{t_{D_i}} = f(t_{D_i}); i = \overline{1, L}; t_{D_i} \in \Delta; \Delta = \text{const}\}. \quad (5)$$

Исследования показывают, что анализируемый случайный процесс в сети IoT можно считать мультифрактальным, поскольку при разных временных шкалах (при разном временном разрешении) величина ФР изменяется. В общем случае оценка ФР является случайной величиной $\widehat{H} \in N(m_{\widehat{H}}, \sigma_{\widehat{H}}^2)$ и полно характеризуется моментами распределения – средним значением $m_{\widehat{H}}$ и дисперсией $\sigma_{\widehat{H}}^2$ оценки.

Для оценки характеристик МФ-спектра ФР рассматриваемых процессов в сетях IoT в виде (5) были выбраны следующие параметры:

- окно оценки ФР $\Delta = 2000$ отсчетов;
- количество окон $L = 5$, так что $i = \overline{1, 5}$;
- время дискретизации наблюдаемых процессов в анализируемых пяти окнах: $t_{D_1} = 100$ мс, $t_{D_2} = 500$ мс, $t_{D_3} = 1$ с, $t_{D_4} = 2$ с, $t_{D_5} = 10$ с.

По итогам исследования были получены значения МФ-спектра ФР для нормального трафика в разных точках описанной топологии сети IoT и разных типов КА типа Mirai, что иллюстрируется на рисунке 1d. В таблице 2 приведены статистические характеристики оценок показателя Херста \widehat{H} в скользящем окне с применением процедуры трешолдинга для пяти окон оценивания размером 100 мс, 500 мс, 1,5 с, 10 с и 1 мин, соответственно.

Количественный анализ полученных результатов показывает, что в отсутствии КА трафик IoT характеризуется оценками среднего значения $m_{\widehat{H}}$ в интервале $\{0...0,5\}$ для интервалов дискретизации: $t_{D_1} = 100$ мс, $t_{D_4} = 2$ с, $t_{D_5} = 10$ с. Это означает, что анализируемый случайный процесс при этих интервалах дискретизации не обладает самоподобием. При $t_{D_2} = 500$ мс и $t_{D_3} = 1$ с значение $m_{\widehat{H}}$ лежит в диапазоне $\{0,5...1,0\}$, что свидетельствует о наличии фрактальных свойств у нормального трафика при этом временном разрешении.

Для КА типа Mirai фрактальными свойствами атака обладает при $t_{D_1} = 100$ мс, $t_{D_2} = 500$ мс, $t_{D_5} = 10$ с. В этом случае значение $m_{\widehat{H}}$ лежит в диапазоне $\{0,5...1,0\}$, что свидетельствует о наличии у КА фрактальных свойств при этом временном разрешении. При $t_{D_3} = 1$ с, $t_{D_4} = 2$ с параметр $m_{\widehat{H}} > 1$, что указывает на наличие аномалий или на нестационарность обрабатываемого процесса.

Указанные значения ФР могут быть использованы в качестве дополнительных атрибутов алгоритма обнаружения атак в сетях IoT для атаки Mirai. На рисунке 2 показаны $m_{\widehat{H}}$ и СКО оценок в скользящем окне Δ при различном временном разрешении. Величина \widehat{H} обычно характеризует степень самоподобия процесса следующим образом. Случай $0,5 < H < 1,0$ характеризует трендоустойчивый, обладающий длительной памятью процесс, который является самоподобным; $0 < H < 0,5$ – характерен для случайного процесса, не обладающего самоподобием; $H > 1,0$ – соответствует аномалии (нестационарности) анализируемого процесса.

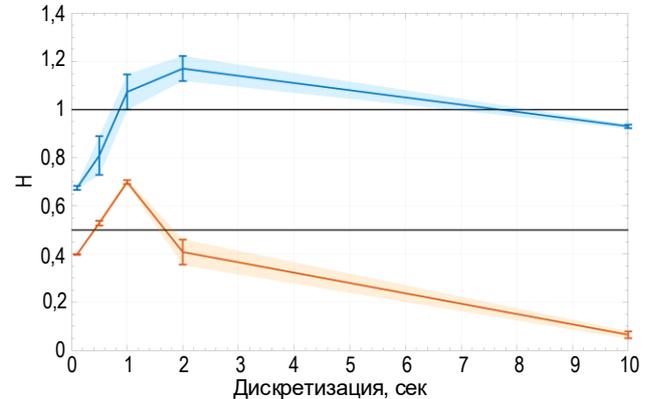


Рис. 2. Оценка показателя Херста при атаке Mirai (синим) и нормального трафика (оранжевым) без аномальных выбросов при разном временном разрешении

Fig. 2. Hurst Exponent Evaluation on Mirai Attack (blue) and Normal Traffic (orange), Filtered Evaluation without Anomalous Outliers at Different Time Resolutions

Используя численные значения среднего $m_{\widehat{H}}$ и СКО фрактальной размерности $\sigma_{\widehat{H}}$ нормального трафика и КА, представленные в таблице 2, предлагается добавить к уже имеющимся атрибутам значения МФ-спектра ФР нормального трафика. Для КА типа атаки Mirai эти пять элементов, характеризующих $\{\widehat{H}_{t_{D_i}}, i = \overline{1, 5}\}$, представлены в строке 24 таблицы 1. В результате количество атрибутов для нормального трафика и КА типа Mirai увеличивается до 120.

ТАБЛИЦА 2. Статистические характеристики оценки нормального / КА трафика IoT с трешолдингом

TABLE 2. Statistical Characteristics of Normal / CA IoT Traffic Assessment with Thresholding

t_{D_i}	$m_{\widehat{H}}$	$\sigma_{\widehat{H}}^2$	$\sigma_{\widehat{H}}$
100 мс	0,3983 / 0,6745	0,00003 / 0,000075	0,0019 / 0,0087
500 мс	0,5285 / 0,8089	0,00096 / 0,0065	0,0098 / 0,0804
1 с	0,6987 / 1,073	0,000069 / 0,0054	0,0084 / 0,0732
2 с	0,4080 / 1,1703	0,0027 / 0,0027	0,0522 / 0,052
10 с	0,0646 / 0,9303	0,0002 / 0,0004	0,0143 / 0,007

Информативная значимость атрибутов

Для оценки влияния на качество классификации КА введенных дополнительных параметров МФ-спектра ФР была оценена их информационная значимость в случае бинарной и многоклассовой классификации. Результаты оценки по индексу

Джини без добавления и с добавлением МФ-спектра ФР приведены в виде гистограмм на рисунке 3. Оценка информативности проводилась относительно классовых меток о наличии (отсутствии) КА типа Mirai Botnet.

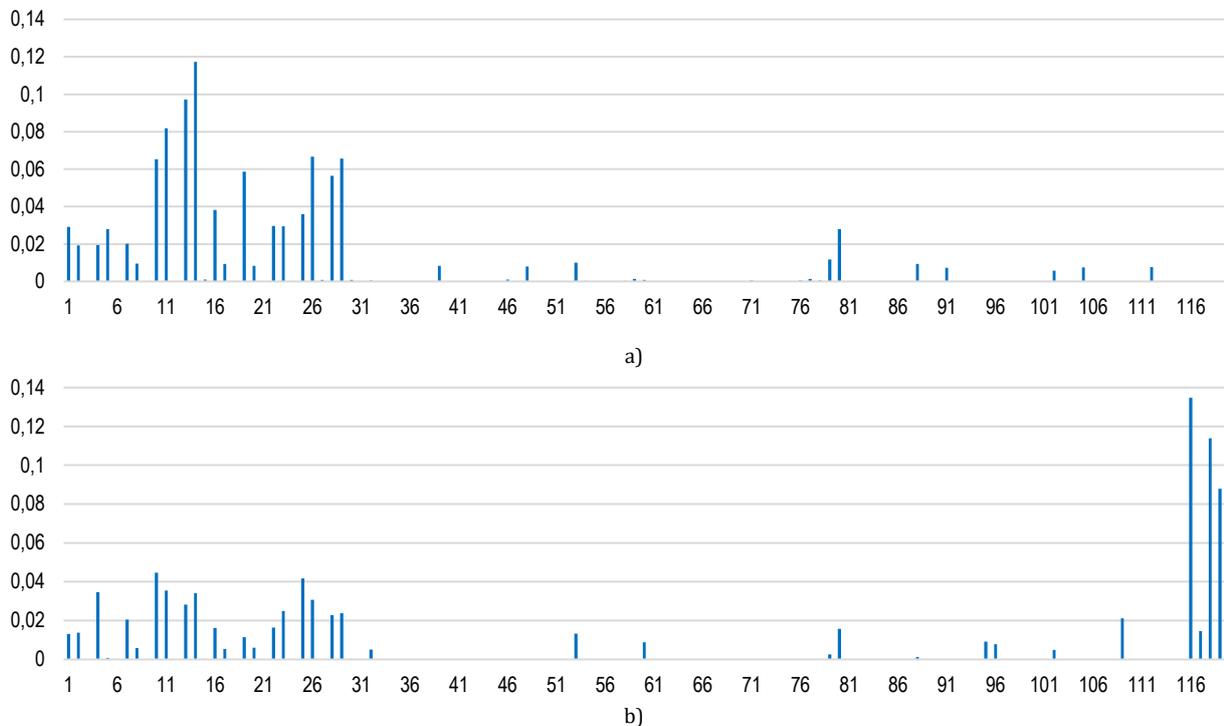


Рис. 3. Оценка информативной значимости атрибутов в задаче бинарной классификации КА типа Mirai Botnet по индексу Джини для двух случаев: без добавления (а) и с добавлением МФ-спектра ФР (б)

Fig. 3. Assessment of the Informative Significance of Attributes in the Task of Binary Classification of the Mirai Botnet Spacecraft Using the Gini Index for Two Cases: a) without Adding Multifractal Spectrum Characteristics of Fractal Dimension (MSFD); b) with the Addition of MSFD

Для сопоставления размерности гистограмм в первом случае оценка важности по представленным в таблице 1 атрибутам 116–120 присвоена равной 0. Был проведен анализ первых 15 наиболее значимых атрибутов для двух случаев – без добавления и с добавлением МФ-спектра ФР.

Анализ распределения на рисунке 3а показал, что наиболее информативными являются атрибуты компьютерной сети (КС), полученные во временном окне 100 мс (см. таблицу 2) и $\lambda = 5$. В число первых 15 наиболее значимых атрибутов, вычисленных для случая без добавления МФ-спектра ФР, попало: 10 – вычисленных во временном окне 100 мс; 4 – 500 мс; 1 атрибут – 10 с. Анализ наиболее значимых атрибутов выявил только 2 «дублирования» по разным временным окнам (атрибуты № 5 и 28 – σ длин комбинаций MAC-IP в битах и атрибуты № 11 и 80, дисперсия длины Channel в битах), в остальном все значимые атрибуты уникальны и не пересекаются.

«Концентрация» наиболее значимых атрибутов в области $\lambda = 5$ может быть обусловлена возможностью детектирования КА во временном окне 100 мс.

Атрибуты, вычисленные в других временных окнах, являются вспомогательными. Добавление МФ-спектра ФР в атрибутное пространство изменяет распределение его информационной значимости по оси ординат (атрибуты 1 ... 115 снизили значимость, в среднем, на 50 %, однако их ранжирование практически не претерпело изменений).

Анализ 15 наиболее значимых атрибутов с учетом добавления МФ-спектра ФР показал, что 6 из 15 атрибутов (40 %) – уникальны. В их число включается 4 атрибута, связанных с МФ-спектром ФР. 7 атрибутов из 15 вычислены во временном окне 100 мс. Четыре атрибута – вычислены для временного окна 500 мс. Один атрибут вычислен для временного окна 1,5 с, один – для временного окна 2 с, и 2 атрибута – для временного окна 10 с.

Анализ атрибутов № 116 ... 120, связанных с МФ-спектром ФР, демонстрирует корреляцию, близкую к линейной, между МФ-спектром ФР и классовыми метками о наличии (отсутствии) КА типа Mirai Botnet. Столь высокая корреляция обусловлена тем, что во время проведения КА типа Mirai Botnet ряд атрибутов КС, связанных с сете-

вым взаимодействием (в таблице 2, атрибуты № 10, 11, 13 и 14, связаны с количеством исходящих пакетов), резко меняют свое распределение (количество пакетов резко возрастает). Таким образом, добавление МФ-спектра ФР в атрибутивное пространство изменяет распределение его информационной значимости по оси ординат.

Так, атрибуты 1...115 снизили значимость, в среднем на 50 %, однако их ранжирование практически не претерпело изменений. Оценка информативности атрибутов в задаче многоклассовой классификации КА типов Mirai Botnet и OS Scan по критерию Джини представлена на рисунке 4.

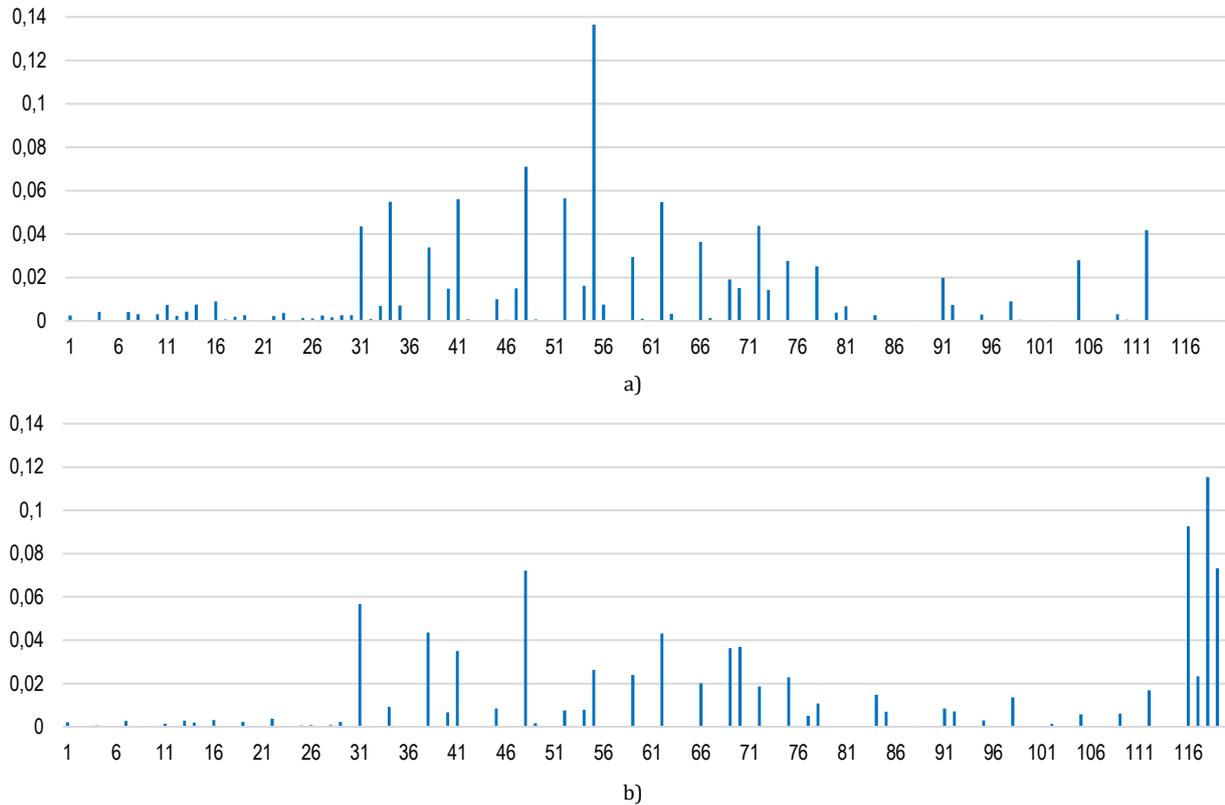


Рис. 4. Оценка информативной значимости атрибутов в задаче многоклассовой классификации КА типов Mirai Botnet и OS Scan по критерию Джини для двух случаев без добавления (а) и с добавлением ФР (б)

Fig. 4. Assessment of the Informative Significance of Attributes in the Task of Multi-Class Classification of the Mirai Botnet and OS Scan Spacecraft Using the Gini Criterion for Two Cases: a) without Adding Fractal Dimension; b) with the Addition of Fractal Dimension

В сравнении с рисунком 3 из данных, представленных на рисунке 4, видно, что распределение атрибутивного пространства «сдвинуто» в сторону более широкого временного окна 500 мс (атрибуты с 24 по 46) и 1,5 с (атрибуты с 47 по 69).

Аналогично случаю бинарной классификации, был проведен анализ первых 15 наиболее значимых атрибутов для двух случаев – без добавления и с добавлением МФ-спектра ФР.

В число первых 15 наиболее значимых атрибутов, вычисленных для случая без добавления МФ-спектра ФР, не попало ни одного атрибута, вычисленного для временного окна в 100 мс. Основная концентрация атрибутов наблюдается на интервале 500 мс...1,5 с и составляет 67 %, остальные атрибуты распределены в диапазоне 2...10с. «Сдвиг» информационной значимости атрибутов в область более широких временных окон может

быть обусловлен наличием атаки второго типа – OS Scan, а также большого количества данных о нормальном функционировании КС. С учетом объединения наборов данных (для КА типов Mirai Botnet и OS Scan) доля «нормальных» записей в итоговом наборе составляет 92 % (2 274 666 шт.) против 84 % (642 516 шт.) в исходном наборе данных Mirai Botnet.

При классификации двух КА в условиях усилившегося дисбаланса классов, временное окно в 100 мс не является достаточно информативным. Больше информации может быть извлечено из атрибутов, полученных на временных окнах от 500 мс и выше.

Анализ 15 наиболее значимых атрибутов с учетом добавления МФ-спектра ФР позволил сделать выводы, схожие со случаем бинарной классификации. Семь из 15 атрибутов (47 %) – уникальны. В

их число входят 5 атрибутов (против 4 атрибутов в случае бинарной классификации), связанных с МФ-спектром ФР. Линейная корреляция между последним и классовыми метками о наличии или отсутствии КА типа Mirai Botnet сохраняется.

Таким образом, добавление фрактальной размерности КА типа Mirai Botnet в атрибутное пространство изменяет распределение информативности атрибутов аналогично эксперименту с бинарной классификацией. Изменение по оси ординат не столь выражено, поскольку фрактальная размерность добавлена только для КА типа Mirai Botnet.

Заключение

Введено понятие МФ-спектра ФР в виде последовательности текущих оценок ФР $\hat{H}_{t_{d_i}}$ в окне анализа фиксированной длины в зависимости от интервала разрешения.

Найденные экспериментальные значения параметров МФ-спектра ФР, представленные в виде дополнительных атрибутов в таблице 1 (атрибуты № 116...120), представляющих собой текущие оценки ФР $\hat{H}_{t_{d_i}}$ в окне анализа для различных интервалов разрешения.

Полученные дополнительные атрибуты нормального трафика и трафика под КА, а также рас-

пределения их информационной значимости могут быть использованы для повышения достоверности обнаружения и эффективности классификации КА методами машинного обучения в сетях IoT, как это показано в [25].

Для задачи бинарной классификации КА типа Mirai Botnet для двух случаев: без добавления и с добавлением МФ-спектра ФР, – получена оценка информативной значимости атрибутов по индексу Джини. Показано, что наиболее информативными являются атрибуты КС, полученные во временном окне 100 мс.

Добавление МФ-спектра ФР в атрибутное пространство изменяет распределение его информационной значимости. Атрибуты № 116...120, связанные с МФ-спектром ФР, демонстрируют корреляцию, близкую к линейной, между МФ-спектром ФР и классовыми метками о наличии (отсутствии) КА типа Mirai Botnet.

Показано, что основная концентрация наиболее значимых атрибутов приходится на интервал 500 мс ... 1,5 с (67 %), остальные распределены в диапазоне 2...10 с. «Сдвиг» информационной значимости атрибутов в область более широких временных окон обусловлен наличием атаки второго типа – OS Scan, а также большого количества данных о нормальном функционировании КС.

Список источников

1. Park K., Willinger W. Self-Similar Network Traffic: An Overview // In: Self-Similar Network Traffic and Performance Evaluation. John Wiley & Sons, 2000. DOI:10.1002/047120644X.ch1
2. Шелухин О.И., Осин А.В., Смольский С.М. Самоподобие и фракталы. Телекоммуникационные приложения. М: Физматлит, 2008. С. 362. EDN:MVSWAB
3. Sheluhin O., Smolskiy S., Osin A. Self-Similar Processes in Telecommunications. John Wiley & Sons, 2007. 334 p.
4. Шелухин О.И. Сетевые аномалии. Обнаружение, локализация, прогнозирование. М: Горячая линия – Телеком, 2019. С. 448.
5. Sheluhin O., Kazhemiyskiy M. Influence Of Fractal Dimension Statistical Characteristics On Quality Of Network Attacks Binary Classification // Proceedings of the 28th Conference of Open Innovations Association (FRUCT, Moscow, Russia, 27–29 January 2021). Vol. 28. IEEE, 2021. PP. 407–413. DOI:10.23919/FRUCT50888.2021.9347600. EDN:XMLZKW
6. Sheluhin O.I., Rybakov S.Y., Vanyushina A.V. Detection of Network Anomalies with the Method of Fixing Jumps of the Fractal Dimension in the Online Mode // Proceedings of the 28th Conference at Wave Electronics and Its Application in Information and Telecommunication Systems (WECONF, St. Petersburg, Russia, 30 May 2022 – 03 June 2022). Vol. 5. IEEE, 2022. PP. 430–435. DOI:10.1109/WECONF55058.2022.9803635. EDN:UEYFUM
7. Шелухин О.И., Рыбаков С.Ю., Ванюшина А.В. Влияние фрактальной размерности на качество классификации компьютерных атак методами машинного обучения // Научные технологии в космических исследованиях Земли. 2023. Т. 15. № 1. С. 57–64. DOI:10.36724/2409-5419-2023-15-1-57-64. EDN:EVELAW
8. Котенко И.В., Саенко И.Б., Лаута О.С., Крибель А.М. Метод раннего обнаружения кибератак на основе интеграции фрактального анализа и статистических методов // Первая миля. 2021. № 6(98). С. 64–71. DOI:10.22184/2070-8963.2021.98.6.64.70. EDN:KRIUAD
9. Перов Р.А., Лаута О.С., Крибель А.М., Федупов Ю.М. Комплексная методика обнаружения кибератак на основе интеграции фрактального анализа и статистических методов // Научные технологии в космических исследованиях Земли. 2022. Т. 14. № 2. С. 44–51. DOI:10.36724/2409-5419-2022-14-2-44-51. EDN:ELALFA
10. Котенко И.В., Саенко И.Б., Лаута О.С., Крибель А.М. Методика обнаружения аномалий и кибератак на основе интеграции методов фрактального анализа и машинного обучения // Информатика и автоматизация. 2022. Т. 21. № 6. С. 1328–1358. DOI:10.15622/ia.21.6.9. EDN:IWILXQ
11. Карачанская Е.В., Соседова Н.И. Метод выявления аномалий сетевого трафика, основанный на его самоподобной структуре // Безопасность информационных технологий. 2019. Т. 26 № 1. С. 98–110. EDN:YZELNB

12. Vieira F.H.T., Bianchi G.R., Lee L.L. A Network Traffic Prediction Approach Based on Multifractal Modeling // *Journal of High Speed Networks*. 2010. Vol. 17(2). PP. 83–96. DOI:10.3233/JHS-2010-0334
13. Зегжда П.Д., Лаврова Д.С., Штыркина А.А. Мультифрактальный анализ трафика магистральных сетей интернет для обнаружения атак отказа в обслуживании // *Проблемы информационной безопасности. Компьютерные системы*. 2018. № 2. С. 48–58. EDN:ХТКTFZ
14. Лаврова Д.С., Зегжда Д.П., Зегжда П.Д., Штыркина А.А. Оценка киберустойчивости информационно-технологических систем на основе самоподобия // *Материалы 25-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации»*. СПб.: Изд-во Политехн. Ун-та, 2016. С. 101–104. EDN:YPUWMH
15. Штыркина А.А., Зегжда П.Д., Лаврова Д.С. Обнаружение аномалий в трафике магистральных сетей Интернет с использованием мультифрактального анализа // *Материалы 27-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации»*. СПб.: Изд-во Политехн. Ун-та, 2018. С. 14–15. EDN:YPUXQD
16. Шелухин О.И., Панкрушин А.В. Обнаружение аномальных выбросов в реальном масштабе времени методами мультифрактального анализа // *Нелинейный мир*. 2016. Т. 14. № 2. С. 72–82. EDN:VTZNTH
17. Sheluhin O.I., Lukin I.Y. Network Traffic Anomalies Detection Using a Fixing Method of Multifractal Dimension Jumps in a Real-Time Mode // *Automatic Control and Computer Sciences*. 2018. Vol. 52. Iss. 5. PP. 421–430. DOI:10.3103/S0146411618 050115. EDN:OJQHKD
18. Riedi R.H., Crouse M.S., Ribeiro V.J., Baraniuk R. A multifractal wavelet model with application to network traffic // *IEEE Transactions on Information Theory*. 1999. Vol. 45. Iss. 3. PP. 992–1018. DOI:10.1109/18.761337
19. Taqqu M.S., Teverovsky V., Willinger W. Is Network Traffic Self-Similar or Multifractal? // *Fractals*. 1997. Vol. 5. PP. 63–73. DOI:10.1142/S0218348X97000073
20. Sheluhin O.I., Garmashev A.B., Aderemi A.A. Detection of teletraffic anomalies using multifractal analysis // *International Journal of Advancements in Computing Technology*. 2011. Vol. 3. Iss. 4. PP. 174–182. DOI:10.4156/ijact.vol3.issue4.19. EDN:PDYTSP
21. Шелухин О.И. Мультифракталы: инфокоммуникационные приложения. М.: Горячая линия – Телеком, 2011. 576 с. EDN:QMUYXJ
22. Mirsky Y., Doitshman T., Elovici Y., Shabtai A. Kitsune: an Ensemble of Autoencoders for Online Network Intrusion Detection // *arXiv:1802.09089v2*. 2018. DOI:10.48550/arXiv.1802.09089
23. Miyamoto K., Goto H., Ishibashi R., Han C., Ban T., Takahashi T., et al. Malicious Packet Classification Based on Neural Network Using Kitsune Features // *Proceedings of the 2nd International Conference on Intelligent Systems and Pattern Recognition (ISPR 2022, Hammamet, Tunisia, 24–26 March 2022)*. Communications in Computer and Information Science. Vol. 1589. Cham: Springer, 2022. PP. 306–314. DOI:10.1007/978-3-031-08277-1_25
24. Шелухин О.И., Рыбаков С.Ю. Статистические характеристики фрактальной размерности трафика IoT на примере набора данных Kitsune // *Труды учебных заведений связи*. 2023. Т. 9. № 5. С. 112–119. DOI:10.31854/1813-324X-2023-9-5-112-119. EDN:YMSJRF
25. Шелухин О.И., Рыбаков С.Ю., Раковский Д.И. Классификация компьютерных атак с использованием мультифрактального спектра фрактальной размерности // *Вопросы кибербезопасности*. 2024. № 2(60) С.107–119. DOI:10.21681/2311-3456-2024-2-107-119. EDN:GKOSBB

References

1. Park K., Willinger W. Self-Similar Network Traffic: An Overview. In: *Self-Similar Network Traffic and Performance Evaluation*. John Wiley & Sons, 2000. DOI:10.1002/047120644X.ch1
2. Sheluhin O.I., Osin A.V., Smolskiy S.M. *Self-Similarity and Fractals. Telecommunication Applications*. Moscow: Fizmatlit Publ.; 2008. 362 p. (in Russ.) EDN:MVSWAB
3. Sheluhin O., Smolskiy S., Osin A. *Self-Similar Processes in Telecommunications*. John Wiley & Sons, 2007. 334 p.
4. Sheluhin O.I. *Network Anomalies. Detection, Localization, Forecasting*. Moscow: Goryachaya liniya –Telekom Publ.; 2019. 448 p. (in Russ.)
5. Sheluhin O., Kazhenskiy M. Influence Of Fractal Dimension Statistical Characteristics On Quality Of Network Attacks Binary Classification. *Proceedings of the 28th Conference of Open Innovations Association, FRUCT, 27–29 January 2021, Moscow, Russia, vol.28*. IEEE; 2021. p.407–413. DOI:10.23919/FRUCT50888.2021.9347600. EDN:XMLZKW
6. Sheluhin O.I., Rybakov S.Y., Vanyushina A.V. Detection of Network Anomalies with the Method of Fixing Jumps of the Fractal Dimension in the Online Mode. *Proceedings of the 28th Conference at Wave Electronics and Its Application in Information and Telecommunication Systems, WECONF, 30 May 2022 – 03 June 2022, St. Petersburg, Russia. vol.5*. IEEE; 2022. p.430–435. DOI:10.1109/WECONF55058.2022.9803635. EDN:UEYFUM
7. Sheluhin O.I., Rybakov S.Yu., Vanyushina A.V. Influence of fractal dimension on quality classification of computer attacks by machine learning methods. *H&ES Reserch*. 2023;15(1):57–64. (in Russ.) DOI:10.36724/2409-5419-2023-15-1-57-64. EDN:EVELAW
8. Kotenko I., Saenko I., Lauta O., Kribel A. The method of early detection of cyber attacks based on the integration of fractal analysis and statistical methods. *Pervaya milya*. 2021;6(98):64–71. DOI:10.22184/2070-8963.2021.98.6.64.70. EDN:KRIUAD
9. Perov R.A., Lauta O.S., Kribel A.M., Fedulov Yu.M. A comprehensive technique for detecting cyber attacks based on the integration of fractal analysis and statistical methods. *H&ES Reserch*. 2022;14(2):44–51. (in Russ.) DOI:10.36724/2409-5419-2022-14-2-44-51. EDN:ELALFA

10. Kotenko I., Saenko I., Lauta O., Kribel A. Anomaly and cyber attack detection technique based on the integration of fractal analysis and machine learning methods. *Informatics and Automation*. 2022;6(21):1328–1358. (in Russ.) DOI:10.15622/ia.21.6.9. EDN:IWILXQ
11. Karachanskaya E.V., Sosedova N.I. Method for detection of network traffic anomalies which is based on its self-similar traffic structure. *Bezopasnost informacionnyh tehnology*. 2019;26(1):98–110. (in Russ.) EDN: YZELNB
12. Vieira F.H.T., Bianchi G.R., Lee L.L. A Network Traffic Prediction Approach Based on Multifractal Modeling. *Journal of High Speed Networks*. 2010;17(2):83–96. DOI:10.3233/JHS-2010-0334
13. Zegzhda P.D., Lavrova D.S., Shtyrkina A.A. Multifractal Analysis of Backbone Network Traffic for Denial-of-Service Attacks Detection. *Information Security Problems. Computer Systems*. 2018;2:48–58. (in Russ.) EDN:XTKTFZ
14. Lavrova D.S., Zegzhda D.P., Zegzhda P.D., Shtyrkina A.A. Assessment of cyber resilience of information technology systems based on self-similarity. *Proceedings of the 25th Scientific and Technical Conference on Methods and Technical Means of Ensuring Information Security*. St Petersburg: Peter the Great St. Petersburg Polytechnic University Publ.; 2016. p.101–104. (in Russ.) EDN:YPUWMH
15. Shtyrkina A.A., Zegzhda P.D., Lavrova D.S. Detecting anomalies in Internet backbone traffic using multifractal analysis. *Proceedings of the 27th Scientific and Technical Conference on Methods and Technical Means of Ensuring Information Security*. St Petersburg: Peter the Great St. Petersburg Polytechnic University Publ.; 2018. p.14–15. (in Russ.) EDN:YPUXQD
16. Sheluhin O.I., Pankrushin A.V. Detection of Anomalies in Real Time Using the Methods of Multifractal Analysis. *Nonlinear World*. 2016;14(2):72–82. (in Russ.) EDN:VTZNTN
17. Sheluhin O.I., Lukin I.Y. Network Traffic Anomalies Detection Using a Fixing Method of Multifractal Dimension Jumps in a Real-Time Mode. *Automatic Control and Computer Sciences*. 2018;52(5):421–430. DOI:10.3103/S0146411618050115. EDN:OJQHKD
18. Riedi R.H., Crouse M.S., Ribeiro V.J., Baraniuk R. A multifractal wavelet model with application to network traffic. *IEEE Transactions on Information Theory*. 1999;45(3):992–1018. DOI:10.1109/18.761337
19. Taqqu M.S., Teverovsky V., Willinger W. Is Network Traffic Self-Similar or Multifractal? *Fractals*. 1997;5:63–73. DOI:10.1142/S0218348X97000073
20. Sheluhin O.I., Garmashev A.B., Aderemi A.A. Detection of teletraffic anomalies using multifractal analysis. *International Journal of Advancements in Computing Technology*. 2011;3(4):174–182. DOI:10.4156/ijact.vol3.issue4.19. EDN:PDYTSP
21. Sheluhin O.I. *Multifractals: Infocommunication Applications*. Moscow: Goryachaya liniya –Telekom Publ.; 2011. 576 p. EDN:QMUYXJ
22. Mirsky Y., Doitshman T., Elovici Y., Shabtai A. Kitsune: an Ensemble of Autoencoders for Online Network Intrusion Detection. *arXiv:1802.09089v2*. 2018. DOI:10.48550/arXiv.1802.09089
23. Miyamoto K., Goto H., Ishibashi R., Han C., Ban T., Takahashi T., et al. Malicious Packet Classification Based on Neural Network Using Kitsune Features. *Proceedings of the 2nd International Conference on Intelligent Systems and Pattern Recognition, ISPR 2022, 24–26 March 2022, Hammamet, Tunisia. Communications in Computer and Information Science, vol.1589*. Cham: Springer; 2022. p.306–314. DOI:10.1007/978-3-031-08277-1_25
24. Sheluhin O., Rybakov S. IoT Traffic Fractal Dimension Statistical Characteristics on the Kitsune Dataset Example. *Proceedings of Telecommunication Universities*. 2023;9(5):112–119. (in Russ.) DOI:10.31854/1813-324X-2023-9-5-112-119. EDN:YMSJRF
25. Sheluhin O.I., Rybakov S.Yu., Rakovsky D.I. Classification of computer attacks using multifractal spectrum of fractal dimension. *Voprosy kiberbezopasnosti*. 2024;2(60):107–119. (in Russ.) DOI:10.21681/2311-3456-2024-2-107-119. EDN:GKOSBB

Статья поступила в редакцию 08.04.2024; одобрена после рецензирования 14.04.2024; принята к публикации 03.06.2024.

The article was submitted 08.04.2024; approved after reviewing 14.04.2024; accepted for publication 03.06.2024.

Информация об авторах:

ШЕЛУХИН
Олег Иванович

доктор технических наук, профессор, заведующий кафедрой «Информационная безопасность» Московского технического университета связи и информатики
 <https://orcid.org/0000-0001-7564-6744>

РЫБАКОВ
Сергей Юрьевич

руководитель НОЦ «Информационная безопасность» Московского технического университета связи и информатики
 <https://orcid.org/0000-0002-4593-9009>

ВАНЮШИНА
Анна Вячеславовна

кандидат технических наук, доцент, доцент кафедры «Информационная безопасность» Московского технического университета связи и информатики
 <https://orcid.org/0000-0001-8729-6729>

Авторы сообщают об отсутствии конфликтов интересов.

The authors declare no conflicts of interests.

Научная статья

УДК 004.056.53

<https://doi.org/10.31854/1813-324X-2024-10-3-116-126>

Оценка визуальных интерфейсов систем управления информационной безопасностью

✉ Андрей Алексеевич Чечулин^{1,2}, chечулин.аа@sut.ru

¹Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, Санкт-Петербург, 199178, Российская Федерация

²Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация

Аннотация

Актуальность. В данной статье рассматриваются методы оценки эффективности форм представления информации в прикладном программном обеспечении, с акцентом на разработке комплексной методики для оценки интерфейсов систем мониторинга и управления информационной безопасностью. Пользовательский интерфейс является ключевым элементом, от которого зависит функциональность, удобство и эстетическая привлекательность программного обеспечения. Эти аспекты, в свою очередь, напрямую влияют на восприятие и качество работы пользователей с программными продуктами, что особенно важно в контексте систем информационной безопасности для обеспечения эффективного и своевременного реагирования на инциденты и угрозы. **Целью данного исследования** является разработка комплексной методики, которая бы позволила оценивать эффективность информационных представлений в системах безопасности, сочетая анкетирование пользователей для получения интегрального показателя качества интерфейса и использование метода GOMS (Goals, Operators, Methods, and Selection Rules) для оценки скорости выполнения задач. **Предлагаемая методика** включает два основных этапа: первый этап – анкетирование, которое позволяет собрать субъективные оценки пользователей и выявить интегральный показатель качества интерфейса; второй этап – применение метода GOMS, который позволяет провести количественную оценку эффективности интерфейса, измеряя время, затрачиваемое пользователем на выполнение задач. Эти два этапа взаимодополняют друг друга, обеспечивая всесторонний подход к оценке пользовательского интерфейса. Полученное таким образом **решение** позволяет классифицировать пользовательские интерфейсы на четыре уровня качества: «отличный», «хороший», «удовлетворительный» и «неудовлетворительный». **Новизна** исследования заключается в том, что предложенный подход, в отличие от аналогов, объединяет субъективные и объективные методы анализа, что обеспечивает более точную и всестороннюю оценку качества интерфейсов систем информационной безопасности.

Теоретическая значимость работы состоит в создании новой методики оценки пользовательских интерфейсов, которая может быть применена к различным системам информационной безопасности.

Практическая значимость заключается в возможности использования полученных результатов для улучшения взаимодействия операторов с системами мониторинга и управления информационной безопасности, что в конечном счете повышает общую защищенность и эффективность работы информационных систем за счет повышения качества принимаемых оператором решений. В рамках будущей работы планируется расширить исследование, включив в него учет дополнительных аспектов, таких как влияние когнитивных нагрузок на операторов и использование адаптивных методов визуализации, которые будут подстраиваться под индивидуальные особенности пользователей.

Ключевые слова: пользовательский интерфейс, usability, графический интерфейс, метод GOMS, оценка эффективности, системы информационной безопасности

Ссылка для цитирования: Чечулин А.А. Оценка визуальных интерфейсов систем управления информационной безопасностью // Труды учебных заведений связи. 2024. Т. 10. № 3. С. 116–126. DOI:10.31854/1813-324X-2024-10-3-116-126. EDN:HZWDEV

Original research

<https://doi.org/10.31854/1813-324X-2024-10-3-116-126>

Evaluation of Visual Interfaces in Information Security Management Systems

 **Andrey A. Chechulin**^{1,2}, chechulin.aa@sut.ru

¹Saint Petersburg Federal Research Center of the Russian Academy of Science,
St. Petersburg, 199178, Russian Federation

²The Bonch-Bruевич Saint Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Annotation

*This article discusses methods for evaluating the effectiveness of information presentation forms in application software, with a focus on developing a comprehensive methodology for assessing interfaces in information security monitoring and management systems. The user interface is a key element that affects the functionality, convenience, and aesthetic appeal of software. These aspects directly influence how users perceive and interact with the software, which is especially important in the context of information security systems to ensure effective and timely responses to incidents and threats. **The aim of this study** is to develop a comprehensive methodology that allows for the evaluation of the effectiveness of information presentations in security systems. This methodology combines user surveys to obtain an overall quality indicator of the interface with the use of the GOMS method (Goals, Operators, Methods, and Selection Rules) to assess the speed of task completion. **The proposed methodology** includes two main stages: the first stage involves user surveys to gather subjective assessments and determine an overall quality indicator of the interface; the second stage involves the application of the GOMS method, which provides a quantitative evaluation of interface efficiency by measuring the time users spend on completing tasks. These two stages complement each other, providing a comprehensive approach to evaluating the user interface. This approach allows for the classification of user interfaces into four quality levels: "excellent", "good", "satisfactory", and "unsatisfactory". **The novelty of the study** lies in its unique approach that combines both subjective and objective methods of analysis, providing a more accurate and comprehensive evaluation of interface quality in information security systems. **The theoretical significance** of the work is in the creation of a new methodology for evaluating user interfaces, which can be applied to various information security systems. **The practical significance** is in the potential use of the results to improve the interaction between operators and information security monitoring and management systems, ultimately enhancing the overall security and efficiency of information systems by improving the quality of operator decision-making. Future research plans include expanding the study to cover additional aspects such as the impact of cognitive loads on operators and adaptive visualization methods that can adjust to individual user characteristics.*

Keywords: *user interface, usability, graphical interface, GOMS method, efficiency evaluation, information security systems*

For citation: Chechulin A.A. Evaluation of Visual Interfaces in Information Security Management Systems. *Proceedings of Telecommunication Universities*. 2024;10(3):116–126. (in Russ.) DOI:10.31854/1813-324X-2024-10-3-116-126. EDN:HZWDEV

Введение

Проектирование пользовательского интерфейса (UI, аббр. от англ. User Interface) – одна из ключевых задач в разработке программного обеспечения, особенно в контексте систем информационной безопасности (ИБ). Функциональность, удобство и эстетическая привлекательность интерфейса напрямую влияют на восприятие и отноше-

ние пользователей к программному продукту. Непродуманный интерфейс может оттолкнуть пользователей, что сведет на нет усилия разработчиков по созданию эффективного и полезного программного обеспечения. При этом восприятие интерфейса каждым пользователем является субъективным, что добавляет сложности к задаче его проектирования.

Одной из важных характеристик пользовательского интерфейса является его удобство (*по англ. usability*), что подразумевает возможность того, что пользователь со средним уровнем знаний и опыта сможет эффективно взаимодействовать с программным продуктом. Достижение высокого уровня usability является основной целью при проектировании интерфейсов, а методики оценки их эффективности служат критерием успешности достигнутых результатов.

Результаты данного исследования направлены на совершенствование визуальных интерфейсов систем ИБ. Эти интерфейсы играют решающую роль в процессе принятия решений операторами, работающими с системами мониторинга и управления ИБ. Качество интерфейса напрямую влияет на скорость и точность принимаемых решений, что особенно важно в условиях высокой ответственности и потенциальных рисков, связанных с ИБ.

В исследовании представлен анализ существующих подходов к оценке визуальных интерфейсов и предложение новой комплексной методики, сочетающей преимущества различных методов. Разработанная методика включает два основных этапа: анкетирование с участием пользователей для определения обобщенного показателя качества интерфейса и применение метода GOMS (*аббр. от англ. Goals, Operators, Methods, and Selection Rules* – цели, объекты, методы и правила выбора) для измерения скорости выполнения задач пользователем. Введение комплексного подхода позволит классифицировать пользовательские интерфейсы на четыре уровня качества: «отличный», «хороший», «удовлетворительный» и «неудовлетворительный».

Контекст научной проблемы и релевантные исследования

При мониторинге ИБ с помощью аналитического моделирования можно выделить четыре основных этапа: 1) сбор данных, 2) формирование моделей; 3) анализ защищенности; 4) представление результатов оператору. На каждом из этих этапов возникают проблемы неполноты и неточности.

На первом этапе данные могут быть противоречивы и неполны, что затрудняет создание точной и полной картины состояния информационной системы.

На втором – используемые для анализа модели могут не полностью соответствовать особенностям реальных компьютерных сетей, что приводит к неточностям в анализе.

На третьем – вычисляемые характеристики могут отражать не те аспекты, которые реально важны для обеспечения ИБ.

На четвертом – неудачно выбранные модели визуализации могут вводить оператора в заблуждение и приводить к принятию неверных решений.

Данная статья является частью цикла исследований [1] и посвящена рассмотрению подходов к повышению эффективности последнего (четвертого) этапа моделирования – визуализации результатов анализа защищенности. Основное внимание уделяется оценке качества программных интерфейсов систем ИБ. В работе рассматриваются текущие подходы к визуализации данных и предлагается комплексная методика для оценки эффективности интерфейсов. Эта методика учитывает как субъективное мнение пользователей, так и объективные показатели производительности. Такой подход поможет улучшить взаимодействие операторов с системами мониторинга и управления ИБ, а также повысить точность и оперативность принимаемых решений.

Информация в современных системах ИБ представляется в двух основных формах: текстовой и графической. Для компонентов, обеспечивающих принятие решений в системах мониторинга и управления ИБ, наиболее эффективной является графическая форма, реализуемая в интерфейсе пользователя (GUI, *аббр. от англ. Graphical User Interface*). Графический интерфейс позволяет операторам системы ИБ быстрее и эффективнее взаимодействовать с данными, что способствует принятию более качественных решений в условиях ограниченного времени и высокой ответственности. Важным направлением является разработка систем визуального анализа данных, которые обеспечивают более эффективное принятие решений на основе визуальных представлений больших объемов информации [2].

Современные графические интерфейсы состоят из совокупности диалоговых окон, включающих в себя элементы управления, такие как полосы меню, панели инструментов, строки состояния и другие компоненты. Привлекательность и удобство графического интерфейса зависят от множества факторов, включая грамотное расположение элементов управления, их информативность, оформление и документирование [3]. Критически важны такие аспекты, как наличие подписей, всплывающих подсказок, пиктограмм, способы группировки элементов, их доступность (например, активация по «горячим клавишам»), цветовое оформление и другие параметры.

Эффективность взаимодействия пользователя с программным средством определяется тем, насколько интерфейс понятен и привлекателен для пользователя, а также тем, как быстро пользователь может решать свои задачи с его помощью. В контексте систем ИБ это приобретает особую значимость, так как правильность и скорость принятия решений операторами могут существенно влиять на общую безопасность системы.

Для оценки эффективности форм представления информации в графических интерфейсах выделяют два основных подхода [4] (рисунок 1): тестирование с участием группы пользователей и формальные расчеты.

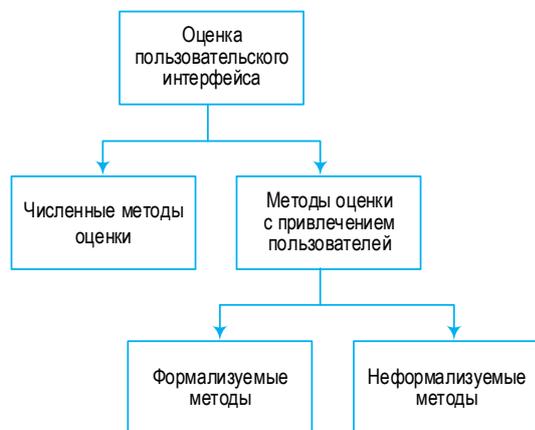


Рис. 1. Классификация подходов к оценке пользовательского интерфейса

Fig. 1. Classification of Approaches to User Interface Evaluation

Тестирование с привлечением пользователей включает сбор и анализ информации о субъективном восприятии интерфейса, что позволяет выявить и устранить замечания пользователей, а также получить количественные характеристики оценки интерфейса. Различные методы, такие как прототипирование, тест ожиданий, эвристическая оценка, анкетирование и метод фокус-групп предоставляют разнообразные инструменты для оценки интерфейса на ранних и промежуточных этапах его разработки. Формальные методы оценки основываются на количественных расчетах, что позволяет проводить автоматизированную оценку графических интерфейсов. Метрики сложности интерфейса (ICM, аббр. от англ. Interface Complexity Metric) и метрики удобства, такие как плотность и баланс, позволяют количественно оценить сложность и удобство представления информации. Методы слежения за взглядом и прогнозирования пользовательского внимания дополняют картину, помогая выявить наиболее значимые зоны интерфейса [5].

Методика оценки эффективности форм представления информации с привлечением группы пользователей

Классическим способом оценки эффективности форм представления информации программными средствами является привлечение к процессу оценивания как квалифицированных, так и обычных пользователей, с целью собрать и проанализировать информацию об их субъективном восприятии пользовательского интерфейса. Целью такой методики является, с одной стороны, фиксация заме-

чаний пользователей и их устранение, с другой – получение количественных характеристик оценки интерфейса. Существует множество подходов к опросу пользовательского мнения. Результаты опроса могут представляться как в формализованном виде в результате оценки пользовательского интерфейса по определенным критериям, так и на естественном языке, что достигается при помощи соответствующих дискуссий.

На ранних этапах разработки программного обеспечения целесообразно применять метод прототипирования [6]. Данный метод заключается в том, что пользователю вместо анкет предлагаются различные прототипы будущего интерфейса, а его задача состоит в том, чтобы провести сопоставительный анализ. Целью прототипирования является определение наиболее перспективного интерфейса, который затем будет использоваться в качестве основного. На практике представляется целесообразным доверить разработку прототипов разным специалистам и предоставить пользователям возможность выбрать лучший из них. Допустимо как составление полноценного прототипа, так и прототипа отдельных узловых частей. Для сравнения представленных прототипов следует также определить критерии их оценки (скорость ввода данных, простота принятия решения на основе представленной информации, субъективная оценка привлекательности прототипа и др.).

Оценка пользовательского интерфейса при помощи теста ожиданий состоит в том, что пользователю ставится определенная задача, а он указывает на конкретный элемент управления, с которого он начнет ее выполнение. Тест считается пройденным, если пользователь выбрал правильный компонент. Тест ожиданий позволяет понять, насколько предложенный интерфейс является интуитивно понятным для пользователя, а также выявить ошибки в группировке его управляющих элементов (например, меню).

Следует отметить, что такие методы оценки пользовательского интерфейса, как прототипирование и тест ожиданий, следует применять на начальных этапах разработки программного продукта. Применение указанных методов снижает вероятность получения неудовлетворительных результатов при оценке итоговой версии пользовательского интерфейса.

Среди наиболее простых и распространенных подходов можно выделить процесс оценки пользовательского интерфейса при помощи эвристик (например, стандарт ISO 9241). Под эвристикой следует понимать какое-либо наиболее общее правило, характерное для человеко-машинного взаимодействия. Совокупность таких правил представляет собой контрольный список или чек-лист (от англ. Check List). В ходе своей оценки

пользователь устанавливает, соответствуют ли элементы представленного интерфейса перечисленным в контрольном списке критериям. В случае обнаружения несоответствий их необходимо устранить.

Оценка пользовательского интерфейса может также осуществляться путем составления рейтингов завершенности (*по англ.* Completion Rate). Для составления такого рейтинга пользователю предоставляется список задач, характерных для рассматриваемого программного средства, которые ему необходимо решить путем взаимодействия с его интерфейсом. В случае успешного решения задачи пользователь присваивает ей значение «1», в случае неудачи – значение «0». На основе полученных данных подсчитывается рейтинг завершенности каждой задачи как отношение количества пользователей, успешно ее решивших, к общему числу пользователей. В результате анализа более, чем 1200 задач, поставленных перед пользователями, установлено, что среднее значение всех рейтингов завершенности составляет 78 % [7]. Таким образом, значения рейтинга ниже указанного уровня могут свидетельствовать о фатальных ошибках, допущенных при проектировании пользовательского интерфейса.

Другим подходом к оценке пользовательского интерфейса является анкетирование. В ходе анкетирования пользователю предлагается дать свою субъективную оценку заранее подготовленным утверждениям, характеризующим работу с программным средством. Каждое утверждение оценивается по определенной для каждой анкеты шкале. Основная цель анкетирования – дать возможность пользователю передать свое впечатление о пользовательском интерфейсе, в том числе о его usability. Для некоторых типичных анкет подсчитаны средние показатели, с помощью которых разработчики могут оценивать результаты собственного анкетирования. Например, в результате исследования 500 анкет, заполненных по форме, предложенной в [8], установлено, что средним показателем оценки интерфейса является значение 68 при максимальном значении 100 [6].

Для оценки привлекательности интерфейса и эмоционального восприятия его дизайна пользователю может быть предложено множество прилагательных, среди которых он выбирает такие прилагательные, которые наиболее выразительно характеризуют представленный ему интерфейс. Зачастую для определения общего концепта исследуемого интерфейса целесообразно добавить дополнительные прилагательные, не относящиеся непосредственно к задачам, для решения которых разрабатывался данный интерфейс.

Преимущество представленных подходов, в которых для оценки привлекаются пользователи, заключается в том, что человеческое восприятие приобретает формальный характер. К недостаткам можно отнести тот факт, что результат оценки сильно зависит от того, насколько точно и качественно были разработаны предлагаемые пользователю задания.

Рассмотрим методику оценки пользовательского интерфейса, при которой пользователи предлагают улучшения на естественном языке, используя метод фокус-групп. Этот подход помогает избежать обработки большого объема разнородных данных, поступающих от пользователей с различным уровнем подготовки.

Метод фокус-групп включает привлечение нескольких небольших групп заинтересованных пользователей, каждая из которых состоит из 7–10 человек. Участники этих групп могут быть разделены по различным критериям, но на практике целесообразно формировать группы по уровню знаний: опытные пользователи, пользователи среднего уровня и новички. На обсуждение, цель которого – выявление наиболее проблемных участков интерфейса и установление способов их устранения, предлагается прототип разрабатываемого интерфейса. В ходе обсуждения пользователи каждой группы выражают свое мнение относительно представленного прототипа. Полученные по окончании обсуждений сведения задают дальнейшее направление совершенствования разрабатываемого интерфейса. Заметим, что после устранения выявленных пользователями замечаний возможно повторное использование метода фокус-групп для анализа полученных результатов и выявления новых недостатков.

Эффект от метода фокус-групп и проведенных улучшений для i -й итерации применения этого метода можно рассчитать по формуле, предложенной в [9]:

$$I_i = \frac{P_i}{T_i} \times 100 \%, \quad (1)$$

где P_i – замечания пользователей, для которых предложено новое решение; T_i – общее количество замечаний пользователей на i -й итерации.

Однако формула (1) не учитывает возможности неудачного устранения выявленных пользователями ошибок, которые исправлялись повторно на следующей итерации. В [10] приведен общий критерий неудовлетворенности качеством интерфейса Q_n учитывающий $n - 1$ повторных исправлений:

$$Q_n = \frac{\sum_{i=1}^n P'_i}{\sum_{i=0}^n T_i} \times 100 \%, \quad (2)$$

где $\sum_{i=1}^n P'_i$ – общее количество замечаний, для которых предлагались повторные исправления; $\sum_{i=0}^n T_i$ – общее количество замечаний на всех итерациях. Очевидно, что показателем успешности проводимых изменений является динамика:

$$Q_n \rightarrow 0 \%$$

Методы оценки эффективности форм представления данных, в которых участвуют пользователи, позволяют контролировать развитие пользовательского интерфейса с самого начала разработки. Они включают в себя постоянное обсуждение и корректировку интерфейса на промежуточных стадиях, а также окончательную количественную оценку на финальном этапе создания программного обеспечения.

Методика оценки эффективности форм представления информации, основанная на формальном расчете

Одним из альтернативных способов оценки пользовательского интерфейса, исключающим участие пользователей и осуществляемым автоматически, является метод, основанный на формальных расчетах эффективности графического интерфейса. Этот метод использует заранее известные формулы, в которые подставляются данные, касающиеся самого интерфейса и, в некоторых случаях, задачи, выполняемой виртуальным пользователем. Поскольку характеристики индивидуальных пользователей не учитываются, расчеты проводятся на основе средних значений.

Во время взаимодействия с графическим интерфейсом важную роль играет сложность визуального представления информации и расположение элементов управления. Соотношение сложности интерфейса и комфорта пользователя приведено на рисунке 2 [11].

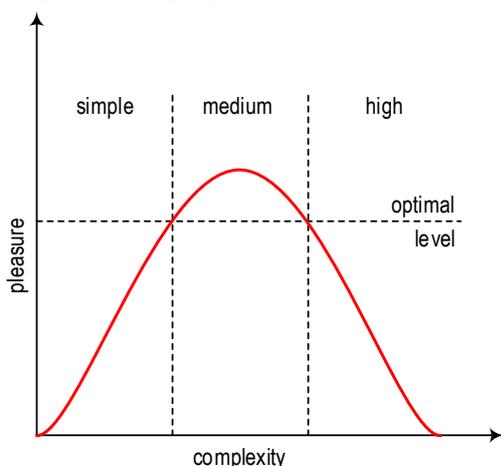


Рис. 2. Сложность интерфейса и уровень комфорта пользователя

Fig. 2. Interface Complexity and User Pleasure Level

Кривая показывает, что удобство интерфейса для пользователя возрастает с увеличением сложности до определенного оптимального уровня, после чего начинает снижаться (см. рисунок 2) – это иллюстрирует важность правильного выбора сложности интерфейса для достижения максимального удобства для пользователей.

Сложность визуального представления информации может быть подсчитана при помощи метрик ISM. Существуют разные подходы к определению таких метрик. Метод, предложенный в [12], позволяет проводить оценку сложности интерфейса, основываясь на человеческом восприятии элементов пользовательского интерфейса и их визуальном оформлении. Принцип, заложенный в данном методе, аналогичен процессу сжатия изображения по алгоритму JPEG: чем сложнее изображение, тем больший размер имеет файл, полученный в результате его сжатия.

Формула сложности пользовательского интерфейса X , реализующая данный принцип, имеет вид:

$$X = A \times O \times S, \tag{3}$$

где A – количество функциональных элементов (кнопки, флажки, переключатели, списки выбора и др.); O – количество группирующих элементов (меню, вкладки и др.); S – суммарная энтропия значений RGB, посчитанная на скриншоте экрана (от англ. Screenshot) исследуемого интерфейса. Формула (3) разработана для вычисления сложности представления информации на интернет-страницах. Для подсчета сложности пользовательского интерфейса, выполненного при помощи диалогового окна и элементов управления, целесообразно использовать следующую модификацию [12]:

$$X = A \times O. \tag{4}$$

Расположение элементов управления играет важную роль при попытке оценить пользовательский интерфейс с точки зрения эстетики представления информации. К метрикам оценки эстетического представления информации можно отнести равновесие, симметрию, последовательность, связность, пропорцию, простоту, регулярность, экономность, однородность, ритм, порядок и сложность. В [13] в качестве основных метрик эстетического представления используются понятия плотности и баланса. Плотность расположения элементов управления в окне зависит от его площади и суммарной площади элементов управления.

Таким образом, плотность прямо пропорциональна количеству пикселей, занимаемых элементами управления, и обратно пропорциональна общему количеству пикселей, занимаемых окном:

$$D = 1 - \frac{\sum_i^n a_i}{a_f} \in [0,1], \quad (5)$$

где a_i – площадь i -го элемента управления; a_f – площадь окна; n – количество элементов управления в окне.

Баланс можно определить как распределение визуальных весов в окне, когда под визуальным весом понимается восприятие того, что некоторые элементы управления или их группы «тяжелее», чем другие. Так, к примеру, чем больше объект, тем он выглядит «тяжелее». Сбалансированное представление элементов управления достигается их равномерным распределением по окну, в его нижней, верхней, правой и левой частях. Расчет баланса производится по формуле:

$$B = 1 - \frac{|B_v| + |B_h|}{2} \in [0,1], \quad (6)$$

где B_v и B_h – вертикальный и горизонтальный баланс, соответственно, расчет которых производится в соответствии с формулами (7 и 8):

$$B_v = \frac{W_L - W_R}{\max(W_L, W_R)}, \quad (7)$$

$$B_h = \frac{W_T - W_B}{\max(W_T, W_B)}, \quad (8)$$

$$w_j = \sum_i^{n_j} a_{ij} d_{ij}, j = L, R, T, B, \quad (9)$$

где буквы L , R , T и B обозначают левую и правую части, а также верх и низ окна, соответственно; a_{ij} – площадь элемента управления i на стороне j ; d_{ij} – расстояние между центральными линиями элемента управления и окна; n_j – общее количество элементов управления на стороне j .

Другим методом для оценки сбалансированности интерфейса и выявления ключевых зон, привлекающих внимание пользователя, является анализ движений глаз. Этот метод позволяет создать тепловую карту интерфейса, показывающую, где пользователь сосредотачивает свое внимание. Более интенсивные зоны отображаются яркими, «теплыми» цветами, такими как красный. Обычно, для реализации этого метода требуется специализированное программное и аппаратное обеспечение, что делает его довольно дорогим. Однако существуют системы, которые могут эмулировать и предсказывать внимание пользователя. Пример такой системы представлен в работе [14].

Среди различных методик, применяемых для формальной оценки пользовательских интерфейсов, выделяется метод GOMS. Этот метод позволяет определить, сколько времени в среднем требуется опытному пользователю для выполнения определенной задачи с использованием конкретного интерфейса.

Метод GOMS предполагает, что каждая задача (*по англ.* Goal) выполняется через определенный набор методов (*по англ.* Methods), которые представляют собой последовательность действий, необходимых для достижения цели в рамках интерфейса. Выбор методов или правил (*по англ.* Selection Rules) зависит от текущего контекста пользователя и его знаний о системе.

Каждый метод разбивается на элементарные действия, называемые операторами (*по англ.* Operators). Для достижения точных результатов оценки с использованием метода GOMS, предполагается, что пользователь полностью владеет интерфейсом.

Согласно методу KLM GOMS (*от англ.* Keystroke-Level Model – модель уровня нажатия на кнопку) [15], можно выделить четыре вида операторов: K – нажатие на кнопку на клавиатуре или мыши; P – наведение указателя мыши на нужный элемент управления; H – перемещение рук на клавиатуру или мышь; M – время, необходимое пользователю для приготовления к выполнению задачи.

Для указанных операторов можно подсчитать среднее время t их выполнения в секундах:

$$t(K) = 2; t(P) = 1,1; t(H) = 0,4; t(M) = 1,35.$$

Метод GOMS применяется для оценки эффективности форм представления информации путем вычисления среднего времени, которое потребуется пользователю для выполнения заданных задач. Интерфейс считается более удачным, если указанное время выполнения задач минимально.

Результаты, полученные с помощью метода GOMS, могут быть более точными, если включить в расчеты время, затрачиваемое пользователем на перемещение указателя мыши к нужному объекту:

$$T = a + b \times \log_2 \left(\frac{D}{S} + 1 \right), \quad (10)$$

где a – среднее время от начала до завершения движения; b – коэффициент, отражающий обычную скорость работы пользователя; D – расстояние от начальной точки курсора до целевого элемента; S – размер целевого объекта по направлению движения курсора. Формула (10) известна как закон Фиттса.

В случаях, когда пользователь обладает правом выбора из нескольких вариантов, среднее время, которое он затрачивает на выбор одного варианта, может быть вычислено по закону Хика:

$$T = a + b \times \log_2(n + 1), \quad (11)$$

где a , b – константы; n – количество вариантов выбора. Значения констант a и b зависят от многих факторов, при этом, чем сложнее выбор из представленных вариантов, или чем хуже пользова-

тель знаком с представленным ему интерфейсом, тем больше значения этих констант. Одним из главных недостатков данного метода является предположение, что пользователь всегда действует безошибочно и знает, как достичь нужного результата при работе с интерфейсом.

Численные методы оценки эффективности форм представления информации позволяют сравнивать различные интерфейсы между собой или с эталонными показателями. Однако эти методы не могут предоставить ответ на вопрос, насколько конкретный интерфейс является понятным и удобным для пользователя.

Комплексная методика оценки эффективности форм представления информации в системах поддержки принятия решений

Предлагаемая методика включает в себя два этапа оценки. На первом этапе оценивания используется метод анкетирования с привлечением группы пользователей, результатом которого должен быть обобщенный интегральный показатель качества пользовательского интерфейса. На втором этапе применяется метод GOMS с целью оценки скорости выполнения пользователем поставленных перед ним задач.

Этап 1. Анкетирование. На данном этапе группа экспертов M проходит анкетирование, результаты которого позволяют получить обобщенный интегральный показатель качества пользовательского интерфейса, на основе анализа множества отдельных характеристик интерфейса K . В опросе участвуют эксперты с различными уровнями компетентности, которые оценивают интерфейс по нескольким критериям. Ниже приводится пошаговая реализация этапа.

1) Каждый эксперт $m^i \in M$ выставляют уровень своей компетенции по шкале от 0 до 3, где 0 – это отсутствие, а 3 – это максимальный уровень компетенций. Предполагается, что среди экспертов есть хотя бы один, чей уровень компетенции выше 0. Нормализованный уровень компетенции эксперта q^i вычисляется по формуле:

$$q^i = \frac{S^i}{\sum_{j=1}^{|M|} S_j^i} \tag{12}$$

2) Каждый эксперт $m^i \in M$ выбирает $K_i \subseteq K$ и ранжирует $k_j^i \in K_i$ подмножество оцениваемых характеристик. Для этого между двумя соседними характеристиками k_j^i и k_{j+1}^i эксперт определяет соотношения важности, выставляя условия «>>» (много больше), «>» (больше) или «=» (равно).

3) Весовые коэффициенты x_j^i и x_{j+1}^i , характеризующие относительную значимость факторов, устанавливаются на основе ранжирования характеристик k_j^i и k_{j+1}^i следующим образом:

- если $k_j^i = k_{j+1}^i$, то $\frac{x_j^i}{x_{j+1}^i} = \frac{1}{1}$;
- если $k_j^i > k_{j+1}^i$, то $\frac{x_j^i}{x_{j+1}^i} = \frac{1/j}{1/(j+1)} = \frac{j+1}{j}$ (гармоническое соотношение);
- если $k_j^i \gg k_{j+1}^i$, то $\frac{x_j^i}{x_{j+1}^i} = \frac{1}{1/2} = \frac{2}{1}$ (геометрическое соотношение).

4) Для первой и наиболее значимой характеристики ее весовой коэффициент x_j^i устанавливается равным 1. При проведении оценки экспертам не обязательно выбирать все доступные характеристики, поскольку ранжирование уменьшает весовые коэффициенты. На практике, после нормализации весовых коэффициентов, можно сосредоточиться только на тех характеристиках, чьи весовые коэффициенты превышают 10 % от значения самой важной характеристики.

5) Нормализованные весовые коэффициенты $\{x_j^i\}_{j=1}^{|K_i|}$ рассчитываются для получения интегрального показателя качества интерфейса по следующей формуле:

$$p_j^i = \frac{x_j^i}{\sum_{j=1}^{|K_i|} x_j^i}, 0 \leq p_j^i \leq 1. \tag{13}$$

6) В результате нормализации будет справедливо следующее соотношение:

$$\sum_{j=1}^{|K_i|} p_j^i \tag{14}$$

7) Каждый эксперт $m^i \in M$ оценивает каждую характеристику $k_j^i \in K_i$ по шкале от 0 до 5 баллов, где 5 – это наименьшая, а 0 – наивысшая степень удовлетворенности экспертом соответствующей характеристикой интерфейса.

8) Интегральный показатель качества пользовательского интерфейса рассчитывается для каждого эксперта следующим образом:

$$W^i = \frac{\sum_{j=1}^{|K_i|} (p_j^i \times X_j^i)}{5}, \tag{15}$$

где X_j^i – количество баллов, которое i -й эксперт присвоил j -й характеристике. Из формулы (15) следует, что: если каждый $X_j^i \rightarrow 0$, то $W^i \rightarrow 0$; если каждый $X_j^i \rightarrow 5$, то $W^i \rightarrow 1$. Таким образом, $W^i \in [0, 1]$.

9) Обобщенный интегральный показатель качества интерфейса W рассчитывается как средневзвешенное значение на множестве $\{W^i\}$ с учетом нормированных весовых коэффициентов q^i , отражающих компетентность каждого эксперта:

$$W = \sum_{i=1}^{|M|} (q^i \times W^i). \tag{16}$$

10) Класс качества пользовательского интерфейса определяется согласно таблице 1.

ТАБЛИЦА 1. Уровни ранжирования и классы качества

TABLE 1. Ranking Levels and Quality Classes

Значение W	Уровень	Класс качества
0–0,25	отличный	0
0,25–0,5	хороший	1
0,5–0,75	удовлетворительный	2
0,75–1,0	неудовлетворительный	3

Этап 2. Применение метода GOMS. На данном этапе используется метод GOMS для оценки скорости выполнения задач пользователем. Этот метод позволяет определить среднее время, необходимое пользователю для выполнения определенной задачи, с использованием интерфейса; интерфейс считается тем лучше, чем меньше времени требуется пользователю на выполнение задач. Ниже приводится пошаговая реализация этапа.

1) Задачи разбиваются на элементарные действия (операторы). Для выполнения задачи $s \in S^N$ (где S – это множество всех возможных задач, которые можно выполнить с использованием оцениваемого интерфейса, а подмножество $S^N \subseteq S$ включает наиболее часто решаемые задачи) пользователь должен последовательно выполнить ряд элементарных операторов $\{a_i\}_{i=1}^{m^s}$, $a_i \in \{K, P, H, M\}$, где K, P, H, M – см. выше в описании метода GOMS, а m^s – методы, используемые для решения задачи s .

2) Среднее время $G(s)$ выполнения задачи вычисляется как сумма времени выполнения всех операторов a_i при помощи метода GOMS по формуле (предполагается, что пользователь хорошо знаком с данным интерфейсом и выполняет задачи без ошибок):

$$G(s) = \sum_{i=1}^{m^s} t(a_i). \quad (17)$$

3) Интегральный показатель времени T , характеризующий время, необходимое для решения задачи при помощи анализируемого интерфейса рассчитывается по формуле:

$$T = \sum_{i=1}^N (G(s_i) \times w_i), \quad (18)$$

где $\{w\}_{i=1}^N$ – набор весов, заданных следующим образом:

$$w_i = \frac{h_i}{\sum_{j=1}^N h_j}, w_i \in [0,1],$$

где, в свою очередь, h_i – частота выполнения задачи t_i .

4) Класс скорости пользовательского интерфейса определяется согласно таблице 2.

ТАБЛИЦА 2. Уровни ранжирования и классы скорости

TABLE 2. Ranking Levels and Speed Classes

Значение T , сек	Уровень	Класс скорости
1–5	отличный	0
5–8	хороший	1
8–10	удовлетворительный	2
более 10	неудовлетворительный	3

Комплексная оценка эффективности интерфейса может быть рассчитана по формуле:

$$C(I) = \min\{C_q(I), C_v(I)\}. \quad (19)$$

Полученная в результате оценка позволяет не только объективно измерить качество интерфейса, но и выявить ключевые области для улучшения. Классификация интерфейсов на четыре уровня качества обеспечивает наглядное представление об их состоянии, что значительно упрощает процесс принятия решений по их доработке и оптимизации. Таким образом, данная оценка способствует созданию более интуитивно понятных и удобных интерфейсов систем ИБ, что, в конечном счете, повышает общую безопасность и эффективность работы информационных систем.

Заключение

В данной статье описаны различные методики оценки графического пользовательского интерфейса. Все рассмотренные методики можно разделить на два класса.

К первому классу относятся методики с привлечением группы пользователей-экспертов. Преимуществами данных методик являются возможность оценивать эмоциональное восприятие интерфейса человеком, его соответствие общепринятым нормам, а также возможность учитывать замечания пользователей и своевременно вносить необходимые изменения в проектируемый интерфейс. Недостатками указанных методик является их трудоемкость, слабая формализация получаемых результатов, сильная зависимость результатов от правильности формулировок поставленных перед пользователями задач и невозможность автоматизировать сам процесс оценивания.

Ко второму классу относятся методики, основанные на формальных расчетах. Их преимуществами являются простота и дешевизна проведения процесса оценивания с возможностью его автоматизации. К недостаткам таких методик следует отнести отсутствие возможности оценить, насколько дружелюбным и комфортным для человека является исследуемый интерфейс. В ряде случаев формальные оценки являются опосредованными оценками самих пользователей.

Также в статье представлена комплексная методика для оценки эффективности визуальных интерфейсов систем поддержки принятия решений для мониторинга и управления ИБ компьютерных сетей. Этот подход объединяет метод экспертной оценки с участием группы пользователей и метод, основанный на формальных расчетах. Применение данной методики позволяет классифицировать пользовательский интерфейс на один из четырех уровней: «отличный», «хороший», «удовлетворительный» и «неудовлетворительный».

Исследование продемонстрировало важность интеграции как субъективных, так и объективных методов анализа для оценки визуальных интер-

фейсов систем управления ИБ. В будущем планируется расширить данное исследование, включив в него дополнительные аспекты, такие как влияние когнитивных нагрузок на операторов при работе с интерфейсом и адаптивные методы визуализации, которые будут подстраиваться под индивидуальные особенности пользователей. Также предполагается разработка автоматизированных инструментов для непрерывного мониторинга и оценки качества интерфейсов в реальном времени, что позволит оперативно выявлять и устранять их уязвимости. Эти направления исследований будут способствовать дальнейшему повышению эффективности и надежности систем управления ИБ.

Список источников

1. Левшун Д.С., Гайфулина Д.А., Чечулин А.А., Котенко И.В. Проблемные вопросы информационной безопасности киберфизических систем // Информатика и автоматизация. 2020. № 5(19). С. 1050–1088. DOI:10.15622/ia.2020.19.5.6. EDN:NIWASO
2. Gan M., Lyu M. Investigation on Visual Communication Design Based on Information Systems // Proceedings of the 2nd International Conference on Data Analytics, Computing and Artificial Intelligence (ICDACAI, Zakopane, Poland, 17–19 October 2023). IEEE, 2023. PP. 720–725. DOI:10.1109/ICDACAI59742.2023.00143
3. Kolomeec M.V., Gonzalez-Granadillo G., Doynikova E.V., Chechulin A.A., Kotenko I.V., Debar H. Choosing Models for Security Metrics Visualization // Proceedings of the 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security (MMM-ACNS 2017, Warsaw, Poland, 28–30 August 2017). Lecture Notes in Computer Science. Cham: Springer, 2017. Vol. 10446. PP. 75–87. DOI:10.1007/978-3-319-65127-9_7
4. Вострых А.В. Метод и алгоритмы многокритериальной оценки графических пользовательских интерфейсов программных продуктов МЧС России // Национальная безопасность и стратегическое планирование. 2022. № 4(40). С. 57–64. DOI:10.37468/2307-1400-2023-2022-4-57-64. EDN:GCHUOC
5. Сервис Feng-GUI для оценки качества графического интерфейса пользователя // Feng-Gui. URL: <http://www.feng-gui.com> (Accessed 06.05.2024)
6. Scott B. The Art of UI Prototyping. 2006. URL: <https://msdn.microsoft.com/en-us/library/ms993294.aspx> (Accessed 06.05.2024)
7. Sauro J. 10 Benchmarks for User Experience Metrics. 2012. URL: <https://measuringu.com/ux-benchmarks> (Accessed 06.05.2024)
8. System Usability Scale (SUS) // Usability.gov. URL: <http://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html> (Accessed 06.05.2024)
9. Sawyer P., Flanders A., Wixon D. Making a Difference – The Impact of Inspections // Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (Vancouver, Canada, 13–18 April 1996). New York: ACM Press, 1996. PP. 376–382. DOI:10.1145/238386.238579
10. Medlock M.C., Wixon D., Terrano M., Romero R.L., Fulton B. Using the RITE method to improve products; a definition and a case study. URL: <https://citeseeerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=5340ef8a91900840263a4036b0433a389b7097b2> (Accessed 06.05.2024)
11. Novikova E., Kotenko I., Fedotov E. Interactive Multi-View Visualization for Fraud Detection in Mobile Money Transfer Services // International Journal of Mobile Computing and Multimedia Communications. 2014. Vol. 6. Iss. 4. PP. 73–97. DOI:10.4018/IJMCMC.2014100105
12. Stickel C., Ebner M., Holzinger A. The XAOS Metric – Understanding Visual Complexity as Measure of Usability // Proceedings of the 6th Symposium of the Workgroup Human-Computer Interaction and Usability Engineering (USAB 2010, Klagenfurt, Austria, 4–5 November 2010). Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2009. Vol. 6389. PP. 278–290. DOI:10.1007/978-3-642-16607-5_18
13. Vanderdonckt J. Automated evaluation of graphical user interface metrics. Louvain-la-Neuve: Année académique, 2010–2011.
14. Card S., Moran T.P., Newell A. The Psychology of Human-Computer Interaction. Hillsdale: Lawrence Erlbaum Associates, 1983. 469 p.
15. Card S.K., Moran T.P., Newell A. The Key Stroke-Level Model for User Performance Time with Interactive Systems // Communications of the ACM. 1980. Vol. 23. Iss. 7. PP. 396–410. DOI:10.1145/358886.358895

References

1. Levshun D., Gaifulina D., Chechulin A., Kotenko I. Problematic Issues of Information Security of Cyber-Physical Systems. *Informatics and Automation*. 2020;5(19):1050–1088. (in Russ.) DOI:10.15622/ia.2020.19.5.6. EDN:NIWASO
2. Gan M., Lyu M. Investigation on Visual Communication Design Based on Information Systems. *Proceedings of the 2nd*

International Conference on Data Analytics, Computing and Artificial Intelligence, ICDACAI, 17–19 October 2023, Zakopane, Poland. IEEE; 2023. p.720–725. DOI:10.1109/ICDACAI59742.2023.00143

3. Kolomeec M.V., Gonzalez-Granadillo G., Doynikova E.V., Chechulin A.A., Kotenko I.V., Debar H. Choosing Models for Security Metrics Visualization. *Proceedings of the 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2017, 28–30 August 2017, Warsaw, Poland. Lecture Notes in Computer Science, vol.10446.* Cham: Springer; 2017. p.75–87. DOI:10.1007/978-3-319-65127-9_7

4. Vostryh A. Method and algorithms of multi-criteria evaluation of graphical user interfaces of software products of the Ministry of emergency situations of Russia. *National Security and Strategic Planning.* 2022;4(40):57–64. (in Russ.) DOI:10.37468/2307-1400-2023-2022-4-57-64. EDN:GCHUOC

5. *Feng-Gui.* Feng-GUI service for assessing the quality of the graphical user interface. URL: <http://www.feng-gui.com> [Accessed 06.05.2024]

6. Scott B. *The Art of UI Prototyping.* 2006. URL: <https://msdn.microsoft.com/en-us/library/ms993294.aspx> [Accessed 06.05.2024]

7. Sauro J. *10 Benchmarks for User Experience Metrics.* 2012. URL: <https://measuringu.com/ux-benchmarks> [Accessed 06.05.2024]

8. *Usability.gov.* System Usability Scale (SUS). URL: <http://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html> [Accessed 06.05.2024]

9. Sawyer P., Flanders A., Wixon D. Making a Difference – The Impact of Inspections. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 13–18 April 1996, Vancouver, Canada.* New York: ACM Press; 1996. p.376–382. DOI:10.1145/238386.238579

10. Medlock M.C., Wixon D., Terrano M., Romero R.L., Fulton B. *Using the RITE method to improve products; a definition and a case study.* URL: <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=5340ef8a91900840263a4036b0433a389b7097b2> [Accessed 06.05.2024]

11. Novikova E., Kotenko I., Fedotov E. Interactive Multi-View Visualization for Fraud Detection in Mobile Money Transfer Services. *International Journal of Mobile Computing and Multimedia Communications.* 2014;6(4):73–97. DOI:10.4018/IJMCMC.2014100105

12. Stickel C., Ebner M., Holzinger A. The XAOS Metric – Understanding Visual Complexity as Measure of Usability. *Proceedings of the 6th Symposium of the Workgroup Human-Computer Interaction and Usability Engineering, USAB 2010, 4–5 November 2010, Klagenfurt, Austria. Lecture Notes in Computer Science, vol.6389.* Berlin, Heidelberg: Springer; 2009. p.278–290. DOI:10.1007/978-3-642-16607-5_18

13. Vanderdonckt J. *Automated evaluation of graphical user interface metrics.* Louvain-la-Neuve: Année académique; 2010–2011.

14. Card S., Moran T.P., Newell A. *The Psychology of Human-Computer Interaction.* Hillsdale: Lawrence Erlbaum Associates; 1983. 469 p.

15. Card S.K., Moran T.P., Newell A. The Key Stroke-Level Model for User Performance Time with Interactive Systems. *Communications of the ACM.* 1980;23(7):396–410. DOI:10.1145/358886.358895

Статья поступила в редакцию 07.05.2024; одобрена после рецензирования 30.05.2024; принята к публикации 10.06.2024.

The article was submitted 07.05.2024; approved after reviewing 30.05.2024; accepted for publication 10.06.2024.

Информация об авторе:

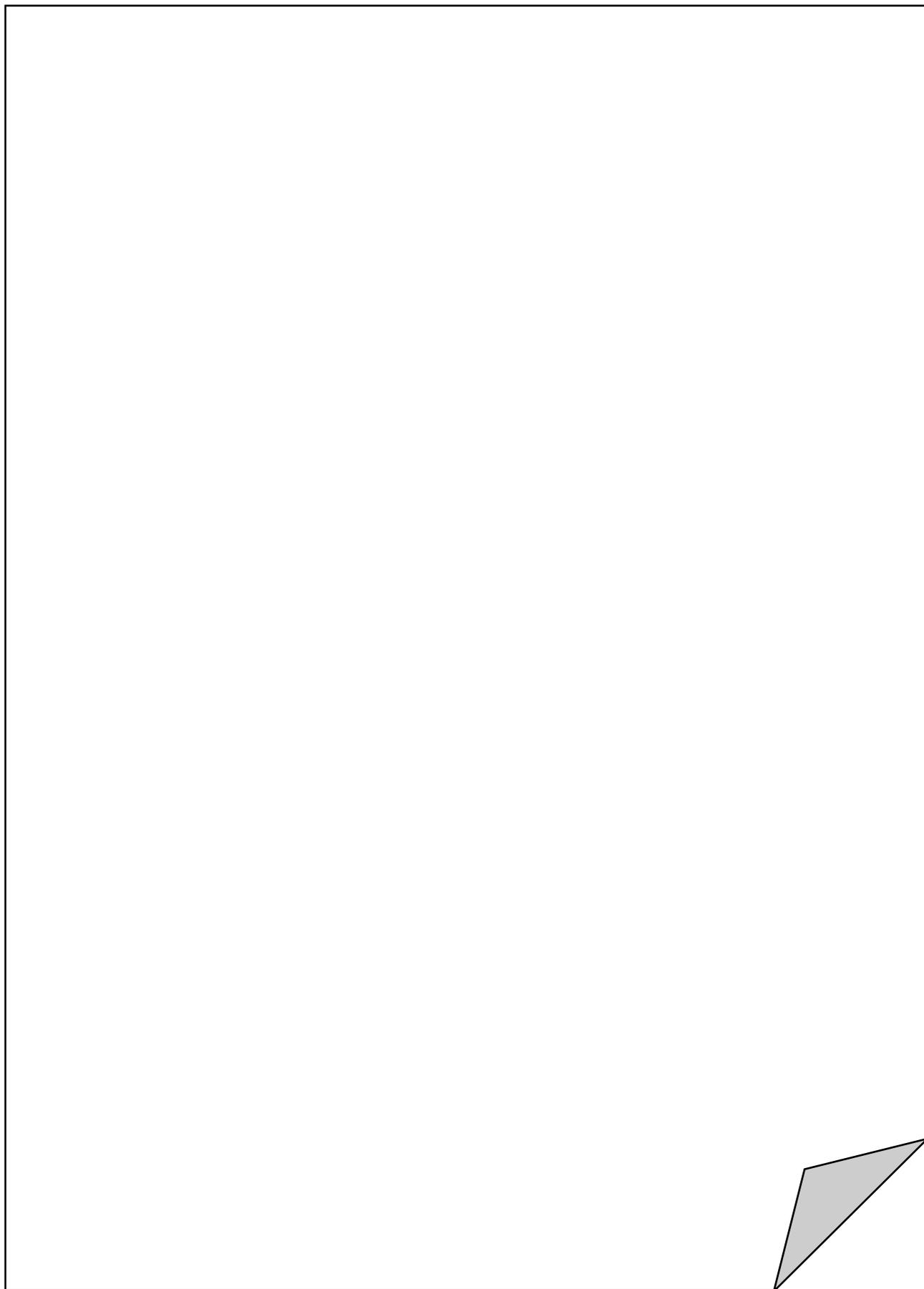
ЧЕЧУЛИН
Андрей Алексеевич

кандидат технических наук, доцент, ведущий научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
 <https://orcid.org/0000-0001-7056-6972>

Автор сообщает об отсутствии конфликтов интересов.

The author declares no conflicts of interests.

ДЛЯ ЗАМЕТОК



План издания научной литературы 2024 г., п. 7

Усл.-печ. л.
16,0

Формат
60×84_{1/8}

Заказ
№ 1603

Учредитель и издатель:

Федеральное государственное бюджетное образовательное учреждение
высшего образования "Санкт-Петербургский государственный университет
телекоммуникаций им. проф. М.А. Бонч-Бруевича"

E-mail: tuzs@sut.ru Web: tuzs.sut.ru VK: vk.com/spbtuzs

