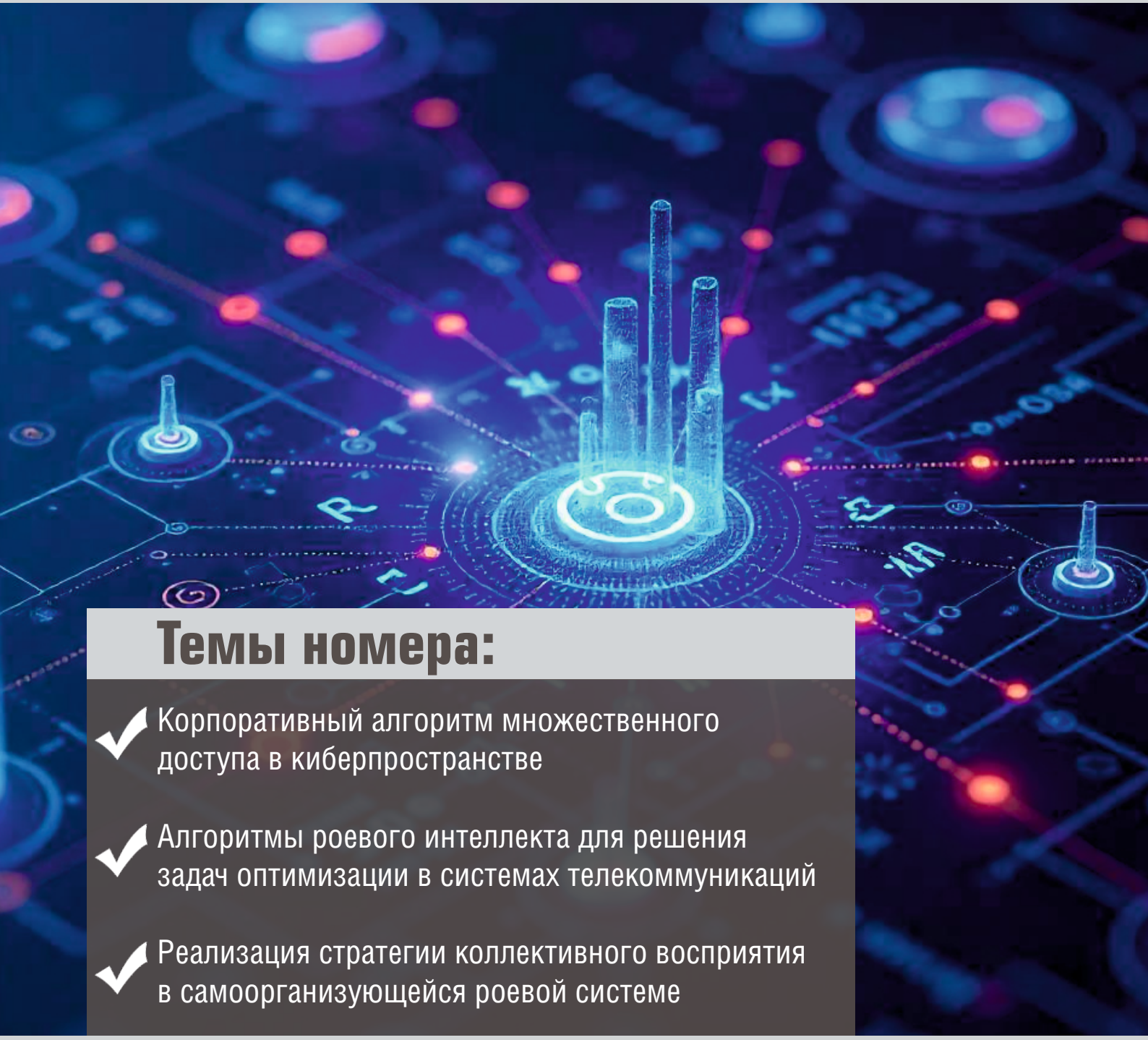
ISSN 1813-324X (Print)
ISSN 2712-8830 (Online)

ТРУДЫ УЧЕБНЫХ ЗАВЕДЕНИЙ СВЯЗИ

Том 11. № 3
2025



Темы номера:

- Корпоративный алгоритм множественного доступа в киберпространстве
- Алгоритмы роевого интеллекта для решения задач оптимизации в системах телекоммуникаций
- Реализация стратегии коллективного восприятия в самоорганизующейся роевой системе

Vol. 11. Iss. 3
2025

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 11. № 3

Proceedings of Telecommunication Universities

Vol. 11. Iss. 3

Санкт-Петербург

2025

Труды учебных заведений связи. 2025. Т. 11. № 3
ISSN 1813-324X (Print), ISSN 2712-8830 (Online)

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.

Proceedings of Telecommunication Universities. 2025. Vol. 11. Iss. 3
Trudy učebnyh zavedenij svâzi. ISSN 1813-324X (Print), ISSN 2712-8830 (Online)

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

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

E-mail: tuzs@sut.ru

Web: http://tuzs.sut.ru

ВК: http://vk.com/spbtuzs

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

E-mail: tuzs@sut.ru

Web: http://tuzs.sut.ru

Ответственный редактор **Татарникова И.М.**
Выпускающий редактор **Яшугин Д.Н.**
Дизайн: **Коровин В.М.**, изображение на обложке сгенерировано ИИ freepik https://ru.freepik.com/ai

Executive Editor **Tatarnikova I.M.**
Commissioning Editor **Yashugin D.N.**
Design: **Korovin V.M.**, cover image generated by AI freepik https://ru.freepik.com/ai

ВЫХОДНЫЕ ДАННЫЕ / IMPRINT

Дата выхода в свет: 09.07.2025
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: 07.07.2025
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

DOI:10.31854/1813-324X-2025-11-3

Обзорная статья
УДК 004.023:621.391
https://doi.org/10.31854/1813-324X-2025-11-3-7-24
EDN:JUAAMB

Алгоритмы роевого интеллекта для решения задач оптимизации в системах телекоммуникаций

Леонид Сергеевич Адонин ✉, adonin.ls@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

Актуальность. *В современном мире телекоммуникации играют критически важную роль в обеспечении цифровой экономики. Сложность и масштаб современных телекоммуникационных сетей, характеризующихся высокой динамичностью, гетерогенностью и постоянным ростом трафика, обуславливают необходимость разработки и применения эффективных методов оптимизации. Традиционные аналитические методы часто оказываются неспособными справиться с комбинаторной сложностью и нелинейностью задач, возникающих в данной области, что делает актуальным поиск альтернативных подходов. В этом контексте алгоритмы роевого интеллекта представляют собой перспективный класс методов, основанных на коллективном поведении биологических организмов и способных эффективно решать сложные задачи оптимизации.*

Целью *настоящей работы является систематизация и анализ современных исследований, посвященных применению алгоритмов роевого интеллекта в телекоммуникационных сетях. Особое внимание уделено таким методам, как алгоритм пчелиной колонии, алгоритм муравьиной колонии и алгоритм стаи серых волков, а также их модификациям. Основной задачей исследования является выявление ключевых тенденций и направлений развития эвристических алгоритмов с целью повышения производительности, надежности и устойчивости телекоммуникационных систем в условиях роста трафика и усложнения сетевых архитектур.*

Научная новизна *заключается в проведении систематического обзора современных публикаций, посвященных практическому применению алгоритмов роевого интеллекта в сфере телекоммуникаций. Представлена таксономия рассматриваемых методов, а также проанализированы их основные принципы функционирования и эффективность при решении специфических задач оптимизации в данной предметной области. Особый акцент сделан на адаптации и гибридизации алгоритмов для повышения их производительности в реальных сетевых сценариях.*

Теоретическая значимость *исследования состоит в обобщении существующего опыта применения бионспирированных методов оптимизации в телекоммуникациях, что открывает возможности для дальнейшей разработки более эффективных и масштабируемых подходов к управлению сложными динамическими системами. Полученные результаты способствуют углублению понимания потенциала алгоритмов роевого интеллекта в решении задач маршрутизации, распределения ресурсов, планирования сетей и других проблем, характерных для современной цифровой экономики.*

Ключевые слова: *оптимизация систем телекоммуникаций, метаэвристические методы, роевой интеллект, ABC, ACO, GWO*

Ссылка для цитирования: Адонин Л.С., Владыко А.Г. Алгоритмы роевого интеллекта для решения задач оптимизации в системах телекоммуникаций // Труды учебных заведений связи. 2025. Т. 11. № 3. С. 7–24. DOI:10.31854/1813-324X-2025-11-3-7-24. EDN:JUAAMB

Review research
https://doi.org/10.31854/1813-324X-2025-11-3-7-24
EDN:JUAAMB

Swarm Intelligence Algorithms for Solving Optimization Problems in Telecommunication Systems

Leonid S. Adonin ✉, adonin.ls@sut.ru
Andrey G. Vladyko, vladyko@sut.ru

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

Annotation

Relevance. *In the modern world, telecommunications play a critically important role in supporting the digital economy. The complexity and scale of contemporary telecommunication networks – characterized by high dynamism, heterogeneity, and continuously growing traffic – necessitate the development and application of efficient optimization methods. Traditional analytical approaches often prove inadequate in addressing the combinatorial complexity and nonlinearity of problems arising in this domain, making the search for alternative solutions increasingly relevant. In this context, swarm intelligence algorithms represent a promising class of methods inspired by the collective behavior of biological organisms, capable of effectively solving complex optimization tasks.*

The aim of this study *is to systematize and analyze current research devoted to the application of swarm intelligence algorithms in telecommunication networks. Particular attention is given to such methods as the Artificial Bee Colony (ABC) algorithm, Ant Colony Optimization (ACO), and the Grey Wolf Optimizer (GWO), as well as their modifications. The main objective of the research is to identify key trends and development directions of heuristic algorithms aimed at enhancing the performance, reliability, and resilience of telecommunication systems under increasing traffic loads and evolving network architectures.*

Scientific novelty *lies in conducting a systematic review of recent publications focusing on the practical application of swarm intelligence algorithms in the field of telecommunications. A taxonomy of the considered methods is presented, and their core operational principles and effectiveness in solving specific optimization problems within this domain are analyzed. Special emphasis is placed on the adaptation and hybridization of algorithms to improve their performance in real-world network scenarios.*

The theoretical significance *of the study consists in summarizing existing practices of applying bio-inspired optimization techniques in telecommunications, thereby opening up opportunities for further development of more efficient and scalable approaches to managing complex dynamic systems. The obtained results contribute to a deeper understanding of the potential of swarm intelligence algorithms in solving routing, resource allocation, network planning, and other critical problems typical of the modern digital economy.*

Keywords: *telecommunication system optimization, metaheuristic algorithms, swarm intelligence, ABC, ACO, GWO*

For citation: Adonin L.S., Vladyko A.G. Swarm Intelligence Algorithms for Solving Optimization Problems in Telecommunication Systems. *Proceedings of Telecommunication Universities.* 2025;11(3):7–24. (in Russ.) DOI:10.31854/1813-324X-2025-11-3-7-24. EDN:JUAAMB

Введение

Современные телекоммуникационные системы при переходе к сетям следующего поколения отличаются сложной архитектурой, высокой скоростью обработки данных, ультранизкой задержкой и необходимостью автоматизации ключевых процессов, таких как маршрутизация, управление сетью, обеспечение качества обслуживания (QoS, *аббр. от англ.* Quality of Service) и спектроселективное декодирование [1]. В связи с возрастанием масштабов и динамичности задач классические методы оптимизации становятся неэффективными из-за значи-

тельных вычислительных затрат. В таких условиях широкое применение находят метаэвристические алгоритмы, позволяющие получать приемлемые решения за относительно короткое время [2].

Биоинспирированные методы продемонстрировали высокую эффективность при решении сложных задач оптимизации в различных областях, включая телекоммуникации (таблица 1). Среди наиболее популярных метаэвристических алгоритмов, применяемых в данной области, следует выделить метод оптимизации роя частиц (PSO, *аббр. от англ.* Particle Swarm Optimization), моделирующий социальное поведение птиц и рыб [3–5]. Также широкое распространение получил алгоритм оптимизации стаи сальп (SSO, *аббр. от англ.* Salp Swarm Optimization), осуществляющий поиск оптимальных решений за счет параллельного исследования пространства решений посредством популяции агентов. Данный алгоритм использует стратегии межагентного взаимодействия для нахождения глобального экстремума и часто превосходит другие методы по скорости сходимости и качеству получаемых решений [6].

Не менее востребованными остаются генетический алгоритм (GA, *аббр. от англ.* Genetic Algorithm), воспроизводящий принципы естественного отбора, и дифференциальная эволюция (DE, *аббр. от англ. Differential Evolution*), основанная на механизмах природной эволюции [7, 8]. К числу перспективных подходов относятся также алгоритм оптимизации кормления бактерий (BFO, *аббр. от англ.* Bacterial Foraging Optimization) и алгоритм летучих мышей (BA, *аббр. от англ.* Bat Algorithm), которые имитируют соответственно поведение бактерий при поиске пищи и эхолокационные навыки летучих мышей [7, 9]. Перечисленные алгоритмы успешно применяются в различных предметных областях, демонстрируя высокую универсальность и эффективность при решении задач оптимизации [8, 10] (см. таблицу 1). Для выбора наиболее подходящего метода необходимо проведение сравнительного анализа по таким критериям, как скорость сходимости, точность решения и адаптивность к изменяющимся условиям [2, 3, 11].

В рамках настоящего исследования рассматриваются три наиболее часто применяемых роевых алгоритма:

– пчелиной семьи (ABC, *аббр. от англ.* Artificial Bee Colony);

– муравьиной колонии (ACO, *аббр. от англ.* Ant Colony Optimization);

– стаи серых волков (GWO, *аббр. от англ.* Grey Wolf Optimizer).

ТАБЛИЦА 1. Разнообразие метавристических алгоритмов и область их применения

TABLE 1. Diversity of Metaheuristic Algorithms and Their Areas of Application

Область применения	Алгоритм
Инженерное проектирование	GP, GSA, SA, WOA
Компьютерные сети и телекоммуникации	ABC, ACO, CSA, EPO, GA, GWO, MHSA, MBO, MMA, PSO, SSO
Энергетика и энергоменеджмент	BBO, CSA, FA, GWO, HHO, KHA, MFO, PSO, SSO, WOA
Анализ данных и машинное обучение	ABC, ALO, FA, GA, GSA, GOA, GWO, PSO, RIO, SA, WOA
Робототехника	GP, GSA, SA, WOA
Медицинская диагностика	ABC, ACO, BA, BMO, CSA, EPO, PBA, PSO
Информатика и другие области	BA, BBO, BNSS, DFO, ESA, FOA, LA, MPA, SHO

Список принятых сокращений:
ABC – Алгоритм пчелиного семьи (Artificial Bee Colony)
ACO – Алгоритм муравьиной колонии (Ant Colony Optimization)
ALO – Алгоритм оптимизации муравьиных львов (Ant Lion Optimizer)
BA – Алгоритм летучих мышей (Bat Algorithm)
BBO – Биогеографическая оптимизация (Biogeography-Based Optimization)
BNSS – Алгоритм поиска с новой стратегией обновления решений (Backtracking Search Algorithm with Novel Solution Updating Strategy)
BMO – Оптимизация на основе броуновского движения (Brownian Motion Optimization)
CSA – Алгоритм поиска кукушки (Cuckoo Search Algorithm)
DFO – Дифференциальная оптимизация опыления цветов (Differential Flower Pollination Optimization)
EPO – Улучшенный алгоритм роя частиц (Enhanced Particle Optimizer)
ESA – Эволюционный поисковый алгоритм (Evolutionary Search Algorithm)
FA – Алгоритм светлячков (Firefly Algorithm)
FOA – Алгоритм оптимизации мушек-дрозофил (Fruit Fly Optimization Algorithm)
GA – Генетический алгоритм (Genetic Algorithm)
GSA – Алгоритм гравитационного поиска (Gravitational Search Algorithm)
GOA – Алгоритм оптимизации саранчи (Grasshopper Optimisation Algorithm)
GP – Генетическое программирование (Genetic Programming)
GWO – Алгоритм стаи серых волков (Grey Wolf Optimizer)
HHO – Алгоритм оптимизации ястребов Харриса (Harris Hawks Optimization)
KHA – Алгоритм стада криля (Krill Herd Algorithm)
LA – Алгоритм лиги чемпионатов (League Championship Algorithm)
MFO – Алгоритм оптимизации молей и пламени (Moth-Flame Optimization)
MHSA – Многоуниверсальный гармонический поиск (Multi-Verse Harmony Search Algorithm)
MMA – Метод движущихся асимптот (Method of Moving Asymptotes)
MPA – Алгоритм морских хищников (Marine Predators Algorithm)
PBA – Политический алгоритм оптимизации / Парламентский алгоритм (Political/Parliamentary Optimization Algorithm)
PSO – Алгоритм роя частиц (Particle Swarm Optimization)
RIO – Алгоритм оптимизации на основе поведения крыс (Rat-Inspired Optimization)
SA – Имитация отжига (Simulated Annealing)
SHO – Алгоритм прыгающих лягушек (Shuffled Frog Leaping Algorithm)
SSO – Алгоритм социальных пауков (Social Spider Optimization)
WOA – Алгоритм оптимизации китов (Whale Optimization Algorithm)

Алгоритм ABC, вдохновленный поведением медоносных пчел, характеризуется простотой реализации и применимостью к задачам машинного обучения и управления технологическими процессами. Однако он может сталкиваться с проблемами замедленной сходимости и недостаточной точности [12]. Алгоритм ACO, основанный на механизме феромонных троп, хорошо зарекомендовал себя при решении задач дискретной оптимизации, особенно в области маршрутизации и планирования [2]. Алгоритм GWO, моделирующий социальную иерархию и охотничьи стратегии серых волков, отличается высокой скоростью сходимости и точностью, но склонен к преждевременной сходимости и снижению разнообразия популяции [13]. Современные модификации, включая многоступенчатые стратегии адаптивного поиска, способствуют повышению его устойчивости к попаданию в локальные оптимумы и расширению диапазона практического применения.

В работе рассматриваются теоретические основы указанных алгоритмов, их адаптация к специфике задач телекоммуникационных систем, а также результаты экспериментальных исследований, представленных в научной литературе. Особое внимание уделено анализу эффективности, устойчивости и масштабируемости алгоритмов.

Теоретические основы роевых алгоритмов

Теоретические основы роевых алгоритмов базируются на принципах коллективного интеллекта и самоорганизации, позволяющих решать сложные оптимизационные задачи за счет взаимодействия множества простых агентов. Эти алгоритмы имитируют природные явления, такие как поведение стай птиц, координация рыб или социальное взаимодействие насекомых, что обеспечивает эффективное исследование пространства решений в условиях высокой размерности и неопределенности [14, 15].

Одним из ключевых представителей данного класса является алгоритм PSO, который получил широкое распространение благодаря вычислительной простоте и быстрой конвергенции. Однако его использование ограничено риском попадания в локальные оптимумы и преждевременной конвергенцией. Для преодоления этих недостатков разработаны усовершенствованные версии, включающие механизмы адаптивного отбора лидерских качеств и полеты Леви [16, 17].

Общими характеристиками роевых алгоритмов являются децентрализованное управление, параллельная обработка информации и использование простых правил локального взаимодействия между агентами. Эти свойства обеспечивают высокую устойчивость к локальным оптимумам и позволяют эффективно работать в условиях неполной информации и динамической изменчивости среды [18, 19]. Благодаря своей гибкости и адаптивности данные алгоритмы находят применение в различных областях, включая телекоммуникации, робототехнику, логистику, мониторинг окружающей среды и планирование маршрутов [19, 20].

Среди наиболее известных роевых алгоритмов выделяются ABC, ACO и GWO. Алгоритм ABC моделирует поведение медоносных пчел при поиске пищи, эффективно балансируя между разведкой новых источников и эксплуатацией известных. ACO основывается на механизме феромонных троп муравьев, что позволяет находить оптимальные пути в сложных пространствах решений [21]. GWO имитирует социальную иерархию и охотничье поведение серых волков, демонстрируя высокую скорость и точность конвергенции. Современные модификации GWO направлены на решение проблем преждевременной конвергенции и локальной оптимизации [22, 23].

ABC предложен Д. Карабогой в 2005 г. [24]. Несмотря на свою эффективность в задачах непрерывной оптимизации, алгоритм сталкивается с проблемами слабого локального поиска и преждевременной конвергенции. Для улучшения его производительности были разработаны модификации, такие как использование *k*-средних для кластеризации и хаотического поиска [25].

ACO, разработанный М. Дориго в начале 1990-х годов [26], основывается на механизме отложения феромонов. Искусственные муравьи строят решения, выделяя феромоны, что создает положительную обратную связь и направляет поиск к оптимальным решениям [27]. Эффективность ACO может быть дополнительно повышена за счет корректировки численности популяции муравьев [28].

GWO моделирует социальную иерархию и охотничье поведение серых волков. Современные модификации, такие как ATgWO и EGWO, улучшают исследование пространства решений за счет адаптивного взвешивания лидеров и инновационных стратегий обновления позиций [29].

Все три алгоритма демонстрируют различный баланс между исследованием новых решений и эксплуатацией известных. ABC использует вероятностный выбор и случайный поиск, ACO – следы феромонов и эвристическую информацию, а GWO – социальную иерархию и координированное перемещение агентов [12]. Это позволяет преодолевать локальные оптимумы, что является ключевой задачей в сложных задачах оптимизации [30].

Вычислительная сложность рассматриваемых алгоритмов находится в полиномиальных пределах, что делает их применимыми к реальным задачам [31]. Их адаптация для параллельных вычисле-

ний обеспечивает значительное ускорение и масштабируемость [32]. Параметрическая настройка играет важную роль в оптимизации производительности каждого алгоритма [33].

Сравнительный анализ показывает, что ACO эффективен для маршрутизации и планирования путей, но чувствителен к коэффициенту испарения феромонов, веса эвристической информации и интенсивности откладывания феромонов [34]. GWO отличается быстрой сходимостью, но склонен к преждевременной конвергенции [35]. ABC хорошо работает с непрерывными функциями, но менее эффективен в дискретных задачах [35].

Важной особенностью всех трех алгоритмов является их способность к адаптации. Современные модификации значительно расширяют их возможности, подчеркивая актуальность и перспективность использования метаэвристических алгоритмов в современных приложениях [36].

Анализ практической реализации алгоритмов

Все три алгоритма, ABC, ACO и GWO, реализуют общую стратегию итеративного улучшения решений без использования градиентной информации, полагаясь на коллективное поведение агентов для исследования и эксплуатации пространства решений. Несмотря на общую цель – нахождение глобального оптимума посредством коллективного поиска – алгоритмы ABC, ACO и GWO демонстрируют принципиальные отличия в операторе обновления решений, стратегии обмена информацией между агентами и в методах балансировки разведки и эксплуатации, что определяет их относительную эффективность при решении различных классов оптимизационных задач. Эти различия, подкрепленные соответствующими математическими моделями и эмпирическими исследованиями, позволяют исследователям и практикам делать обоснованный выбор методологии в зависимости от конкретных требований задачи и вычислительных ограничений [37–39].

Алгоритм ABC использует схему трех фаз, которая сочетает локальный поиск (с помощью операций обновления решений в фазе рабочих) с глобальным поиском, осуществляемым фуражирами. Основные преимущества ABC заключаются в простоте реализации, относительно небольшом количестве параметров для настройки и способности избегать преждевременной сходимости за счет случайного поиска новых решений.

Математически обновление решения представлено формулой:

$$x_{ij}(t+1) = x_{ij}(t) + \varphi_{ij}\left[x_{ij}(t) - x_{kj}(t)\right], \qquad (1)$$

где $x_{ij}(t)$ – j-я компонента i-го решения в итерации t; $x_{kj}(t)$ – случайно выбранное значение из другой позиции; φ_{ij} – случайный коэффициент, равномерно распределенный в промежутке [–1, 1].

Алгоритм реализует дифференциальную эволюцию решения через интеграцию случайных компонент [40]. Тем не менее, алгоритм ABC может быть менее эффективным при высоких размерностях, поскольку точная эксплуатация локальных оптимумов требует значительного числа итераций – данное ограничение характерно для его применения в задачах непрерывной оптимизации и комбинаторных задачах, таких как задача коммивояжера [37].

В свою очередь, алгоритм ACO отличается явной зависимостью от истории поиска, которая кодируется в виде следов феромонов.

Вероятностное правило выбора компонента решения выражается формулой:

$$p_{ij}^{k}(t) = \left[\tau_{ij}(t)\right]^{\alpha} \cdot \left[\eta_{ij}(t)\right]^{\beta} / \Sigma_{\text{l}} \in \\ \in J_k(i)[\tau_{il}(t)]^{\alpha} \cdot [\eta_{il}(t)]^{\beta}, \qquad (2)$$

где $\tau_{ij}(t)$ – концентрация феромона на ребре между городами i и j в момент времени t; $\eta_{ij}(t)$ – эвристическая информация, часто обратная расстоянию между i и j; α и β – параметры, определяющие относительную значимость феромона и эвристики; $J_k(i)$ – множество доступных вершин для муравья k, находящегося в вершине i [38].

Правило выбора демонстрирует, каким образом интенсивность феромона и эвристическая информация (например, обратное расстояние) комбинируются для формирования оптимальных маршрутов [38].

В дополнение к этому ключевую роль играет механизм испарения феромона, описываемый уравнением:

$$\tau_{ij}(t+1) = (1-\rho) \cdot \tau_{ij}(t) + \Delta\tau_{ij}, \qquad (3)$$

где $\rho \in (0, 1)$ – коэффициент испарения; $\Delta\tau_{ij}$ – дополнительное количество феромона, внесенное муравьями, часто вычисляемое как сумма вкладов каждого муравья, прошедшего через ребро.

Эта процедура (3) позволяет усилить те компоненты решений, которые ведут к построению качественных маршрутов, и одновременно снижать влияние менее оптимальных путей.

ACO особенно эффективен в решении дискретных задач оптимизации, где представление решения естественным образом соответствует графовой модели, однако из-за своей вычислительной сложности и зависимости от обновления феромонов его реализация может быть затруднена для задач с большим числом вершин или переменных. Алгоритм GWO, напротив, опирается на модель социальной и охотничьей динамики стаи, где лучшие решения играют роль лидеров.

Основное уравнение обновления позиции:

$$X(t+1) = X(t) - A \cdot D, \qquad (4)$$

где $X(t)$ – текущая позиция волка в итерации t; $D = C \cdot X_{\text{р}} - X(t) \vee$ – расстояние до «добычи» (или лучшего решения $X_{\text{р}}$); коэффициенты A и C рассчитываются по выражению:

$$A = 2a \cdot r_1 - a \text{ и } C = 2 \cdot r_2,$$

где a – параметр, уменьшающийся линейно от 2 до 0 за время работы алгоритма; r_1 и r_2 – равномерно распределенные в интервале [0, 1] случайные векторы [39, 41].

Уравнение с описанными коэффициентами A и C (4) демонстрирует, как случайные компоненты, адаптивно изменяющиеся в процессе работы, обеспечивают как глобальный, так и локальный поиск. Важным аспектом реализации GWO является линейное уменьшение параметра a, что способствует переключению алгоритма от разведки (исследования пространства) к эксплуатации (точное улучшение найденных оптимальных решений). В отличие от ABC и ACO, GWO обладает естественной способностью поддерживать баланс между диверсификацией популяции и сходимостью к оптимуму за счет многократного обновления позиций под влиянием трех лидеров стаи – альфа, бета и дельта. Это делает GWO универсальным инструментом как для непрерывных, так и для некоторого класса дискретных задач – в частности, при решении задач оптимизации в энергетических системах, управления или проектирования [42].

Таким образом каждый из них реализует уникальный подход к балансировке разведки и эксплуатации: ABC использует простую схему случайного поиска с фазами локального и глобального улучшения, ACO полагается на феромонные следы и вероятностный выбор решений, особенно эффективно в дискретных задачах, а GWO моделирует социальную иерархию и охотничью динамику, обеспечивая хороший баланс между исследованием и сходимостью. Эти различия в стратегиях и математических моделях обуславливают специфические сильные стороны и ограничения каждого алгоритма, что позволяет выбирать наиболее подходящий метод в зависимости от типа задачи, ее размерности и вычислительных требований.

Применение роевых алгоритмов в системах телекоммуникаций

Роевые алгоритмы получили широкое распространение в решении задач, связанных с управлением и оптимизацией в телекоммуникациях. Их способность эффективно работать с большими объемами данных и адаптироваться к динамически изменяющимся условиям делает их незаменимыми для современных сетей [43].

Особого внимания заслуживает применение ACO для оптимизации маршрутизации. Этот алгоритм демонстрирует высокую эффективность за счет имитации феромонных механизмов, что позволяет улучшить ключевые метрики производительности, включая коэффициент доставки пакетов и пропускную способность [44]. Модифицированный подход на основе алгоритма муравьиной колонии (MACO, *аббр. от англ.* Modified ACO), учитывающий текущее состояние сети, обеспечивает повышение пропускной способности и снижение задержек [45]. Гибридные модели, интегрирующие ACO с методами машинного обучения, показали значительный потенциал в беспроводных сенсорных сетях, где они способствуют снижению энергопотребления [46].

Алгоритм ABC также зарекомендовал себя как эффективный инструмент многоцелевой оптимизации. Он успешно применяется для минимизации задержек и энергопотребления в программно-определяемых сетях, где улучшает параметры QoS [47]. В логистических приложениях ABC обеспечивает маршрутизацию с учетом специфических ограничений, например – температурного режима [48].

Значительный вклад в развитие сетей 5G внес адаптированный GWO, который успешно решает задачи маршрутизации с учетом требований QoS [49]. Интеграция этого алгоритма с традиционными протоколами позволяет осуществлять динамическую корректировку трафика в реальном времени [50].

Интеллектуальные электросети, интегрирующие датчики, умные счетчики и устройства интернета вещей (IoT, *аббр. от англ.* Internet of Things), сталкиваются с необходимостью обработки больших объемов данных в реальном времени. Традиционные облачные системы не всегда справляются с высокой нагрузкой, что снижает QoS. В интересах минимизации задержки и повышения эффективности обработки запросов в [51] была предложена гибридная архитектура «облако–туман», обеспечивающая трехуровневое распределение вычислений между пользователями, туманными узлами и облаком. В модели применяются как стандартные алгоритмы (Round Robin, Throttled), так и биовдохновленные методы: PSO, ACO, ABC и их гибриды, например, гибридный и адаптивный вариант алгоритма муравьиных колоний (HABACO, *аббр. от англ.* Hybrid Adaptive Binary Ant Colony Optimization), способный избегать локальных оптимумов и предназначенный для решения задач оптимизации в бинарном пространстве. Эффективность подхода подтверждена симуляциями и многими исследованиями [52–55].

Гибридная архитектура предусматривает разделение функций: на уровне пользователей собираются данные, туманные узлы выполняют предва-

рительную обработку, а облако – глубокий анализ и управление ресурсами. Особое внимание уделено алгоритму HABACO, который объединяет ABC и ACO для более точного распределения задач. Симуляции показали снижение времени отклика до 60–90 % по сравнению с PSO и ACO, при этом общие затраты на вычисления остаются оптимальными даже при увеличении числа виртуальных машин. Полученные результаты согласуются с выводами других исследований [54–56]. Для практического внедрения требуется разработка прототипов и интеграция с технологиями безопасности. Представленная методология открывает возможности для повышения энергоэффективности и надежности умных сетей будущего.

В области распределения ресурсов роевые алгоритмы демонстрируют высокую эффективность. ABC повышает спектральную эффективность в мобильных сетях, а ACO используется для оптимизации распределения электроэнергии в радиосистемах [45]. Особое место занимает GWO, который успешно справляется с ограничениями, связанными с полосой пропускания и энергопотреблением [57]. Управление спектром становится все более актуальным в условиях развития технологий 5G и IoT. ABC эффективно решает задачи динамического распределения спектра между операторами связи [58], а ACO оптимизирует частотное планирование в сотовых сетях. Интеграция методов искусственного интеллекта в управление спектром позволяет осуществлять его динамическую корректировку [59].

Энергоэффективное планирование является важным аспектом современных телекоммуникаций. Алгоритмы ABC и ACO позволяют оптимизировать работу базовых станций и маршруты передачи данных, что приводит к значительной экономии энергии. Разработка систем управления энергопотреблением для базовых станций способствует снижению зависимости от электросети. В сфере безопасности телекоммуникационных сетей роевые алгоритмы находят применение в различных задачах. ACO успешно используется для оптимизации систем шифрования, GWO демонстрирует высокую точность в выявлении аномалий сетевого трафика [60], а ABC оптимизирует стратегии распределения спектра [61].

Интеграция различных роевых алгоритмов открывает новые возможности для решения сложных задач в SDN (*аббр. от англ.* Software-Defined Networking) и IoT. Гибридные подходы, сочетающие ABC и ACO, эффективно решают проблемы размещения контроллеров [62], а комбинация GWO и ABC обеспечивает энергоэффективную маршрутизацию [63].

Адаптация алгоритмов роя к динамическим условиям современных сетей подтверждает их универсальность. MACO демонстрирует высокую эффективность в управлении маршрутизацией [45], модификации ACO успешно решают задачи многокритериальной оптимизации [64], а GWO показывает отличные результаты в распределенных системах [63]. Синергия роевых алгоритмов с методами машинного обучения создает основу для развития интеллектуальных систем управления. ACO эффективно применяется для динамического распределения полосы пропускания [65], GWO оптимизирует параметры нейронных сетей [66], а методы роевого обучения находят применение в интеллектуальных транспортных системах [67].

Таким образом все рассмотренные роевые алгоритмы демонстрируют высокую эффективность при решении широкого круга задач в телекоммуникациях – от маршрутизации и распределения ресурсов до обеспечения безопасности и энергоэффективности. Их способность адаптироваться к динамически изменяющимся условиям, работать с большими объемами данных и находить компромисс между разведкой и эксплуатацией делает их ценным инструментом в управлении современными сетями, особенно в условиях развития SDN, IoT и технологий 5G. Интеграция этих алгоритмов с методами машинного обучения и гибридные подходы открывают новые перспективы для построения интеллектуальных, самонастраивающихся систем связи.

Сравнительный анализ эффективности алгоритмов

Сравнительный анализ эффективности алгоритмов оптимизации в телекоммуникациях выполнен на основе обзора существующих исследований и публикаций, в которых использовались как тестовые функции, так и практические задачи из области связи. Оценка осуществлялась по ключевым критериям: скорость сходимости, точность решений, вычислительная сложность, устойчивость к локальным оптимумам и способность обработки ограничений.

Оптимизатор GWO демонстрирует наиболее высокую скорость конвергенции среди рассматриваемых алгоритмов, достигая приемлемых решений на начальных итерациях в 42 и 58 % случаев, соответственно [66]. Однако это преимущество сопровождается риском преждевременной конвергенции, что может привести к снижению разнообразия популяций [9, 68]. В отличие от GWO, алгоритм ABC характеризуется более стабильной конвергенцией на поздних этапах оптимизации, что обеспечивает эффективное решение задач с многочисленными локальными оптимумами [66]. Современные модификации GWO направлены на преодоление указанных ограничений за счет интеграции адаптивных стратегий и гибридных подходов [69, 70].

При оценке точности алгоритмов ABC показал наилучший результат – 97,3 %, особенно эффективен в непрерывных пространствах решений. ACO достиг точности 95,8 % и продемонстрировал преимущества в дискретных задачах [71]. GWO занял промежуточное положение с точностью 96,5 %, сохраняя стабильную производительность в обоих типах задач [72]. Универсальность ABC особенно заметна при решении нелинейных задач в энергосистемах [73]. Сравнительные характеристики рассмотренных алгоритмов обобщены в таблице 2.

Анализ вычислительной сложности выявил значительные различия между алгоритмами. ABC характеризуется минимальной сложностью $O(n^2)$, что делает его применимым в различных областях, включая энергосистемы и беспроводные сенсорные сети [73, 74]. ACO имеет более высокую временну́ю сложность $O(n^3)$ из-за необходимости поддержания матрицы феромонов, что увеличивает использование памяти [10]. GWO занимает промежуточное положение с сложностью $O(n^2 \log n)$, балансируя между производительностью и потреблением ресурсов [75] (см. таблицу 2).

В контексте способности к преодолению локальных оптимумов ABC достигает глобального оптимума в 87 % случаев, опережая GWO (82 %) и ACO (76 %) [76] (см. таблицу 2). При этом ACO демонстрирует наилучшие результаты в выполнении ограничений, находя допустимые решения в 92 % случаев [35, 77]. Статистический анализ методом ANOVA ($p < 0,05$) подтвердил стабильность ABC, который показал коэффициент вариации 12,3 % по сравнению с 15,8 % для ACO и 14,2 % для GWO [73, 78]. Эта характеристика особенно важна для приложений, требующих надежных решений.

Практическое применение алгоритмов в задачах *маршрутизации* показало, что ABC обеспечивает минимальную задержку (12,3 мс), опережая ACO (14,2 мс) и GWO (13,1 мс) [79]. Однако ACO демонстрирует лучшую балансировку нагрузки с коэффициентом вариации 0,15 против 0,21 для ABC и 0,18 для GWO [45, 79]. В задачах *энергоэффективного планирования* GWO достиг наибольшего значения целевой функции (0,87), превышая показатели ABC (0,82) и ACO (0,84) [80, 81]. Тем не менее, ABC проявил большую стабильность энергопотребления в динамичных сетевых условиях. Метод анализа иерархий подтвердил *приоритеты* алгоритмов: ABC получил вес 0,38; GWO – 0,35; ACO – 0,27 [82, 83]. ABC и GWO характеризуются высокой универсальностью, тогда как ACO наиболее эффективен в специализированных сценариях с элементами неопределенности [84]. Результаты подчеркивают необходимость учета контекста применения при выборе алгоритма оптимизации.

ТАБЛИЦА 2. Сравнительные характеристики роевых алгоритмов

TABLE 2. Comparative Characteristics of Swarm Intelligence Algorithms

Характеристика (показатель)	ABC	ACO	GWO	*R*
Скорость сходимости	Умеренная	Умеренная	Высокая	[58]
Точность решения	97,3 %	95,8 %	96,5 %	[63], [64]
Вычислительная сложность	$O(n^2)$	$O(n^3)$	$O(n^2 \log n)$	[66]
Устойчивость к локальным оптимумам	Высокая (87 %)	Средняя (76 %)	Средняя (82 %)	[67], [68]
Разнообразие популяций	Высокое	Среднее	Низкое	[60]
Пригодность для непрерывных задач	Отличная	Средняя	Хорошая	[65], [64]
Пригодность для дискретных задач	Средняя	Отличная	Хорошая	[63], [64]
Применение в маршрутизации	Эффективен (минимизация задержек)	Высокоэффективен (особенно в беспроводных сетях)	Хорошо работает (учитывает требования QoS)	[37]
Применение в задачах разгрузки трафика, балансировки нагрузки	Оптимизация нагрузки на серверы	Маршрутизация трафика по сети	Балансировка ресурсов в сетях	[69], [70]
Энергоэффективность	Высокая (экономия до 20 МВт/год)	Средняя	Высокая (в облачных сетях)	[71]
Спектральная эффективность	Высокая	Средняя	Средняя	[49]
Обработка ограничений	Хорошая (85 %)	Отличная (92 %)	Хорошая (88 %)	[72], [27]
Коэффициент вариации	Низкий (12,3 %)	Средний (15,8 %)	Средний (14,2 %)	[65], [73]
Сложность реализации	Простая	Средняя	Простая	[3], [74]
Использование памяти	Низкое	Высокое	Среднее	[3], [74]
Гибридизация	Возможна (с машинным обучением)	Возможна (с генетическими алгоритмами)	Возможна (с адаптивными стратегиями)	[61]
Применение в 5G	Умеренное	Высокое	Высокое	[41], [55]
Безопасность	Средняя	Высокая	Высокая	[52]
Универсальность	Высокая	Средняя	Высокая	[76]

Усл. обозначения:

R – Источник

Таким образом, алгоритмы ABC, ACO и GWO находят применение соответственно в непрерывных задачах и энергоэффективности, маршрутизации и задачах с ограничениями, а также в обеспечении высокой скорости сходимости и QoS [26, 28].

Перспективы развития и гибридизация алгоритмов

Перспективы развития и гибридизация алгоритмов роевого интеллекта представляют собой одно из ключевых направлений современных исследований в области оптимизации телекоммуникационных систем. Анализ актуальных научных разработок позволяет выделить несколько основных трендов, характеризующих эволюцию данных алгоритмов.

В первую очередь, значительное внимание уделяется интеграции роевых алгоритмов с технологиями машинного обучения. Так, сочетание ABC с глубокими нейронными сетями демонстрирует повышенную эффективность в задачах прогнозирования сетевого трафика и маршрутизации [85–87]. Особую значимость приобретает разработка адаптивных систем роевого интеллекта для обработки больших данных, где нейросетевые подходы обеспечивают улучшение поисковых механизмов.

Комбинирование ABC и ACO показывает синергетический эффект благодаря механизму памяти ACO, что приводит к повышению производительности на 15–20 % [88]. Интеграция GWO с генетическими алгоритмами способствует увеличению разнообразия популяций и предотвращению преждевременной конвергенции. Особенно перспективным представляется сочетание алгоритмов Honey Badger (HBA) и оптимизации роя песчаных кошек (SCSO), демонстрирующее высокие результаты в глобальной оптимизации [89].

Значительный прогресс наблюдается в области самоадаптации параметров алгоритмов. В контексте GWO разработаны стратегии динамической адаптации, позволяющие регулировать такие параметры как частота мутаций в зависимости от характеристик пространства решений [90, 91]. Адаптивный динамический алгоритм самообучающейся оптимизации серых волков (ASGWO, *аббр. от англ.* Adaptive Dynamic Self-Learning Grey Wolf Optimization Algorithm) включает инновационные механизмы обновления позиций, что существенно повышает скорость и точность конвергенции [92].

Интеграция с блокчейн-технологиями открывает новые возможности для децентрализованного управления ресурсами. Концепция Swarm Intelligence демонстрирует высокую адаптивность в динамичных приложениях, а двухфакторный блокчейн-консенсус обеспечивает защиту коммуникационных каналов [93]. Появление технологии Swarm Contracts позволяет минимизировать зависимость от централизованных систем управления [94].

Особого внимания заслуживает внедрение квантовых вычислений в роевые алгоритмы. QACO (*аббр. от англ.* Quantum Ant Colony Algorithm) и QPSO (*аббр. от англ.* Quantum Particle Swarm Optimization) демонстрируют значительное улучшение скорости конвергенции и качества решений [95], что подтверждает перспективность данного направления. Развитие механизмов коллективного обучения также представляет собой важный аспект модернизации алгоритмов роя. Системы, основанные на обмене опытом между агентами, показывают высокую эффективность в сложных задачах оптимизации [2, 48]. Внедрение справедливых механизмов вознаграждения стимулирует участие ресурсоемких организаций в процессе коллективного обучения [96].

Интеграция с технологиями цифровых двойников значительно расширяет возможности оптимизации телекоммуникационных сетей. Комбинация GWO с цифровыми двойниками обеспечивает точное моделирование сетевых элементов и прогнозирование операционных проблем. Платформы типа GH-Twin, использующие обучение графам, предоставляют надежные инструменты самовосстановления [97].

Заключение

На основе проведенного анализа представляется возможным сделать вывод о том, что каждый из рассмотренных роевых алгоритмов характеризуется уникальными особенностями, делающими их пригодными для решения различных задач в сфере телекоммуникаций. ABC демонстрирует наилучшие показатели общей производительности и стабильности при решении задач непрерывной оптимизации, особенно в условиях наличия множества локальных оптимумов. ACO остается незаменимым инструментом для задач маршрутизации и планирования с жесткими ограничениями, тогда как GWO проявляет высокую эффективность в задачах с множественными критериями оптимизации, где требуется быстрая сходимость.

Для задач, связанных с энергоэффективным планированием и оптимизацией спектральных ресурсов, рекомендуется применять алгоритм ABC благодаря его точности и стабильности. В задачах маршрутизации и распределения ресурсов с жесткими ограничениями предпочтение следует отдавать ACO, обладающему эффективным механизмом работы с ограничениями. GWO наиболее подходит для задач реального времени, таких как выгрузка трафика, где требуется оперативная сходимость при сохранении приемлемой точности решения.

Перспективы дальнейших исследований в данной области должны быть направлены на развитие гибридных подходов, сочетающих сильные стороны различных алгоритмов. Особое внимание следует уделить разработке механизмов самоадаптации параметров и созданию распределенных версий алгоритмов для их применения в крупно-

масштабных телекоммуникационных сетях. Интеграция роевых алгоритмов с технологиями машинного обучения и цифровых двойников также представляет собой перспективное направление, способствующее созданию интеллектуальных систем управления сетью.

Важным аспектом будущих исследований является разработка методов оценки и сравнения эффективности роевых алгоритмов в условиях динамической работы сетей связи. Необходимы дополнительные исследования по оптимизации вычислительной сложности алгоритмов при сохранении их производительности. Также представляет научный и практический интерес развитие квантовых версий роевых алгоритмов и исследование их применимости в приложениях метавселенной [98].

Список источников

1. Ateya A.A., El-Latif A.A.A., Muthanna A., Volkov A., Koucheryavy A. Enabling Metaverse and Telepresence Services in 6G Networks. NY: River Publishers, 2025. 254 p. DOI:10.1201/9788770046749

2. Zangana H.M., Sallow Z.B., Alkawaz M.H., Omar M. Unveiling the Collective Wisdom: A Review of Swarm Intelligence in Problem Solving and Optimization // Inform: Jurnal Ilmiah Bidang Teknologi Informasi Dan Komunikasi. 2024. Vol. 9. Iss. 2. PP. 101–110. DOI:10.25139/inform.v9i2.7934. EDN:WJAKIJ

3. Mao S., Hu F., Lang J., Chen T., Cheng S. Comparative Study of Impacts of Typical Bio-Inspired Optimization Algorithms on Source Inversion Performance // Frontiers in Environmental Science. 2022. Vol. 10. P. 894255. DOI:10.3389/fenvs.2022.894255

4. Duan H., Li P. Bio-inspired computation in unmanned aerial vehicles. Berlin, Heidelberg: Springer, 2014. DOI:10.1007/978-3-642-41196-0

5. Hao Z., Huang H., Cai R. Bio-inspired Algorithms for TSP and Generalized TSP // Greco F. (ed.) Traveling Salesman Problem. IntechOpen, 2008. DOI:10.5772/5583

6. Ateya A.A., Muthanna A., Vybornova A., Algarni A.D., Abuarqoub A., Koucheryavy Y., et al. Chaotic salp swarm algorithm for SDN multi-controller networks // Engineering Science and Technology, an International Journal. 2019. Vol. 22. Iss. 4. PP. 1001–1012. DOI:10.1016/j.jestch.2018.12.015. EDN:DOSQQF

7. Alanis A.Y., Arana-Daniel N., López-Franco C. Bio-inspired Algorithms // Bio-inspired Algorithms for Engineering. Elsevier, 2018. PP. 1–14. DOI:10.1016/B978-0-12-813788-8.00001-9

8. Subramanian S., Bhojaneet N., Madhnani H., Pant S., Kumar A., Kotecha K. A Comprehensive Review of Nature-Inspired Optimization Techniques and Their Varied Applications // Nature-Inspired Optimization Algorithms for Cyber-Physical Systems. IGI Global Scientific Publishing, 2025. PP. 105–174. DOI:10.4018/979-8-3693-6834-3.ch005

9. Li P., Duan H. Bio-inspired Computation Algorithms // Bio-inspired Computation in Unmanned Aerial Vehicles. Berlin, Heidelberg: Springer, 2014. PP. 35–69. DOI:10.1007/978-3-642-41196-0_2

10. Almufti M.S., Marqas R.B., Saeed V.A. Taxonomy of bio-inspired optimization algorithms // Journal of Advanced Computer Science & Technology. 2019. Vol. 8. Iss. 2. PP. 23–31. DOI:10.14419/jacst.v8i2.29402

11. Zhang Z., Xu T., Zou K., Tan S., Sun Z. Multi-Objective Grey Wolf Optimizer Based on Improved Head Wolf Selection Strategy // Proceedings of the 43rd Chinese Control Conference (CCC, Kunming, China, 28–31 July 2024). IEEE, 2024. PP. 1922–1927. DOI:10.23919/CCC63176.2024.10662658

12. Peng Q., Zhan R., Wu H., Shi M. Comparative Study of Wolf Pack Algorithm and Artificial Bee Colony Algorithm: Performance Analysis and Optimization Exploration // International Journal of Swarm Intelligence Research. 2024. Vol. 15. Iss. 1. PP. 1–24. DOI:10.4018/IJSIR.352061

13. Yang J., Gu W. A multi-stage time-backtracking grey wolf optimizer introducing a new hierarchy mechanism // Research Square. 2024. DOI:10.21203/rs.3.rs-4126903/v1

14. Zhao S. Research on the Application of Swarm Behavior to Artificial Intelligence Systems // Applied and Computational Engineering. 2025. Vol. 120. PP. 158–163. DOI:10.54254/2755-2721/2025.19403. EDN:OGCKKC

15. Tyagi N., Bhargava D., Ahlawat A. Implementation of Particle Swarm Optimization Algorithm Inspired by the Social Behaviour of Birds // Proceedings of the 4th International Conference on Technological Advancements in Computational Sciences (ICTACS, Tashkent, Uzbekistan, 13–15 November 2024). IEEE, 2024. PP. 750–754. DOI:10.1109/ICTACS62700.2024.10840529

16. Cai T., Zhang S., Ye Z., Zhou W., Wang M., He Q., Chen Z., et al. Cooperative metaheuristic algorithm for global optimization and engineering problems inspired by heterosis theory // Scientific Reports. 2024. Vol. 14. Iss. 1. P. 28876. DOI:10.1038/s41598-024-78761-0. EDN:QOGXNY

17. Wu Y., Zhu X., Zhao W., Xia X. A Novel Particle Swarm Optimization Algorithm for Meta-Heuristic Analysis Mechanism Based on Population Learning Strategies and Adaptive Selection of Leadership Particles // Proceedings of the 11th International Conference on Data Science and Advanced Analytics (DSAA, San Diego, USA, 06–10 October 2024). IEEE, 2024. PP. 1–9. DOI:10.1109/DSAA61799.2024.10722812

18. Yazıcı A.M., Ömür G.A., Celik D.A. Applications and Future Perspectives of Swarm Intelligence in Unmanned and Autonomous Systems: Innovative Conceptual Approaches to Social Sciences // Sosyal Mucit Academic Review. 2024. Vol. 5. Iss. Innovative Conceptual Approaches to Social Sciences. PP. 106–130. DOI:10.54733/smar.1555925. EDN:QUVHXT

19. Pachajoa G.M.M., Achicanoy W., Garzón Ramos D. Automating the Evaluation of the Scalability, Flexibility, and Robustness of Collective Behaviors for Robot Swarms // Proceedings of the Brazilian Symposium on Robotics (SBR) and 2024 Workshop on Robotics in Education (WRE, Goiania, Brazil, 13–15 November 2024). Piscataway: IEEE, 2024. PP. 144–149. DOI:10.1109/SBR/WRE63066.2024.10837963

20. Paköz B. Swarm Intelligence and Decentralized AI // Human Computer Interaction. 2024. Vol. 8. Iss. 1. PP. 97–100. DOI:10.62802/k7xhrd47. EDN:GLVTOB

21. Yogi M.K., Chakravarthy A.S.N. Application of Variants of Nature-Inspired Optimization for Privacy Preservation in Cyber-Physical Systems // Nature-Inspired Optimization Algorithms for Cyber-Physical Systems. IGI Global Scientific Publishing, 2025. DOI:10.4018/979-8-3693-6834-3.ch009

22. Cheng H., Zhou H., Shen Y. An improved grey wolf optimization algorithm based on bounded subpopulation re-search strategy // Journal of Physics: Conference Series. 2024. Vol. 2902. P. 012035. DOI:10.1088/1742-6596/2902/1/012035. EDN:ONSHBZ

23. Zhang J., Dai Y., Shi Q. An improved grey wolf optimization algorithm based on scale-free network topology // Heliyon. 2024. Vol. 10. Iss. 16. P. e35958. DOI:10.1016/j.heliyon.2024.e35958. EDN:VACDIH

24. Karaboga D. An idea based on honey bee swarm for numerical optimization. Technical Report-tr06. 2005. URL: https://abc.erciyes.edu.tr/pub/tr06_2005.pdf (Accessed 02.07.2025)

25. Xiao W.-S., Li G., Liu C., Tan L. A novel chaotic and neighborhood search-based artificial bee colony algorithm for solving optimization problems // Scientific Reports. 2023. Vol. 13. P. 20496. DOI:10.1038/s41598-023-44770-8. EDN:MDLWOS

26. Dorigo M., Maniezzo V., Colorni A. Ant system: An Autocatalytic Optimizing Process. 1991.

27. Misra B., Chakraborty S. Ant Colony Optimization – Recent Variants, Application and Perspectives // Dey N. (ed.) Applications of Ant Colony Optimization and its Variants: Case Studies and New Developments. Singapore: Springer Nature, 2024. PP. 1–17. DOI:10.1007/978-981-99-7227-2_1

28. Olivari L. Reducing ACO Population Size to Increase Computational Speed // Tehnički glasnik. 2024. Vol. 18. Iss. 4. PP. 532–539. DOI:10.31803/tg-20230825125127. EDN:ZSJBRX

29. Jiang H., Liu D., Liu X., Wu W., Jiang H. Efficient Grey Wolf Optimization: A High-Performance Optimizer with Reduced Memory Usage and Accelerated Convergence. 2024. DOI:10.20944/preprints202412.1974.v1

30. Kaveh A., Yosefpoor H. Competition of Three Chaotic Meta-heuristic Algorithms with Physical Inspiration for Optimal Design of Truss Structures // Periodica Polytechnica Civil Engineering. 2024. Vol. 68. Iss. 4. PP. 1211–1228. DOI:10.3311/PPci.36853. EDN:SEVTPJ

31. Rodriguez J.S., Parker R.B., Laird C.D., Nicholson B.L., Siirola J.D., Bynum M.L. Scalable Parallel Nonlinear Optimization with PyNumero and Parapint // INFORMS Journal on Computing. 2023. Vol. 35. Iss. 2. PP. 509–517. DOI:10.1287/ijoc.2023.1272. EDN:MQKQXF

32. Fuentes P.A., Tirado F.F., Quintas D.G., Meana J.J., Muniz A.P. On the Fast Evaluation of Polynomials // Journal of Advances in Mathematics and Computer Science. 2022. Vol. 37. Iss. 6. PP. 20–35. DOI:10.9734/jamcs/2022/v37i630457

33. Baichoo S., Ouzounis C.A. Computational complexity of algorithms for sequence comparison, short-read assembly and genome alignment // Biosystems. 2017. Vol. 156-157. PP. 72–85. DOI:10.1016/j.biosystems.2017.03.003

34. Yang H. Analysis and study on path planning algorithms in the further mobile action // Journal of Physics: Conference Series. 2024. Vol. 2824. P. 012006. DOI:10.1088/1742-6596/2824/1/012006. EDN:YVOPJW

35. Shanmugapriya M., Manivannan K.K. Compare the Performance of Meta-Heuristics Algorithm: A Review // Thanigaivelan R., Suchithra M., Kaliappan S., Mothilal T. (ed.) Metaheuristics Algorithm and Optimization of Engineering and Complex Systems. IGI Global Scientific Publishing, 2024. PP. 247–258. DOI:10.4018/979-8-3693-3314-3.ch013

36. Cuevas E., Galvez J., Avalos O., Wario F. Machine Learning and Metaheuristic Computation. John Wiley & Sons, 2024. 437 p. DOI:10.1002/9781394229680

37. Kulkarni V.R., Desai V. ABC and PSO: A comparative analysis // Proceedings of the International Conference on Computational Intelligence and Computing Research (ICCIC, Chennai, India, 15–17 December 2016). IEEE, 2016. DOI:10.1109/ICCIC.2016.7919625

38. Dorigo M., Stützle T. Ant Colony Optimization: Overview and Recent Advances // International Series in Operations Research & Management Science. Springer, 2019. PP. 311–351. DOI:10.1007/978-3-319-91086-4_10

39. Faris H., Aljarah I., Al-Betar M.A., Mirjalili S. Grey wolf optimizer: a review of recent variants and applications // Neural Computing and Applications. 2018. Vol. 30. PP. 413–435. DOI:10.1007/s00521-017-3272-5. EDN:JLGMRW

40. Chaudhari K., Thakkar A. Travelling Salesman Problem: An Empirical Comparison Between ACO, PSO, ABC, FA and GA // Proceedings of the Conference on Emerging Research in Computing, Information, Communication and Applications (ERCICA). Advances in Intelligent Systems and Computing. Singapore: Springer, 2019. Vol. 906. PP. 397–405. DOI:10.1007/978-981-13-6001-5_32

41. Negi G., Kumar A., Pant S., Ram M. GWO: a review and applications // International Journal of System Assurance Engineering and Management. 2020. Vol. 12. P. 1–8. DOI:10.1007/s13198-020-00995-8

42. Seyyedabbasi A., Kiani F. I-GWO and Ex-GWO: improved algorithms of the Grey Wolf Optimizer to solve global optimization problems // Engineering with Computers. 2021. Vol. 37. PP. 509–532. DOI:10.1007/s00366-019-00837-7

43. Миронов А.А., Файзуллин Р.В., Кузикова А.В. Оптимизация параметра величины колонии в муравьином алгоритме для решения задачи маршрутизации в сетях связи // Интеллектуальные системы в производстве. 2024.Т. 22. № 2. С. 63–68. DOI:10.22213/2410-9304-2024-2-63-68. EDN:YDLNPI

44. Kathane K.A., Shete R.M., Nawkhare R., Damahe L.B., Jadhav N.N., Dehankar J.N. Optimizing Dynamic Source Routing Protocol Using Computational Intelligent Approach // Proceedings of the 4th International Conference on Computer, Communication, Control & Information Technology, C3IT, Hooghly, India, 28–29 September 2024. IEEE, 2024. DOI:10.1109/C3IT60531.2024.10829484

45. Kansal V., Al-Farouni M., Bansal S., Michaelson J., Kumar S., Veena C.H. A Novel Ant Colony Optimization Algorithm for Dynamic Routing in Communication Networks // Proceedings of the International Conference on Communication, Computer Sciences and Engineering (IC3SE, Gautam Buddha Nagar, India, 09–11 May 2024). IEEE, 2024. PP. 1640–1645. DOI:10.1109/IC3SE62002.2024.10593344

46. Razooqi Y., Al-Asfoor M., Abed M.H. Optimise Energy Consumption of Wireless Sensor Networks by using modified Ant Colony Optimization // Acta Technica Jaurinensis. 2024. Vol. 17. Iss. 3. PP. 111–117. DOI:10.14513/actatechjaur.00742. EDN:CJUYDE

47. Kumar R., Kumar K., Sharma S. Burst Formation and Burst Assignment to Ingress Nodes in Optical Burst Switching Network Using ABC // International Journal of Electronics and Communication Engineering. 2023. Vol. 10. Iss. 10. PP. 25–39. DOI:10.14445/23488549/ijece-v10i10p103. EDN:YRWAEA

48. Jierui L. Research on the Application of Ant Colony Algorithm in Optimizing Transportation Routes in Cold Chain Logistics // Proceedings of the 2nd International Conference on Mechatronics, IoT and Industrial Informatics (ICMIII, Melbourne, Australia, 12–14 June 2024). IEEE, 2024. PP. 238–243. DOI:10.1109/ICMIII62623.2024.00050

49. Umar M.M., Mohammed A., Abdulazeez A. Review of QoS-aware resource allocation schemes for 5g networks // Dutse Journal of Pure and Applied Sciences. 2024. Vol. 10. Iss. 3c. PP. 296–303. DOI:10.4314/dujopas.v10i3c.28. EDN:YKTOHU

50. Bikkasani D.C., Yerabolu M.R. AI-Driven 5G Network Optimization: A Comprehensive Review of Resource Allocation, Traffic Management, and Dynamic Network Slicing // American Journal of Artificial Intelligence. 2024. Vol. 8. Iss. 2. PP. 55–62. DOI:10.11648/j.ajai.20240802.14. EDN:AOHEEN

51. Zahoor S., Javaid S., Javaid N., Ashraf M., Ishmanov F., Afzal M.K. Cloud–Fog–Based Smart Grid Model for Efficient Resource Management // Sustainability. 2018. Vol. 10. Iss. 6. P. 2079. DOI:10.3390/su10062079

52. Zhang W., Tuo K. Research on Offloading Strategy for Mobile Edge Computing Based on Improved Grey Wolf Optimization Algorithm // Electronics. 2023. Vol. 12. Iss. 11. P. 2533. DOI:10.3390/electronics12112533. EDN:AYUJJB

53. Liu W., Li C., Zheng A., Zheng Z., Zhang Z., Xiao Y. Fog Computing Resource-Scheduling Strategy in IoT Based on Artificial Bee Colony Algorithm // Electronics. 2023. Vol. 12. Iss. 7. P. 1511. DOI:10.3390/electronics12071511. EDN:EVPFUW

54. Мутханна А.С.А. Интегральное решение проблемы размещения контроллеров и балансировки нагрузки: 2 // Труды учебных заведений связи. 2023. Т. 9. № 2. С. 81–93. DOI:10.31854/1813-324X-2023-9-2-81-93. EDN:FTJGMC

55. Лисов А.А., Возмилов А.Г., Гундарев К.А., Кулганатов А.З. Применение алгоритма стаи серых волков и нейронных сетей для решения дискретных задач // Труды учебных заведений связи. 2024. Т. 10. № 5. С. 80–91. DOI:10.31854/1813-324X-2024-10-5-24-35. EDN:BEODCG

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

57. Gaikwad V., Naik A. An improved resource allocation architecture utilising swarm intelligence for mm-wave MIMO communication architecture // International Journal of Wireless and Mobile Computing. 2023. Vol. 25. Iss. 2. PP. 190–199. DOI:10.1504/ijwmc.2023.133070. EDN:VCBTHS

58. Liang Y.-C. Artificial Intelligence for Dynamic Spectrum Management // Dynamic Spectrum Management: From Cognitive Radio to Blockchain and Artificial Intelligence. Singapore: Springer, 2020. PP. 147–166. DOI:10.1007/978-981-15-0776-2_6

59. Alabi C.A., Idakwo M.A., Imoize A.L., Adamu T., Sur S.N. AI for spectrum intelligence and adaptive resource management // Sur S.N., Imoize A.L., Bhattacharya A., Kandar D., Banerjee J.S. (eds.) Artificial Intelligence for Wireless Communication Systems. CRC Press, 2024. 27 p. DOI:10.1201/9781003517689-3

60. Khan K., Goodridge W. Swarm Intelligence-Driven Client Selection for Federated Learning in Cybersecurity applications // arXiv:2411.18877. 2024. DOI:10.48550/arXiv.2411.18877

61. Zhang J., Wang H., Wang X. Application of artificial bee colony algorithm based on homogenization mapping and collaborative acquisition control in network communication security // PLoS One. 2024. Vol. 19. Iss. 7. P. e0306699. DOI:10.1371/journal.pone.0306699. EDN:BTHRFI

62. Ma Y., Chen J., Lv W., Qiu X., Zhang Y., Liu W. An improved artificial bee colony algorithm to minimum propagation latency and balanced load for controller placement in Software Defined Network // Computer Networks. 2024. Vol. 250. P. 110600. DOI:10.1016/j.comnet.2024.110600. EDN:KRNCGH

63. Pliatsios D. Comparison of Swarm Intelligence Methods for Joint Resource Orchestration in Open Radio Access Network // Proceedings of the 14th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP, Rome, Italy, 17–19 July 2024). IEEE, 2024. PP. 632–637. DOI:10.1109/CSNDSP60683.2024.10636586

64. Berlinski M. Ant Colony Algorithms Application for Telco Networks Performance with Multi-criteria Optimization // Proceedings of the International Conference on Software, Telecommunications and Computer Networks (SoftCOM, Split, Croatia, 21–23 September 2023). IEEE, 2023. DOI:10.23919/SoftCOM58365.2023.10271586

65. Venugopal P.S., Bharathy K.R., Gurusamy R., Rajkumar. Optimization of Delay and Energy in Wireless Body Area Networks Using Swarm Intelligence Based Dynamic Bandwidth Allocation Algorithm // Proceedings of the International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS, Bengaluru, India, 17–18 December 2024). IEEE, 2024. PP. 127–131. DOI:10.1109/ICICNIS64247.2024.10823293

66. Zhao Y., Men L. Group Intelligence Optimization Algorithm of Adaptive Trigonometric Function and T-Distributed Perturbation Strategy // Proceedings of the 6th International Conference on Communications, Information System and Computer Engineering (CISCE, Guangzhou, China, 10–12 May 2024). IEEE, 2024. PP. 740–744. DOI:10.1109/CISCE62493.2024.10653078

67. Liu Y., Huo L., Wu J., Bashir A.K. Swarm Learning-Based Dynamic Optimal Management for Traffic Congestion in 6G-Driven Intelligent Transportation System // IEEE Transactions on Intelligent Transportation Systems. 2023. Vol. 24. Iss. 7. PP. 7831–7846. DOI:10.1109/tits.2023.3234444. EDN:ILDTNW

68. Ahmad I., Qayum F., Rahman S.U., Srivastava G. Using Improved Hybrid Grey Wolf Algorithm Based on Artificial Bee Colony Algorithm Onlooker and Scout Bee Operators for Solving Optimization Problems // International Journal of Computational Intelligence Systems. 2024. Vol. 17. Iss. 1. P. 111. DOI:10.1007/s44196-024-00497-6. EDN:DJQIPZ

69. Furio C., Lamberti L., Pruncu C.I. An Efficient and Fast Hybrid GWO-JAYA Algorithm for Design Optimization // Applied Sciences. 2024. Vol. 14. Iss. 20. P. 9610. DOI:10.3390/app14209610

70. Li Y., Lian Z., Zhou K., Dai Y. A quasi-opposition learning and chaos local search based on walrus optimization for global optimization problems // Scientific Reports. 2025. Vol. 15. P. 2881. DOI:10.1038/s41598-025-85751-3. EDN:BZPYYV

71. Sari D.W., Dwijayanti S., Suprapto B.Y. Ant Colony Optimization-Based Path Planning for Autonomous Vehicle Navigation Systems // Proceedings of the International Conference on Electrical Engineering and Computer Science (ICECOS, Palembang, Indonesia, 25–26 September 2024). IEEE, 2024. PP. 135–140. DOI:10.1109/ICECOS63900.2024.10791115

72. Alfa A.A., Misra S., Abayomi-Alli A., Arogundade O., Jonathan O., Ahuja R. Comparative Analysis of Intelligent Solutions Searching Algorithms of Particle Swarm Optimization and Ant Colony Optimization for Artificial Neural Networks Target Dataset // Proceedings of Second International Conference on Computing, Communications, and Cyber-Security. Lecture Notes in Networks and Systems. Singapore: Springer, 2021. Vol. 203. PP. 459–470. DOI:10.1007/978-981-16-0733-2_32

73. Kalpana N. ABC Algorithm for Evaluating the Performance of the SVC and Optimal Power Flow // Proceedings of the International Conference on Recent Trends in Communication and Intelligent Systems (ICRTCIS, Rajasthan, India, 28–29 April 2023). Algorithms for Intelligent Systems. Singapore: Springer Nature, 2023. PP. 37–47. DOI:10.1007/978-981-99-5792-7_3

74. Almajidi A.M., Pawar V.P., Alammari A., Ali N.S. ABC-Based Algorithm for Clustering and Validating WSNs // Proceedings of the International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA, Goa, India, 16–17 August 2019). Algorithms for Intelligent Systems. Singapore: Springer, 2020. PP. 117–125. DOI:10.1007/978-981-15-1632-0_13

75. Ding W., Yao H., Ju H., Huang J., Jiang S., Chen Y. Pheromone-guided parallel rough hypercuboid attribute reduction algorithm // Applied Soft Computing. 2024. Vol. 156. P. 111479. DOI:10.1016/j.asoc.2024.111479. EDN:HKPVIE

76. Warnakulasooriya K., Segev A. Comparative analysis of accuracy and computational complexity across 21 swarm intelligence algorithms // Evolutionary Intelligence. 2024. Vol. 18. P. 18. DOI:10.1007/s12065-024-00997-6. EDN:FHRUUA

77. Khera V. Comparative Study of Evolutionary Algorithms // International Journal of Science and Research. 2023. Vol. 12. Iss. 6. PP. 836–840. DOI:10.21275/sr23610122607. EDN:LPWBXF

78. Kalpana N. Innovative Method for Assessing Optimal Power Flow and SVC Performance Using the ABC Algorithm // Proceedings of the 6th International Conference on Communications and Cyber Physical Engineering (ICCCE, Hyderabad, India, 28–29 April 2023). Lecture Notes in Electrical Engineering. Singapore: Springer Nature, 2024. Vol. 1096. PP. 21–31. DOI:10.1007/978-981-99-7137-4_3

79. Du H., Zhu Z., Gu S. Research on Optimization of Computer Network Routing Based on Ant Colony Algorithm // Proceedings of the 2nd International Conference on Artificial Intelligence and Autonomous Robot Systems (AIARS, Bristol, United Kingdom, 29–31 July 2023). IEEE, 2023. PP. 365–368. DOI:10.1109/AIARS59518.2023.00080

80. Makhadmeh S.N., Al-Betar M.A., Al-Obeidat F., Alomari O.A., Abasi A.K., Tubishat M., et al. A multi-objective grey wolf optimizer for energy planning problem in smart home using renewable energy systems // Sustainable Operations and Computers. 2024. Vol. 5. PP. 88–101. DOI:10.1016/j.susoc.2024.04.001. EDN:HSZMYI

81. Makhadmeh S.N., Al-Betar M.A., Al-Obeidat F., Alomari O.A., Abasi A.K., Tubishat M., et al. A Multi-objective Grey Wolf Optimizer for Power Scheduling Problem in Smart Home Using Renewable Energy Systems // Research Square. 2023. DOI:10.21203/rs.3.rs-3771300/v1

82. Huang X., Xu R., Yu W., Wu S. Evaluation and Analysis of Heuristic Intelligent Optimization Algorithms for PSO, WDO, GWO and OOBO // Mathematics. 2023. Vol. 11. Iss. 21. P. 4531. DOI:10.3390/math11214531. EDN:INHEUT

83. Yadav U.K., Singh V.P. Systematically derived weights based order diminution of continuous systems using GWO algorithm // Journal of the Franklin Institute. 2022. Vol. 359. Iss. 17. P. 9902–9924. DOI:10.1016/j.jfranklin.2022.09.050. EDN:ZXUCUI

84. Shyshatskyi A., Kashkevich S., Kyrychenko I., Khakhlyuk O., Kubrak V., Koval A., et al. Methodical approach to assessing the state of hierarchical systems using a metaheuristic algorithm // Eastern-European Journal of Enterprise Technologies. 2024. Vol. 5. Iss. 4(131). PP. 82–88. DOI:10.15587/1729-4061.2024.311235. EDN:HSRFIL

85. Shahakar M., Mahajan S.A., Patil L. Optimizing System Resources and Adaptive Load Balancing Framework Leveraging ACO and Reinforcement Learning Algorithms // Journal of Electrical Systems. 2024. Vol. 20. Iss. 1s. PP. 244–256. DOI:10.52783/jes.768. EDN:DTXCKX

86. Cao B., Chen Y., Liu X., He H., Song H., Lv Z. Multiobjective Resource Allocation Strategy for Metaverse Resource Management // Proceedings of the International Conference on Metaverse Computing, Networking and Applications (MetaCom, Kyoto, Japan, 26–28 June 2023). IEEE, 2023. PP. 564–570. DOI:10.1109/MetaCom57706.2023.00100

87. Kambhampati R.T. AI Telco Research: Advancements in Telecommunications Scientific Discovery // International Journal for Research in Applied Science & Engineering Technology. 2024. Vol. 12. Iss. 9. PP. 1514–1519. DOI:10.22214/ijraset.2024.64339

88. Jadon S.S., Tiwari R., Sharma H., Bansal J.C. Hybrid Artificial Bee Colony algorithm with Differential Evolution // Applied Soft Computing. 2017. Vol. 58. PP. 11–24. DOI:10.1016/j.asoc.2017.04.018

89. Seyyedabbasi A., Tareq Tareq W.Z., Bacanin N. An Effective Hybrid Metaheuristic Algorithm for Solving Global Optimization Algorithms // Multimedia Tools and Applications. 2024. Vol. 83. PP. 85103–85138. DOI:10.1007/s11042-024-19437-9. EDN:HMWSUL

90. Lehre P.K., Qin X. Self-adaptation Can Improve the Noise-tolerance of Evolutionary Algorithms // Proceedings of the 17th ACM/SIGEVO Conference on Foundations of Genetic Algorithms (FOGA, Potsdam, Germany, 30 August 2023 – 1 September 2023). New York: Association for Computing Machinery, 2023. PP. 105–116. DOI:10.1145/3594805.3607128

91. Lehre P.K., Qin X. Self-adaptation Can Help Evolutionary Algorithms Track Dynamic Optima // Proceedings of the Genetic and Evolutionary Computation Conference (GECCO, Lisbon Portugal, 15–19 July 2023). New York: Association for Computing Machinery, 2023. PP. 1619–1627. DOI:10.1145/3583131.3590494

92. Zhang Y., Cai Y. Adaptive dynamic self-learning grey wolf optimization algorithm for solving global optimization problems and engineering problems // Mathematical Biosciences and Engineering. 2024. Vol. 21. Iss. 3. PP. 3910–3943. DOI:10.3934/mbe.2024174. EDN:UGPDBW

93. Barrion M.H., Bandala A., Maningo J.M., Dadios E., Naguib R. Advancing Robotic Swarms with Blockchain Technology: A Dynamic Two-Factor Authentication Consensus Framework // Research Square. 2024. DOI:10.21203/rs.3.rs-5301694/v1
94. Yang H. Swarm Contract: A Multi-Sovereign Agent Consensus Mechanism // arXiv:2412.19256. 2024. DOI:10.48550/arXiv.2412.19256
95. Li Y. Quantum Ant Colony Algorithm for Solving the Traveling Salesman Problem: A Theoretical and Practical Analysis // Applied and Computational Engineering. 2024. Vol. 110. Iss. 1. PP. 175–181. DOI:10.54254/2755-2721/110/2024MELB0121
96. Tajabadi M., Heider D. Fair swarm learning: Improving incentives for collaboration by a fair reward mechanism // Knowledge-Based Systems. 2024. Vol. 304. P. 112451. DOI:10.1016/j.knosys.2024.112451. EDN:UOAGIK
97. Moustafa N. GH-Twin: Graph Learning Empowered Hierarchical Digital Twin for Optimizing Self-Healing Networks // Sustainable Machine Intelligence Journal. 2024. Vol. 8. PP. 35–45. DOI:10.61356/smij.2024.8289. EDN:DNPELS
98. Wang N., Wu Y., Lorenzo B., Liu B. Semantic-Aware Architecture Design for a Lifelong Swarm Metaverse // IEEE Internet of Things Journal. 2025. Vol. 12. Iss. 9. PP. 12468–12482. DOI:10.1109/JIOT.2024.3520518

References

1. Ateya A.A., El-Latif A.A.A., Muthanna A., Volkov A., Koucheryavy A. *Enabling Metaverse and Telepresence Services in 6G Networks*. NY: River Publishers; 2025. 254 p. DOI:10.1201/9788770046749
2. Zangana H.M., Sallow Z.B., Alkawaz M.H., Omar M. Unveiling the Collective Wisdom: A Review of Swarm Intelligence in Problem Solving and Optimization. *Inform: Jurnal Ilmiah Bidang Teknologi Informasi Dan Komunikasi*. 2024;9(2):101–110. DOI:10.25139/inform.v9i2.7934. EDN:WJAKIJ
3. Mao S., Hu F., Lang J., Chen T., Cheng S. Comparative Study of Impacts of Typical Bio-Inspired Optimization Algorithms on Source Inversion Performance. *Frontiers in Environmental Science*. 2022;10:894255. DOI:10.3389/fenvs.2022.894255
4. Duan H., Li P. *Bio-inspired computation in unmanned aerial vehicles*. Berlin, Heidelberg: Springer; 2014. DOI:10.1007/978-3-642-41196-0
5. Hao Z., Huang H., Cai R. Bio-inspired Algorithms for TSP and Generalized TSP. In: Greco F. (ed.) *Traveling Salesman Problem*. IntechOpen; 2008. DOI:10.5772/5583
6. Ateya A.A., Muthanna A., Vybornova A., Algarni A.D., Abuarqoub A., Koucheryavy Y., et al. Chaotic salp swarm algorithm for SDN multi-controller networks. *Engineering Science and Technology, an International Journal*. 2019;22(4):1001–1012. DOI:10.1016/j.jestch.2018.12.015. EDN:DOSQQF
7. Alanis A.Y., Arana-Daniel N., López-Franco C. Bio-inspired Algorithms. In: *Bio-inspired Algorithms for Engineering*. Elsevier; 2018. p.1–14. DOI:10.1016/B978-0-12-813788-8.00001-9
8. Subramanian S., Bhojaneet N., Madhnani H., Pant S., Kumar A., Kotecha K. A Comprehensive Review of Nature-Inspired Optimization Techniques and Their Varied Applications. In: *Nature-Inspired Optimization Algorithms for Cyber-Physical Systems*. IGI Global Scientific Publishing; 2025. p.105–174. DOI:10.4018/979-8-3693-6834-3.ch005
9. Li P., Duan H. Bio-inspired Computation Algorithms // Bio-inspired Computation in Unmanned Aerial Vehicles. Berlin, Heidelberg: Springer, 2014. PP. 35–69. DOI:10.1007/978-3-642-41196-0_2
10. Almufti M.S., Marqas R.B., Saeed V.A. Taxonomy of bio-inspired optimization algorithms. *Journal of Advanced Computer Science & Technology*. 2019;8(2):23–31. DOI:10.14419/jacst.v8i2.29402
11. Zhang Z., Xu T., Zou K., Tan S., Sun Z. Multi-Objective Grey Wolf Optimizer Based on Improved Head Wolf Selection Strategy. *Proceedings of the 43rd Chinese Control Conference, CCC, 28–31 July 2024, Kunming, China*. IEEE; 2024. p.1922–1927. DOI:10.23919/CCC63176.2024.10662658
12. Peng Q., Zhan R., Wu H., Shi M. Comparative Study of Wolf Pack Algorithm and Artificial Bee Colony Algorithm: Performance Analysis and Optimization Exploration. *International Journal of Swarm Intelligence Research*. 2024;15(1):1–24. DOI:10.4018/IJSIR.352061
13. Yang J., Gu W. A multi-stage time-backtracking grey wolf optimizer introducing a new hierarchy mechanism. *Research Square*. 2024. DOI:10.21203/rs.3.rs-4126903/v1
14. Zhao S. Research on the Application of Swarm Behavior to Artificial Intelligence Systems. *Applied and Computational Engineering*. 2025;120:158–163. DOI:10.54254/2755-2721/2025.19403. EDN:OGCKKC
15. Tyagi N., Bhargava D., Ahlawat A. Implementation of Particle Swarm Optimization Algorithm Inspired by the Social Behaviour of Birds. *Proceedings of the 4th International Conference on Technological Advancements in Computational Sciences, ICTACS, 13–15 November 2024, Tashkent, Uzbekistan*. IEEE; 2024. p.750–754. DOI:10.1109/ICTACS62700.2024.10840529
16. Cai T., Zhang S., Ye Z., Zhou W., Wang M., He Q., Chen Z., et al. Cooperative metaheuristic algorithm for global optimization and engineering problems inspired by heterosis theory. *Scientific Reports*. 2024;14(1):28876. DOI:10.1038/s41598-024-78761-0. EDN:QOGXNY
17. Wu Y., Zhu X., Zhao W., Xia X. A Novel Particle Swarm Optimization Algorithm for Meta-Heuristic Analysis Mechanism Based on Population Learning Strategies and Adaptive Selection of Leadership Particles. *Proceedings of the 11th International Conference on Data Science and Advanced Analytics, DSAA, 06–10 October 2024, San Diego, USA*. IEEE; 2024. p.1–9. DOI:10.1109/DSAA61799.2024.10722812
18. Yazıcı A.M., Ömür G.A., Celik D.A. Applications and Future Perspectives of Swarm Intelligence in Unmanned and Autonomous Systems: Innovative Conceptual Approaches to Social Sciences. *Sosyal Mucit Academic Review*. 2024;5(Innovative Conceptual Approaches to Social Sciences):106–130. DOI:10.54733/smar.1555925. EDN:QUVHXT

19. Pachajoa G.M.M., Achicanoy W., Garzón Ramos D. Automating the Evaluation of the Scalability, Flexibility, and Robustness of Collective Behaviors for Robot Swarms. *Proceedings of the Brazilian Symposium on Robotics (SBR) and 2024 Workshop on Robotics in Education, WRE, 13–15 November 2024, Goiania, Brazil*. Piscataway: IEEE; 2024. p.144–149. DOI:10.1109/SBR/WRE63066.2024.10837963

20. Paköz B. Swarm Intelligence and Decentralized AI. *Human Computer Interaction*. 2024;8(1):97–100. DOI:10.62802/k7xhrd47. EDN:GLVTOB

21. Yogi M.K., Chakravarthy A.S.N. Application of Variants of Nature-Inspired Optimization for Privacy Preservation in Cyber-Physical Systems. *Nature-Inspired Optimization Algorithms for Cyber-Physical Systems*. IGI Global Scientific Publishing; 2025. DOI:10.4018/979-8-3693-6834-3.ch009

22. Cheng H., Zhou H., Shen Y. An improved grey wolf optimization algorithm based on bounded subpopulation re-search strategy. *Journal of Physics: Conference Series.* 2024;2902:012035. DOI:10.1088/1742-6596/2902/1/012035. EDN:ONSHBZ

23. Zhang J., Dai Y., Shi Q. An improved grey wolf optimization algorithm based on scale-free network topology. *Heliyon*. 2024;10(16):e35958. DOI:10.1016/j.heliyon.2024.e35958. EDN:VACDIH

24. Karaboga D. *An idea based on honey bee swarm for numerical optimization*. Technical Report-tr06. 2005. URL: https://abc.erciyes.edu.tr/pub/tr06_2005.pdf [Accessed 02.07.2025]

25. Xiao W.-S., Li G., Liu C., Tan L. A novel chaotic and neighborhood search-based artificial bee colony algorithm for solving optimization problems. *Scientific Reports*. 2023;13:20496. DOI:10.1038/s41598-023-44770-8. EDN:MDLWOS

26. Dorigo M., Maniezzo V., Colorni A. *Ant system: An Autocatalytic Optimizing Process*. 1991.

27. Misra B., Chakraborty S. Ant Colony Optimization – Recent Variants, Application and Perspectives. In: *Dey N. (ed.) Applications of Ant Colony Optimization and its Variants: Case Studies and New Developments*. Singapore: Springer Nature; 2024. p.1–17. DOI:10.1007/978-981-99-7227-2_1

28. Olivari L. Reducing ACO Population Size to Increase Computational Speed. *Tehnički glasnik*. 2024;18(4):532–539. DOI:10.31803/tg-20230825125127. EDN:ZSJBRX

29. Jiang H., Liu D., Liu X., Wu W., Jiang H. *Efficient Grey Wolf Optimization: A High-Performance Optimizer with Reduced Memory Usage and Accelerated Convergence*. 2024. DOI:10.20944/preprints202412.1974.v1

30. Kaveh A., Yosefpoor H. Competition of Three Chaotic Meta-heuristic Algorithms with Physical Inspiration for Optimal Design of Truss Structures. *Periodica Polytechnica Civil Engineering*. 2024;68(4):1211–1228. DOI:10.3311/PPci.36853. EDN:SEVTPJ

31. Rodriguez J.S., Parker R.B., Laird C.D., Nicholson B.L., Siirola J.D., Bynum M.L. Scalable Parallel Nonlinear Optimization with PyNumero and Parapint. *INFORMS Journal on Computing*. 2023;35(2):509–517. DOI:10.1287/ijoc.2023.1272. EDN:MQKQXF

32. Fuentes P.A., Tirado F.F., Quintas D.G., Meana J.J., Muniz A.P. On the Fast Evaluation of Polynomials. *Journal of Advances in Mathematics and Computer Science*. 2022;37(6):20–35. DOI:10.9734/jamcs/2022/v37i630457

33. Baichoo S., Ouzounis C.A. Computational complexity of algorithms for sequence comparison, short-read assembly and genome alignment. *Biosystems*. 2017;156-157:72–85. DOI:10.1016/j.biosystems.2017.03.003

34. Yang H. Analysis and study on path planning algorithms in the further mobile action. *Journal of Physics: Conference Series*. 2024;2824:012006. DOI:10.1088/1742-6596/2824/1/012006. EDN:YVOPJW

35. Shanmugapriya M., Manivannan K.K. Compare the Performance of Meta-Heuristics Algorithm: A Review. In: Thanigaivelan R., Suchithra M., Kaliappan S., Mothilal T. (ed.) *Metaheuristics Algorithm and Optimization of Engineering and Complex Systems*. IGI Global Scientific Publishing; 2024. p.247–258. DOI:10.4018/979-8-3693-3314-3.ch013

36. Cuevas E., Galvez J., Avalos O., Wario F. *Machine Learning and Metaheuristic Computation*. John Wiley & Sons; 2024. 437 p. DOI:10.1002/9781394229680

37. Kulkarni V.R., Desai V. ABC and PSO: A comparative analysis. *Proceedings of the International Conference on Computational Intelligence and Computing Research, ICCIC, 15–17 December 2016, Chennai, India*. IEEE; 2016. DOI:10.1109/ICCIC.2016.7919625

38. Faris H., Aljarah I., Al-Betar M.A., Mirjalili S. Grey wolf optimizer: a review of recent variants and applications. *Neural Computing and Applications*. 2018;30:413–435. DOI:10.1007/s00521-017-3272-5. EDN:JLGMRW

39. Faris H., Aljarah I., Al-Betar M.A., Mirjalili S. Grey wolf optimizer: a review of recent variants and applications. *Neural Computing and Applications*. 2018;30:413–435. DOI:10.1007/s00521-017-3272-5. EDN:JLGMRW

40. Chaudhari K., Thakkar A. Travelling Salesman Problem: An Empirical Comparison Between ACO, PSO, ABC, FA and GA. *Proceedings of the Conference on Emerging Research in Computing, Information, Communication and Applications (ERCICA). Advances in Intelligent Systems and Computing, vol.906*. Singapore: Springer; 2019. p.397–405. DOI:10.1007/978-981-13-6001-5_32

41. Negi G., Kumar A., Pant S., Ram M. GWO: a review and applications. *International Journal of System Assurance Engineering and Management*. 2020;12:1–8. DOI:10.1007/s13198-020-00995-8

42. Seyyedabbasi A., Kiani F. I-GWO and Ex-GWO: improved algorithms of the Grey Wolf Optimizer to solve global optimization problems. *Engineering with Computers*. 2021;37:509–532. DOI:10.1007/s00366-019-00837-7

43. Mironov A.A., Fayzullin R.V., Kuzikova A.V. Optimization of the Colony Size Parameter in the Ant Algorithm for Solving the Routing Problem In Communication Networks. *Intellektual'nye sistemy v proizvodstve.* 2024;22(2):63–68. DOI:10.22213/2410-9304-2024-2-63-68. EDN:YDLNPI

44. Kathane K.A., Shete R.M., Nawkhare R., Damahe L.B., Jadhav N.N., Dehankar J.N. Optimizing Dynamic Source Routing Protocol Using Computational Intelligent Approach. *Proceedings of the 4th International Conference on Computer, Communication, Control & Information Technology, C3IT, 28–29 September 2024, Hooghly, India*. IEEE; 2024. DOI:10.1109/C3IT60531.2024.10829484

45. Kansal V., Al-Farouni M., Bansal S., Michaelson J., Kumar S., Veena C.H. A Novel Ant Colony Optimization Algorithm for Dynamic Routing in Communication Networks. *Proceedings of the International Conference on Communication, Computer Sciences and Engineering, IC3SE, 09–11 May 2024, Gautam Buddha Nagar, India*. IEEE; 2024. p.1640–1645. DOI:10.1109/IC3SE62002.2024.10593344

46. Razooqi Y., Al-Asfoor M., Abed M.H. Optimise Energy Consumption of Wireless Sensor Networks by using modified Ant Colony Optimization. *Acta Technica Jaurinensis*. 2024;17(3):111–117. DOI:10.14513/actatechjaur.00742. EDN:CJUYDE

47. Kumar R., Kumar K., Sharma S. Burst Formation and Burst Assignment to Ingress Nodes in Optical Burst Switching Network Using ABC. *International Journal of Electronics and Communication Engineering*. 2023;10(10):25–39. DOI:10.14445/23488549/ijece-v10i10p103. EDN:YRWAEA

48. Jierui L. Research on the Application of Ant Colony Algorithm in Optimizing Transportation Routes in Cold Chain Logistics. *Proceedings of the 2nd International Conference on Mechatronics, IoT and Industrial Informatics, ICMIII, 12–14 June 2024, Melbourne, Australia*. IEEE; 2024. p.238–243. DOI:10.1109/ICMIII62623.2024.00050

49. Umar M.M., Mohammed A., Abdulazeez A. Review of QoS-aware resource allocation schemes for 5g networks. *Dutse Journal of Pure and Applied Sciences*. 2024;10(3c):296–303. DOI:10.4314/dujopas.v10i3c.28. EDN:YKTOHU

50. Bikkasani D.C., Yerabolu M.R. AI-Driven 5G Network Optimization: A Comprehensive Review of Resource Allocation, Traffic Management, and Dynamic Network Slicing. *American Journal of Artificial Intelligence*. 2024;8(2):55–62. DOI:10.11648/j.ajai.20240802.14. EDN:AOHEEN

51. Zahoor S., Javaid S., Javaid N., Ashraf M., Ishmanov F., Afzal M.K. Cloud–Fog–Based Smart Grid Model for Efficient Resource Management. *Sustainability*. 2018;10(6):2079. DOI:10.3390/su10062079

52. Zhang W., Tuo K. Research on Offloading Strategy for Mobile Edge Computing Based on Improved Grey Wolf Optimization Algorithm. *Electronics*. 2023;12(11):2533. DOI:10.3390/electronics12112533. EDN:AYUJJB

53. Liu W., Li C., Zheng A., Zheng Z., Zhang Z., Xiao Y. Fog Computing Resource-Scheduling Strategy in IoT Based on Artificial Bee Colony Algorithm. *Electronics*. 2023;12(7):1511. DOI:10.3390/electronics12071511. EDN:EVPFUW

54. Muthanna A. Controller Location and Load Balancing Integrated Solution. *Proceedings of Telecommunication Universities*. 2023;9(2):81–93. (in Russ.) DOI:10.31854/1813-324X-2023-9-2-81-93

55. Lisov A.A., Vozmilov A.G., Gundarev K.A., Kulganatov A.Z. Application of the Gray Wolf Optimization. Algorithm and Neural Networks for Solving Discrete Problems. *Proceedings of Telecommunication Universities*. 2024;10(5):80–91. (in Russ.) DOI:10.31854/1813-324X-2024-10-5-24-35. EDN:BEODCG.

56. 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

57. Gaikwad V., Naik A. An improved resource allocation architecture utilising swarm intelligence for mm-wave MIMO communication architecture. *International Journal of Wireless and Mobile Computing*. 2023;25(2):190–199. DOI:10.1504/ijwmc.2023.133070. EDN:VCBTHS

58. Liang Y.-C. Artificial Intelligence for Dynamic Spectrum Management. In: *Dynamic Spectrum Management: From Cognitive Radio to Blockchain and Artificial Intelligence*. Singapore: Springer; 2020. p.147–166. DOI:10.1007/978-981-15-0776-2_6

59. Alabi C.A., Idakwo M.A., Imoize A.L., Adamu T., Sur S.N. AI for spectrum intelligence and adaptive resource management. In: Sur S.N., Imoize A.L., Bhattacharya A., Kandar D., Banerjee J.S. (eds.) *Artificial Intelligence for Wireless Communication Systems*. CRC Press; 2024. 27 p. DOI:10.1201/9781003517689-3

60. Khan K., Goodridge W. Swarm Intelligence-Driven Client Selection for Federated Learning in Cybersecurity applications. *arXiv:2411.18877*. 2024. DOI:10.48550/arXiv.2411.18877

61. Zhang J., Wang H., Wang X. Application of artificial bee colony algorithm based on homogenization mapping and collaborative acquisition control in network communication security. *PLoS One*. 2024;19(7):e0306699. DOI:10.1371/journal.pone.0306699. EDN:BTHRFI

62. Ma Y., Chen J., Lv W., Qiu X., Zhang Y., Liu W. An improved artificial bee colony algorithm to minimum propagation latency and balanced load for controller placement in Software Defined Network. *Computer Networks*. 2024;250:110600. DOI:10.1016/j.comnet.2024.110600. EDN:KRNCGH

63. Pliatsios D. Comparison of Swarm Intelligence Methods for Joint Resource Orchestration in Open Radio Access Network. *Proceedings of the 14th International Symposium on Communication Systems, Networks and Digital Signal Processing, CSNDSP, 17–19 July 2024, Rome, Italy*. IEEE; 2024. p.632–637. DOI:10.1109/CSNDSP60683.2024.10636586

64. Berlinski M. Ant Colony Algorithms Application for Telco Networks Performance with Multi-criteria Optimization. *Proceedings of the International Conference on Software, Telecommunications and Computer Networks, SoftCOM, 21–23 September 2023, Split, Croatia*. IEEE; 2023. DOI:10.23919/SoftCOM58365.2023.10271586

65. Venugopal P.S., Bharathy K.R., Gurusamy R., Rajkumar. Optimization of Delay and Energy in Wireless Body Area Networks Using Swarm Intelligence Based Dynamic Bandwidth Allocation Algorithm. *Proceedings of the International Conference on IoT Based Control Networks and Intelligent Systems, ICICNIS, 17–18 December 2024, Bengaluru, India*. IEEE; 2024. p.127–131. DOI:10.1109/ICICNIS64247.2024.10823293

66. Zhao Y., Men L. Group Intelligence Optimization Algorithm of Adaptive Trigonometric Function and T-Distributed Perturbation Strategy. *Proceedings of the 6th International Conference on Communications, Information System and Computer Engineering, CISCE, 10–12 May 2024, Guangzhou, China*. IEEE; 2024. p.740–744. DOI:10.1109/CISCE62493.2024.10653078

67. Liu Y., Huo L., Wu J., Bashir A.K. Swarm Learning-Based Dynamic Optimal Management for Traffic Congestion in 6G-Driven Intelligent Transportation System. *IEEE Transactions on Intelligent Transportation Systems*. 2023;24(7):7831–7846. DOI:10.1109/tits.2023.3234444. EDN:ILDTNW

68. Ahmad I., Qayum F., Rahman S.U., Srivastava G. Using Improved Hybrid Grey Wolf Algorithm Based on Artificial Bee Colony Algorithm Onlooker and Scout Bee Operators for Solving Optimization Problems. *International Journal of Computational Intelligence Systems*. 2024;17(1):111. DOI:10.1007/s44196-024-00497-6. EDN:DJQIPZ

69. Furio C., Lamberti L., Pruncu C.I. An Efficient and Fast Hybrid GWO-JAYA Algorithm for Design Optimization. *Applied Sciences*. 2024;14(20):9610. DOI:10.3390/app14209610

70. Li Y., Lian Z., Zhou K., Dai Y. A quasi-opposition learning and chaos local search based on walrus optimization for global optimization problems. *Scientific Reports*. 2025;15:2881. DOI:10.1038/s41598-025-85751-3. EDN:BZPYYV

71. Sari D.W., Dwijayanti S., Suprapto B.Y. Ant Colony Optimization-Based Path Planning for Autonomous Vehicle Navigation Systems. *Proceedings of the International Conference on Electrical Engineering and Computer Science, ICECOS, 25–26 September 2024, Palembang, Indonesia*. IEEE; 2024. p.135–140. DOI:10.1109/ICECOS63900.2024.10791115

72. Alfa A.A., Misra S., Abayomi-Alli A., Arogundade O., Jonathan O., Ahuja R. Comparative Analysis of Intelligent Solutions Searching Algorithms of Particle Swarm Optimization and Ant Colony Optimization for Artificial Neural Networks Target Dataset. *Proceedings of Second International Conference on Computing, Communications, and Cyber-Security. Lecture Notes in Networks and Systems, vol.203*. Singapore: Springer; 2021. p.459–470. DOI:10.1007/978-981-16-0733-2_32

73. Kalpana N. ABC Algorithm for Evaluating the Performance of the SVC and Optimal Power Flow. *Proceedings of the International Conference on Recent Trends in Communication and Intelligent Systems, ICRTCIS, 28–29 April 2023, Rajasthan, India*. *Algorithms for Intelligent Systems*. Singapore: Springer Nature; 2023. p.37–47. DOI:10.1007/978-981-99-5792-7_3

74. Almajidi A.M., Pawar V.P., Alammari A., Ali N.S. ABC-Based Algorithm for Clustering and Validating WSNs. *Proceedings of the International Conference on Cybernetics, Cognition and Machine Learning Applications, ICCCMLA, 16–17 August 2019, Goa, India. Algorithms for Intelligent Systems*. Singapore: Springer, 2020. p.117–125. DOI:10.1007/978-981-15-1632-0_13

75. Ding W., Yao H., Ju H., Huang J., Jiang S., Chen Y. Pheromone-guided parallel rough hypercuboid attribute reduction algorithm. *Applied Soft Computing*. 2024;156:111479. DOI:10.1016/j.asoc.2024.111479. EDN:HKPVIE

76. Warnakulasooriya K., Segev A. Comparative analysis of accuracy and computational complexity across 21 swarm intelligence algorithms. *Evolutionary Intelligence*. 2024;18:18. DOI:10.1007/s12065-024-00997-6. EDN:FHRUUA

77. Khera V. Comparative Study of Evolutionary Algorithms. *International Journal of Science and Research*. 2023;12(6):836–840. DOI:10.21275/sr23610122607. EDN:LPWBXF

78. Kalpana N. Innovative Method for Assessing Optimal Power Flow and SVC Performance Using the ABC Algorithm. *Proceedings of the 6th International Conference on Communications and Cyber Physical Engineering, ICCCE, 28–29 April 2023, Hyderabad, India. Lecture Notes in Electrical Engineering, vol.1096.* Singapore: Springer Nature; 2024. p.21–31. DOI:10.1007/978-981-99-7137-4_3

79. Du H., Zhu Z., Gu S. Research on Optimization of Computer Network Routing Based on Ant Colony Algorithm. *Proceedings of the 2nd International Conference on Artificial Intelligence and Autonomous Robot Systems, AIARS, 29–31 July 2023, Bristol, United Kingdom*. IEEE; 2023. p.365–368. DOI:10.1109/AIARS59518.2023.00080

80. Makhadmeh S.N., Al-Betar M.A., Al-Obeidat F., Alomari O.A., Abasi A.K., Tubishat M., et al. A multi-objective grey wolf optimizer for energy planning problem in smart home using renewable energy systems. *Sustainable Operations and Computers.* 2024;5:88–101. DOI:10.1016/j.susoc.2024.04.001. EDN:HSZMYI

81. Makhadmeh S.N., Al-Betar M.A., Al-Obeidat F., Alomari O.A., Abasi A.K., Tubishat M., et al. A Multi-objective Grey Wolf Optimizer for Power Scheduling Problem in Smart Home Using Renewable Energy Systems. *Research Square*. 2023. DOI:10.21203/rs.3.rs-3771300/v1

82. Huang X., Xu R., Yu W., Wu S. Evaluation and Analysis of Heuristic Intelligent Optimization Algorithms for PSO, WDO, GWO and OOBO. *Mathematics*. 2023;11(21):4531. DOI:10.3390/math11214531. EDN:INHEUT

83. Yadav U.K., Singh V.P. Systematically derived weights based order diminution of continuous systems using GWO algorithm. *Journal of the Franklin Institute*. 2022;359(17):9902–9924. DOI:10.1016/j.jfranklin.2022.09.050. EDN:ZXUCUI

84. Shyshatskyi A., Kashkevich S., Kyrychenko I., Khakhlyuk O., Kubrak V., Koval A., et al. Methodical approach to assessing the state of hierarchical systems using a metaheuristic algorithm. *Eastern-European Journal of Enterprise Technologies*. 2024;5(4(131)):82–88. DOI:10.15587/1729-4061.2024.311235. EDN:HSRFIL

85. Shahakar M., Mahajan S.A., Patil L. Optimizing System Resources and Adaptive Load Balancing Framework Leveraging ACO and Reinforcement Learning Algorithms. *Journal of Electrical Systems*. 2024;20(1s):244–256. DOI:10.52783/jes.768. EDN:DTXCKX

86. Cao B., Chen Y., Liu X., He H., Song H., Lv Z. Multiobjective Resource Allocation Strategy for Metaverse Resource Management. *Proceedings of the International Conference on Metaverse Computing, Networking and Applications, MetaCom, 26–28 June 2023, Kyoto, Japan*. IEEE; 2023. p.564–570. DOI:10.1109/MetaCom57706.2023.00100

87. Kambhampati R.T. AI Telco Research: Advancements in Telecommunications Scientific Discovery. *International Journal for Research in Applied Science & Engineering Technology*. 2024;12(9):1514–1519. DOI:10.22214/ijraset.2024.64339

88. Jadon S.S., Tiwari R., Sharma H., Bansal J.C. Hybrid Artificial Bee Colony algorithm with Differential Evolution. *Applied Soft Computing*. 2017;58:11–24. DOI:10.1016/j.asoc.2017.04.018

89. Seyyedabbasi A., Tareq Tareq W.Z., Bacanin N. An Effective Hybrid Metaheuristic Algorithm for Solving Global Optimization Algorithms. *Multimedia Tools and Applications*. 2024;83:85103–85138. DOI:10.1007/s11042-024-19437-9. EDN:HMWSUL

90. Lehre P.K., Qin X. Self-adaptation Can Improve the Noise-tolerance of Evolutionary Algorithms. *Proceedings of the 17th ACM/SIGEVO Conference on Foundations of Genetic Algorithms, FOGA, 30 August 2023 – 1 September 2023, Potsdam, Germany*. New York: Association for Computing Machinery; 2023. p.105–116. DOI:10.1145/3594805.3607128

91. Lehre P.K., Qin X. Self-adaptation Can Help Evolutionary Algorithms Track Dynamic Optima. *Proceedings of the Genetic and Evolutionary Computation Conference, GECCO, 15–19 July 2023, Lisbon, Portugal*. New York: Association for Computing Machinery; 2023. p.1619–1627. DOI:10.1145/3583131.3590494

92. Zhang Y., Cai Y. Adaptive dynamic self-learning grey wolf optimization algorithm for solving global optimization problems and engineering problems. *Mathematical Biosciences and Engineering.* 2024;21(3):3910–3943. DOI:10.3934/mbe.2024174. EDN:UGPDBW

93. Barrion M.H., Bandala A., Maningo J.M., Dadios E., Naguib R. Advancing Robotic Swarms with Blockchain Technology: A Dynamic Two-Factor Authentication Consensus Framework. *Research Square*. 2024. DOI:10.21203/rs.3.rs-5301694/v1
94. Yang H. Swarm Contract: A Multi-Sovereign Agent Consensus Mechanism. *arXiv:2412.19256*. 2024. DOI:10.48550/arXiv.2412.19256
95. Li Y. Quantum Ant Colony Algorithm for Solving the Traveling Salesman Problem: A Theoretical and Practical Analysis. *Applied and Computational Engineering*. 2024;110(1):175–181. DOI:10.54254/2755-2721/110/2024MELB0121
96. Tajabadi M., Heider D. Fair swarm learning: Improving incentives for collaboration by a fair reward mechanism. *Knowledge-Based Systems*. 2024;304:112451. DOI:10.1016/j.knosys.2024.112451. EDN:UOAGIK
97. Moustafa N. GH-Twin: Graph Learning Empowered Hierarchical Digital Twin for Optimizing Self-Healing Networks. *Sustainable Machine Intelligence Journal*. 2024;8:35–45. DOI:10.61356/smij.2024.8289. EDN:DNPELS
98. Wang N., Wu Y., Lorenzo B., Liu B. Semantic-Aware Architecture Design for a Lifelong Swarm Metaverse. *IEEE Internet of Things Journal*. 2025;12(9):12468–12482. DOI:10.1109/JIOT.2024.3520518

Статья поступила в редакцию 23.05.2025; одобрена после рецензирования 27.06.2025; принята к публикации 01.07.2025.
The article was submitted 23.05.2025; approved after reviewing 27.06.2025; accepted for publication 01.07.2025.

Информация об авторах:

АДОНИН Леонид Сергеевич
кандидат биологических наук, и. о. заведующего кафедрой конструирования и производства радиоэлектронных средств Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
https://orcid.org/0000-0003-1563-4615

ВЛАДЫКО Андрей Геннадьевич
кандидат технических наук, декан факультета радиоэлектронных систем и робототехники 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 Deputy editor-in-chief of "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 have 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 004.9
https://doi.org/10.31854/1813-324X-2025-11-3-26-36
EDN:DVEOYM

Разработка системы AMS для университета: потребности в системе управленческого учета

Александр Борисович Гольдштейн[1,2], goldstein@sut.ru
Сергей Викторович Кисляков[1,2] ✉, kislyakov@sut.ru
Артём Алексеевич Кузнецов[3], avoit5@yandex.ru
Егор Андреевич Лочкарев[4], lochkarev.egor00@mail.ru
Илья Андреевич Рыбаков[5], ifisher37bonch@gmail.com
Даниил Игоревич Сухомлинов[4], d.sukhomlinov.spb@gmail.com

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация
[2]ООО «НТЦ АРГУС», Санкт-Петербург, 197198, Российская Федерация
[3]АО «Селектел», Санкт-Петербург, 196006, Российская Федерация
[4]ООО «placeholder», Санкт-Петербург, 197191, Российская Федерация
[5]ООО «НТЦ ПРОТЕЙ», Санкт-Петербург, 194044, Российская Федерация

Аннотация

Актуальность. *Сегодня университеты – это крупные организации, обладающие большим количеством активов, начиная от недвижимости и заканчивая оборудованием и расходными материалами. Это оборудование имеет свой жизненный цикл, а университетам необходимо поддерживать не только работоспособность оборудования, но и осуществлять функции классической технической поддержки пользователей этого оборудования. Они сталкиваются с проблемами управления активами из-за устаревших бумажных методов учета. Рост объемов активов приводит к сложностям управления их жизненным циклом.*

Цель исследования *заключается в повышении эффективности управления активами университета за счет разработки системы AMS (аббр. от англ. Asset Management System) на основе открытой цифровой архитектуры (ODA, аббр. от англ. Open Digital Architecture), устраняющей пробелы в автоматизации процессов учета и анализа. Для реализации цели исследования использовался объектно-ориентированный анализ (диаграммы прецедентов и последовательности), концептуальное моделирование, а также проектирование с применением микросервисной архитектуры и стандартов ODA.*

Решение. *Разработаны функциональные требования (например, автоматизация списания оборудования, генерация инвентарных номеров) и нефункциональные (производительность, безопасность), а также архитектура системы на основе компонентов ODA.*

Новизна. *ODA пришла на смену давно существующим фреймворкам, таким как NGOSS и Framworx (TM Forum). Предложен подход к построению системы AMS на компонентах ODA.* ***Теоретическая значимость*** *определяется разработкой модели системы на новейшем фреймворке ODA, а* ***практическая значимость*** *– в непосредственно прикладном смысле данной задачи.*

Ключевые слова: *система управления активами (AMS), микросервисы, открытая цифровая архитектура (ODA), автоматизация процессов, интеграция систем, Asset Management*

Ссылка для цитирования: Гольдштейн А.Б., Кисляков С.В., Кузнецов А.А., Лочкарев Е.А., Рыбаков И.А., Сухомлинов Д.И. Разработка системы AMS для университета: потребности в системе управленческого учета // Труды учебных заведений связи. 2025. Т. 11. № 3. С. 26–36. DOI:10.31854/1813-324X-2025-11-3-26-36. EDN:DVEOYM

Original research
https://doi.org/10.31854/1813-324X-2025-11-3-26-36
EDN:DVEOYM

Development of Management Accounting System Model for Universities Based on Open Digital Architecture

Alexandr B. Goldstein[1,2], goldstein@sut.ru
Sergey V. Kislyakov[1,2] ✉, kislyakov@sut.ru
Artem A. Kuznetsov[3], avoit5@yandex.ru
Egor A. Lochkarev[4], lochkarev.egor00@mail.ru
Ilya A. Rybakov[5], ifisher37bonch@gmail.com
Daniil I. Sukhomlinov[4], d.sukhomlinov.spb@gmail.com

[1]The Bonch-Bruevich Saint Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation
[2]LLC "ARGUS",
St. Petersburg, 197198, Russian Federation
[3]CJSC «Selectel»,
St. Petersburg, 196006, Russian Federation
[4]LLC «placeholder»,
St. Petersburg, 197191, Russian Federation
[5]LLC «RTC PROTEI»,
St. Petersburg, 194044, Russian Federation

Annotation

Relevance*. Today, universities are equipped with a large number of modern telecommunications and IT equipment, and other material assets. The university needs to manage the life cycle of all material assets.* ***The purpose of the research*** *is to improve the efficiency of university asset management by developing an AMS (Asset Management System) based on an open digital architecture (ODA), which eliminates gaps in the automation of accounting and analysis processes. The growth of data volumes and the need for integration with IT infrastructure underscore the relevance of developing flexible digital solutions.*

Research methods*: Object-oriented analysis, conceptual modeling, and design based on microservices architecture and ODA standards were applied.*

Results. *An AMS system was developed, including functional modules for automating equipment write-offs, generating inventory numbers, and analytics. The system integrates via API using ODA-components (TMFC014, TMFC039, etc.), ensuring flexibility and scalability.*

For the first time*, an approach to decomposing AMS into ODA-components is proposed, enhancing resource management efficiency and process automation. The work demonstrates the dependence of system flexibility on the application of ODA and creates a foundation for further scaling.*

The theoretical significance *is determined by the development of a system model on the latest ODA framework****,*** *and* ***the practical significance*** *is that the proposed result can be practically used to develop specific AMS solutions.*

Keywords: *asset management system (AMS), microservices, open digital architecture (ODA), process automation, system integration, resource management, data analytics, data security*

For citation: Goldstein A.B., Kislyakov S.V., Kuznetsov A.A., Lochkarev E.A., Rybakov I.A., Sukhomlinov D.I. Development of Management Accounting System Model for Universities Based on Open Digital Architecture. *Proceedings of Telecommunication Universities.* 2025;11(3):26–36. (in Russ.) DOI:10.31854/1813-324X-2025-11-3-26-36. EDN:DVEOYM

Цифровизация процессов: преимущества перед бумажным учетом

Современные университеты ежедневно сталкиваются с огромным объемом данных: это информация о сотрудниках, образовательных программах, учебных помещениях, техническом оборудовании, финансовых ресурсах и партнерских проектах. Управление всеми этими данными на бумаге или через разрозненные таблицы создает множество проблем:

– неэффективность: бумажные документы требуют много времени на обработку, поиск и внесение изменений; процессы согласования и утверждения становятся долгими, особенно, если участвует множество подразделений;

– ошибки и потери данных: ручной ввод информации увеличивает вероятность ошибок; бумажные документы подвержены рискам физической утраты (например, пожар, затопление) и износу;

– ограниченная доступность: доступ к данным ограничен только физическим местонахождением документов; трудности с предоставлением информации заинтересованным сторонам в реальном времени;

– отсутствие аналитики: отдельные электронные файлы в табличном формате или разрозненные (несвязанные) программные системы не позволяют эффективно собирать, агрегировать и анализировать данные; отсутствие аналитики осложняет принятие обоснованных решений.

Цифровая система управленческого учета решает эти проблемы, предоставляя единое пространство для хранения, анализа и управления всеми ресурсами университета.

К основным преимуществам цифровизации можно отнести:

– ускорение процессов: быстрый доступ к данным и автоматизация рутинных операций; мгновенное обновление информации;

– снижение рисков: цифровые данные защищены от потери (например, через резервное копирование); эффективные системы безопасности предотвращают несанкционированный доступ;

– прозрачность и контроль: все действия фиксируются в системе, что облегчает аудит; легче видеть полную картину текущего состояния ресурсов;

– поддержка аналитики и прогнозирования: возможности анализа больших данных позволяют оценивать эффективность и планировать развитие.

Аналогичные преимущества цифровизации демонстрируются в других образовательных системах, например, в веб-системе E-Raport, которая упрощает обработку оценок и предоставляет доступ к данным в реальном времени [1].

Цифровая система управленческого учета представляет интерес для администрации вуза, так как она открывает перед руководством университета новые горизонты управления, выгоды от которых указаны на рисунке 1.

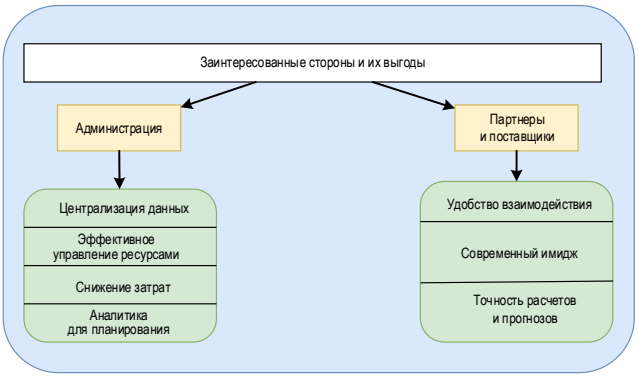


Рис. 1. Анализ востребованности продукта

Fig. 1. Analysis of Product Demand

Централизации данных свойственно хранение всех типов информации в одном месте – от информации о финансах до учета оборудования. В случае *эффективного управления ресурсами* видна текущая нагрузка и доступность аудиторий, оборудования, преподавателей. Еще одна выгода от цифровизации – *снижение затрат* (оптимизация процессов снижает административные издержки). На основе текущих данных можно прогнозировать потребности (*аналитика для планирования*).

Кроме того, для партнеров и поставщиков цифровизация делает университет более привлекательным и надежным, особенно когда реализована интеграция с другими ИТ-системами поддержки процессов и аналитики. В этой связи можно выделить ряд преимуществ: *удобство взаимодействия* (автоматизированные процессы работы с документами и договорами); *современный имидж* (цифровая система демонстрирует технологическую зрелость университета, что повышает его репутацию); *точность расчетов и прогнозов* (партнеры видят, что университет управляет своими ресурсами профессионально).

Таким образом, цифровая система становится мостом между университетом и внешними партнерами, укрепляя доверие и открывая новые возможности для сотрудничества.

Интеграция системы управленческого учета в IT-инфраструктуру университета

Микросервисы – это архитектурный подход, предполагающий, что система состоит из небольших независимых сервисов, каждый из которых отвечает за выполнение определенных функций. Такой подход обеспечивает гибкость, масштабируемость и легкость интеграции с существующими системами [2]. Основными преимуществами микросервисов в разработке приложений являются гибкость интеграции, масштабируемость, минимизация рисков [3].

Гибкость интеграции. Микросервисы позволяют подключить новые модули системы управленческого учета (AMS, *аббр. от англ.* Asset Management System) к существующим решениям университета, не нарушая их работы. Например, можно интегрировать управление ресурсами с системой планирования ресурсов (ERP, *аббр. от англ*. Enterprise Resource Planning), системой технической поддержки или системой управления расписаниями.

Масштабируемость. При увеличении нагрузки (например, во время вступительной кампании) можно масштабировать только те сервисы, которые нуждаются в повышении производительности, без необходимости расширения всей системы.

Минимизация рисков. В случае сбоя одного микросервиса остальные продолжают работать, что обеспечивает стабильность всей системы.

Интеграция AMS в существующую инфраструктуру университета с использованием микросервисов и компонентов ODA (*аббр. от англ*. Open Digital Architecture – открытой цифровой архитектуры) включает 6 этапов. Основные этапы интеграции системы отражены на схеме (рисунок 2).

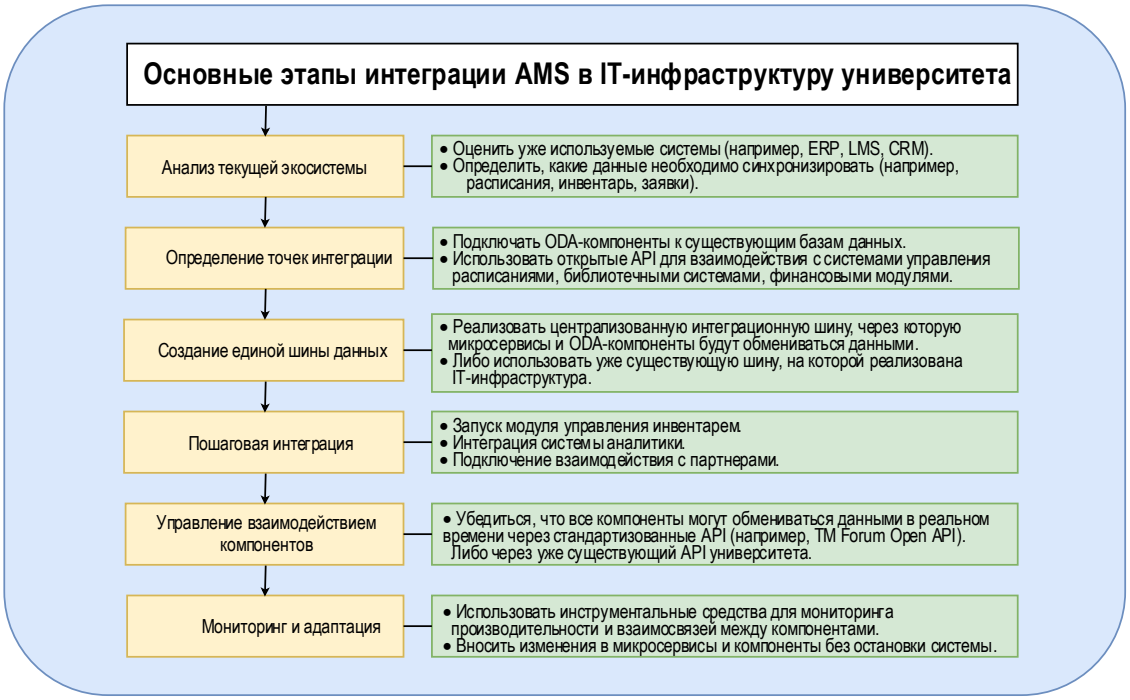


Рис. 2. Этапы интеграции AMS

Fig. 2. The Main Steps of the AMS Integration

Внедрение AMS в ИТ-ландшафт университета

Функциональная архитектура системы AMS строится на основе ключевых блоков, необходимых для эффективного управления:

1) управление ресурсами:

– учет финансовых, материальных и человеческих ресурсов;

– контроль состояния и доступности оборудования, аудиторий, библиотечных фондов;

2) учет использования активов:

– мониторинг использования помещений, оборудования и других университетских ресурсов;

– учет технического состояния и планирование обновлений или ремонта;

3) аналитика и отчетность:

– сбор и обработка данных о работе университета;

– подготовка отчетов для администрации, партнеров и государственных структур.

Проектирование компонентов и разработка модели данных системы AMS

Для реализации системы AMS используется современный стек технологий, обеспечивающий гибкость и масштабируемость. Компоненты разрабатываются с использованием Docker / Kubernetes в качестве платформы управления контейнерами, что позволяет обеспечить их независимость и легкую интеграцию. Основными инструментами разработки являются Helm (упрощение управления развертыванием компонентов и их конфигурацией), PostgreSQL (для хранения и управления структурированными данными, связанными с активами, пользователями и процессами) и Grafana (для визуализации данных и аналитики, предоставляемой системой). Выбор технологий для AMS основан на их гибкости и масштабируемости, однако в других исследованиях для аналогичных систем управления активами в образовательных

учреждениях применяются более простые стеки, такие как PHP и MySQL, что также обеспечивает достаточную функциональность (https://www.tmforum.org/resources/standard/open-digital-architecture-toolkit).

Разработка моделей данных и интеграции

В ходе исследования было применено два основных подхода в разработке и интеграции: модель данных (SID, *аббр. от англ.* Shared Information and Data Model) и интеграция с существующими системами. *Модель SID* объединяет данные и информацию и применяется в тех случаях, когда необходимо иметь легко масштабируемое и легко интегрируемое решение с другими системами ИТ-ландшафта. Такой подход обеспечивает единообразие данных и поддерживает адаптивность системы к изменяющимся потребностям университета. Применение разработок некоммерческой международной компании TMForum для решения AMS позволит реализовать легкую *интеграцию* с CRM, ERP и другими системами университета благодаря использованию RESTful Open APIs.

Основные этапы проектирования системы AMS

С учетом особенностей университетской деятельности можно выделить пять основных этапов проектирования системы.

Этап 1. Сбор и анализ требований:

– определение ключевых задач системы: управление активами, автоматизация процессов, улучшение взаимодействия с заинтересованными сторонами;

– оценка текущей IT-инфраструктуры университета и определение точек интеграции;

– уточнение требований к безопасности данных и нормативным стандартам (например, защита персональных данных в соответствии с локальными и международными законами).

Этап 2. Проектирование архитектуры:

– разработка архитектуры на основе микросервисного подхода, обеспечивающего модульность и гибкость системы;

– создание карты компонентов системы с учетом ODA-принципов (блок управления активами, системы аналитики и мониторинга; интерфейсные модули для взаимодействия с пользователями) [4];

– определение взаимодействия между компонентами через стандартизированные Open APIs.

Этап 3. Разработка прототипа:

– реализация пилотного проекта на Docker/Kubernetes для проверки работоспособности ключевых функций;

– тестирование базовой функциональности (учет ресурсов, аналитика и интеграция с существующими системами).

Этап 4. Внедрение и интеграция:

– разработка окончательной версии системы с постепенным подключением всех функциональных модулей;

– интеграция AMS с системами университета (LMS, ERP, CRM) через единый API-шлюз;

– постепенный запуск системы, начиная с базовых модулей, с минимальными рисками для рабочих процессов.

Этап 5. Обучение и поддержка:

– проведение тренингов для сотрудников и предоставление инструкций по работе с системой;

– организация службы технической поддержки для решения возникающих вопросов.

Принципы безопасности

Основные принципы безопасности, используемые при проектировании системы AMS: *конфиденциальность* (применяются механизмы шифрования данных в состоянии покоя и при передаче (например, TLS/SSL для взаимодействия через API) https://www.tmforum.org/resources), *целостность* (данные защищаются от несанкционированных изменений через механизмы контроля версий и автоматизированный мониторинг), *доступность* (реализуется резервное копирование и план восстановления в случае аварий, что минимизирует простой системы).

В целях обеспечения безопасности системы на всех этапах – от проектирования до внедрения и эксплуатации, применяются известные подходы:

– архитектура с нулевым доверием (*от англ.* Zero Trust): каждый запрос к системе проходит многофакторную аутентификацию и авторизацию, независимо от источника [5];

– роли и ограничения доступа: пользователи системы (администрация, партнеры) получают доступ только к данным и функциональности, которые необходимы для их задач);

– мониторинг и аудит: постоянный контроль активности пользователей и компонентов для выявления подозрительных действий;

– соответствие нормативным стандартам.

Практические результаты

Для определения более детальных требований обратимся к диаграмме прецедентов (рисунок 3), которая поможет нам визуализировать, как пользователи (акторы) взаимодействуют с системой. Это упрощает восприятие архитектуры системы и функций, которые она предлагает. Диаграмма позволяет четко определить, кто будет взаимодействовать с системой (например, сотрудники ИТ-отдела, бухгалтерия, сотрудники отдела технической поддержки и т. д.). Это помогает понять, какие роли необходимы и какие функции нужно разработать для каждой из них [2].

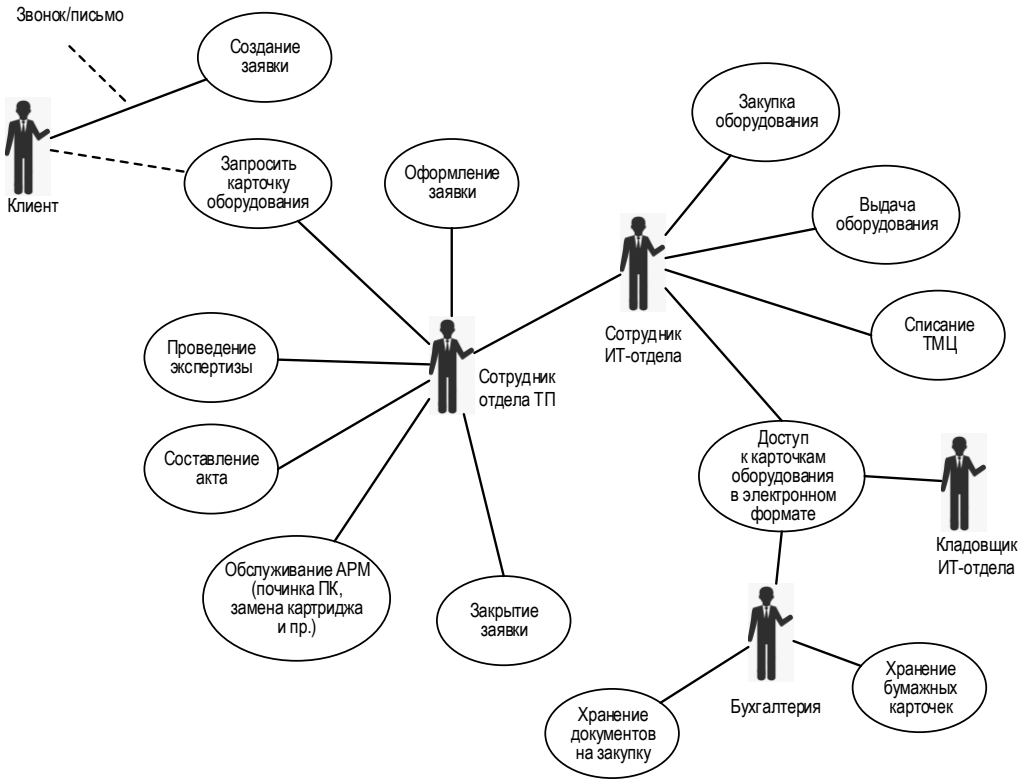


Рис. 3. Диаграмма прецедентов

Fig. 3. Diagram of Precedents

При введении системы AMS можно выделить следующих акторов и их взаимодействия (прецеденты): клиент (заказчик), сотрудник отдела технической поддержки, сотрудник ИТ-отдела, кладовщик ИТ-отдела и бухгалтерия. Указанные отделы взаимодействуют в рамках разных бизнес-процессов (см. рисунок 3).

В любом университете традиционно функционирует три взаимодействующих подразделения:

– ИТ-отдел, функции которого включают закупку оборудования и программного обеспечения, выдачу его заказчикам и учет;

– отдел эксплуатации (сервис технической поддержки), принимающий заявки на обслуживание – ремонт оборудования, замена картриджей и т. п., а также оказывающий информационную поддержку пользователям;

– бухгалтерия.

С помощью диаграмм прецедентов можно определить и задокументировать требования к системе. Каждое действие пользователей и соответствующие им прецеденты служат основой для определения функциональных требований [1].

Не менее важным инструментом в объектно-ориентированном анализе и проектировании, который используется для визуализации взаимодействий между объектами в определенной последовательности во времени, является диаграмма последовательности. Она показывает, как объекты взаимодействуют между собой в течение определенного сценария, помогает понять, как объекты коммуницируют между собой для выполнения конкретной задачи [4] в рамках конкретных бизнес-процессов. Это особенно полезно для аналитиков и дизайнеров: можно увидеть, как разработанные компоненты будут работать вместе.

На рисунке 4 представлена диаграмма последовательности взаимодействия отделов по работе с заявкой. В первом варианте альтернативного события представлен случай, когда система AMS отсутствует. Необходимо совершать много дополнительных действий для получения карточки оборудования. В случае наличия системы AMS у всех отделов будет доступ к электронной карточке оборудования в любое время.

После описания диаграмм перейдем к описанию требований к системе AMS. Разработка этих требований опирается на лучшие практики управления активами, включая автоматизацию процессов, обеспечение безопасности и производительности, что соответствует современным стандартам систем управления активами [5, 6]. Можно выделить функциональные требования (задачи системы) и нефункциональные (характеристики работы).

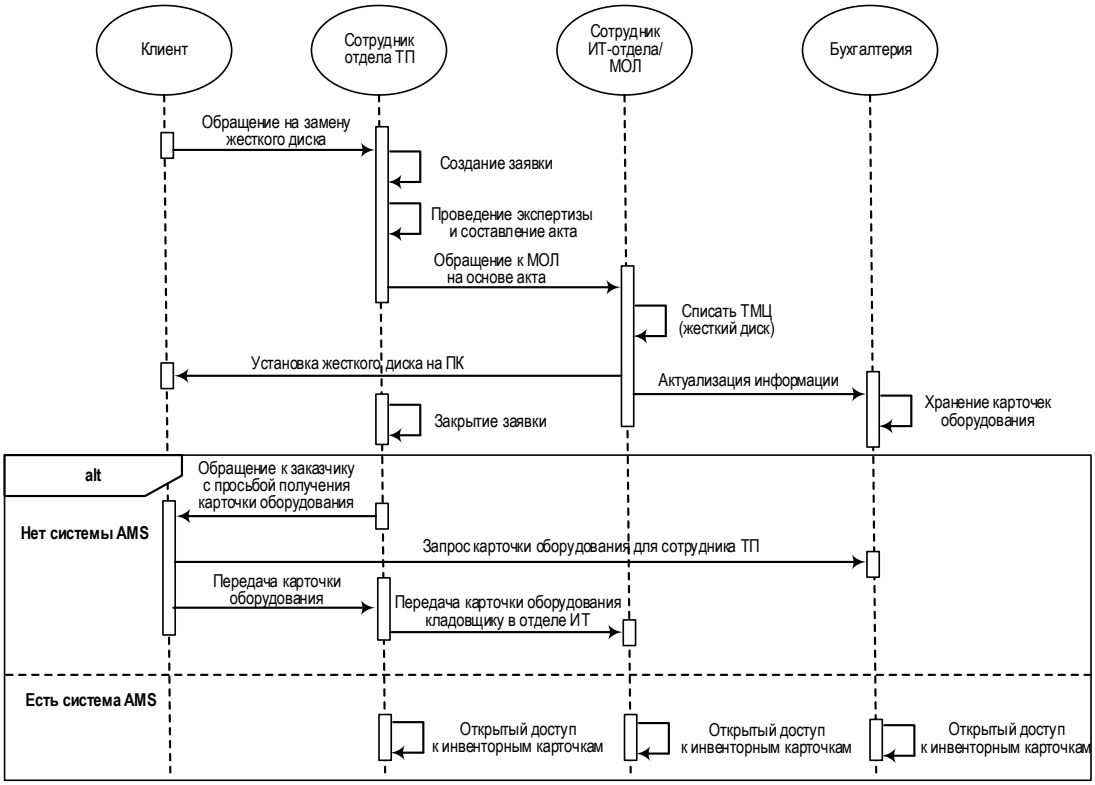


Рис. 4. Диаграмма взаимодействия отделов

Fig. 4. Departments Sequence Diagram

К *функциональным требованиям* можно отнести:

1) списание оборудования (автоматическое создание акта списания с подписями сторон и акта утилизации для снятия оборудования с баланса);

2) учет стоимости (добавление полей «Цена на входе» и «Остаточная стоимость» с сортировкой и списанием объектов ниже заданного порога);

3) генерация инвентарных номеров (автоматическая генерация уникальных номеров для поступающего товара с печатью для наклеивания);

4) печать ярлыков (автоматическая печать ярлыков с инвентарными номерами для инвентаризации);

5) справочник материально-ответственных лиц (учет ФИО, номера кабинета и телефона с возможностью поиска и редактирования);

6) загрузка гарантийных талонов (поддержка загрузки талонов на партию и отдельные экземпляры в систему);

7) работа нескольких пользователей (одновременная работа пользователей с уведомлениями о действиях других);

8) отслеживание конфликтов редактирования (контроль одновременного редактирования данных для сохранения их целостности);

9) опись помещения (формирование описания помещения на основе местоположения товарно-материальных ценностей);

10) генерация расписок для ремонта (автоматическое создание расписок для оформления товарно-материальных ценностей (ТМЦ) в ремонт.

Нефункциональные требования включают в себя:

1) производительность до 5 сек (обработка запросов – создание документов, сортировка, генерация номеров);

2) надежность (доступность системы – не менее 99,9 % с сохранением данных при сбоях);

3) безопасность (шифрование данных, доступ только авторизованным пользователям);

4) хранение (документы хранятся 3 года).

Система AMS на основе открытой цифровой архитектуры

С появлением и развитием технологий, облачных вычислений и мобильных платформ возникла необходимость в создании более гибких решений, способных легко интегрироваться с различными сервисами и платформами. Переход на ODA поддерживается мировыми стандартами, разработанными TM Forum (https://www.tmforum.org). Традиционно, стандарты способствуют унификации и упрощению интеграции систем, повышению гибкости и масштабируемости инноваций в разработке программного обеспечения (https://www.tmforum.org/resources/introductory-guide/oda-component-inventory-v16-0-0-ig1242).

Процесс построения системы AMS на основе концепции ODA включает определение бизнес-требований, выбор группировок бизнес-функций из Функциональной архитектуры ODA, определения программных функций на основе структуры приложений ODA и, наконец, разбиение системы на ODA-компоненты на основе выбранных функций. Результатом будет система, состоящая из множества взаимосвязанных и функционирующих компонентов (таблица 1).

Помимо перечисленных в таблице 1 компонентов ODA, для системы AMS также были выделены все компоненты из блоков ODA Canvas Operators и Engagement Management. Это обусловлено тем, что компоненты этих блоков отвечают за графический интерфейс (GUI, *аббр. от англ.* Graphical User Interface), управление потоками событий и организацию операционных процессов внутри среды выполнения компонентов ODA Canvas внутри ИТ-ландшафта. На рисунке 5 продемонстрировано взаимодействие компонентов ODA из блоков операционных процессов. TMFC039 Agreement Management не связан API, так как его координация и интеграция с остальными компонентами реализована через API TMF 701 Process Flow Management и TMF688 Event Management. TMFC039 необходим для реализации в система справочника, содержащего договоры с различными параметрами.

ТАБЛИЦА 1. Компоненты системы AMS

TABLE 1. AMS System Components

Название компонента	Краткое описание функциональности
Production	
TMFC014 Location Management	Отвечает за управление информацией о местоположениях, например адреса, принадлежность к различным зонам и т. д.
TMFC010 Resource Catalog Management	Организует сбор спецификаций ресурсов, определяющих требования к ним, и предоставляет функционал для отображения клиентского и технического представления ресурсов, а также управления ими на протяжении жизненного цикла
TMFC006 Service Catalog Management	Организует сбор спецификаций услуг, определяющих все требования к ним; Предоставляет функциональность для отображения клиентского и технического представления услуг, позволяя пользователям искать и выбирать необходимые услуги; также включает управление спецификациями, администрирование жизненного цикла услуг и упрощение доступа к ним
TMFC007 Service Order Management	Отвечает за доставку ресурсов клиентского сервиса (CFS) и предоставляет API *ServiceOrder*; Организует процесс доставки, определяя возможные ресурсы и выбирая их из каталога, а также запрашивает обновление выбранных экземпляров ресурсов для доставки CFS
TMFC011 Resource Order Management	Отвечает за выполнение запросов на ресурсы в соответствии с их требованиями; Охватывает все этапы процесса заказа, включая получение и подтверждение заказов, управление доставкой с проверкой доступности ресурсов, отслеживание действий по заказу, сопоставление зависимостей ресурсов, обработку обновлений заказов и отчетность о состоянии жизненного цикла заказа
TMFC032 Supply Chain Management (без спец.)	Включает в себя задачи по планированию ресурсов и услуг, управлению информацией о них, управлению снабжением, запасами, производством, местоположением, транспортировкой, возвратами и логистикой
Intelligence Management	
TMFC038 Resource Performance Management	Обеспечивает доступность и готовность приложений, вычислительных и сетевых ресурсов; Включает в себя создание и управление экземплярами ресурсов, мониторинг и отчетность о возможностях и затратах; Основные обязанности этих процессов включают поддержку внедрения новой инфраструктуры, управление плановыми отключениями, анализ доступности и производительности ресурсов, а также выполнение мероприятий по техническому обслуживанию и ремонту; Кроме того, важными аспектами являются управление запасными частями, оценка угроз и рисков, а также мероприятия по снижению рисков и безопасной конфигурации
TMFC037 Service Performance Management	Отвечает за сбор, контроль, анализ и отчетность о производительности конечного сервиса; Включает в себя мониторинг в реальном времени для обеспечения корректной работы услуг, а также исторический анализ; Функции основаны на данных управления производительностью ресурсов и активных испытаниях производительности, что позволяет получить полное представление о качестве обслуживания; Компонент предоставляет ключевые входные данные для оценки качества сервиса
Party Management	
TMFC039 Agreement Management	Отвечает за создание, хранение, редактирование и отслеживание согласованных соглашений на протяжении всего жизненного цикла; Управляет предложениями, записями принятия и связанными с ними намерениями для установления юридически обязательных соглашений; Кроме того, компонент предоставляет рабочие процессы и шаблоны, которые упрощают сотрудничество и переговоры между сторонами, а также администрирует особенности перевода соглашений в контракты; Обеспечивает безопасное хранение, контроль версий, управление соответствием и уведомления о продлении соглашений

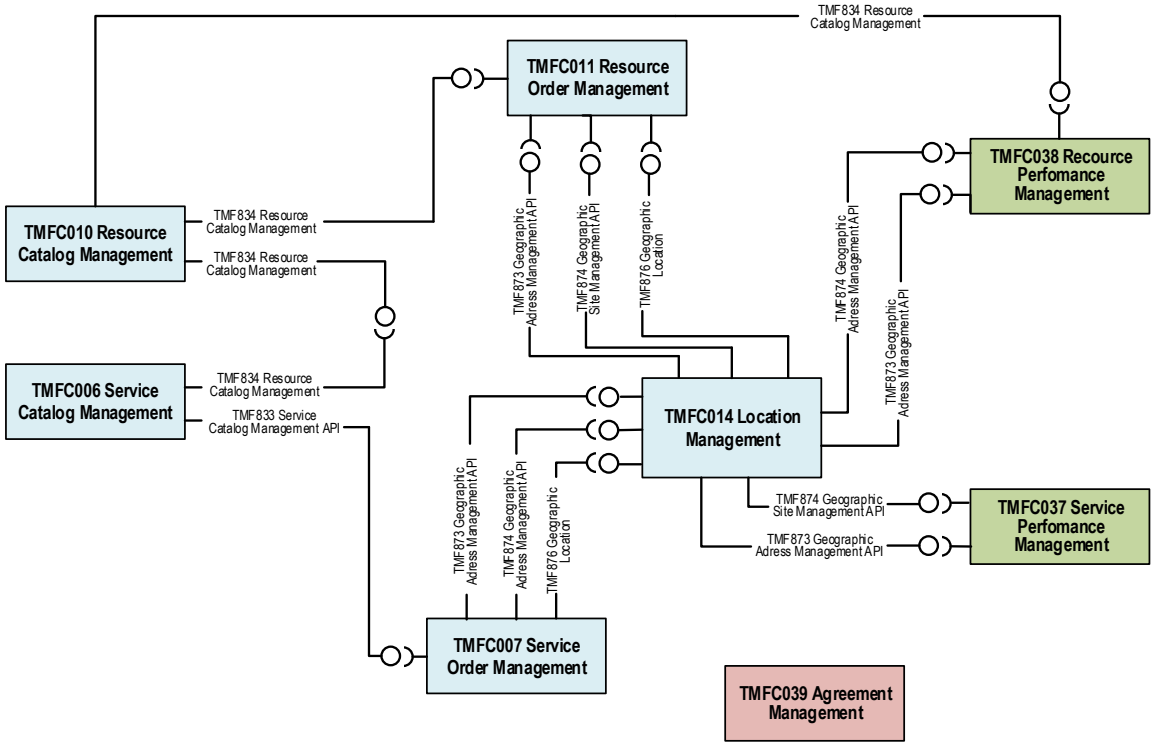


Рис. 5. Взаимодействие компонентов ODA операционных блоков через API

Fig. 5. ODA-Components Interaction through API

Таким образом, система AMS была спроектирована на основе множества компонентов ODA.

Реализация и тестирование системы AMS

Система AMS была реализована на выделенном сервере с использованием контейнеризации через Docker, что обеспечило гибкость и масштабируемость. В качестве основного фреймворка применялся NocoDB – инструмент для создания баз данных с удобным интерфейсом, а для хранения данных использовалась система управления базами данных PostgreSQL, обеспечивающая надежность и производительность. Такой стек технологий позволил быстро развернуть систему и адаптировать ее под нужды университета.

Главная страница системы AMS, реализованная через интерфейс NocoDB (https://nocodb.com/docs/self-hosting/installation/docker-install, отображает доступные базы данных и проекты, предоставляя пользователю удобный доступ к управлению активами. Интерфейс минималистичен: слева расположена панель навигации с разделами *Bases* и *Projects*, а в нижней части – информация о текущем пользователе (например, username@email.com) и кнопка для перехода к облачной версии NocoDB. Главная страница служит отправной точкой для работы с системой, позволяя администраторам и сотрудникам быстро переходить к нужным модулям.

Управление пользователями – одна из ключевых функций AMS, обеспечивающая контроль доступа и распределение ролей. На рисунке 6 показан интерфейс управления пользователями, где отображаются их данные: имена (например, *Test_Observer*, *Test_Creator*), email-адреса, роли (Наблюдатель, Создатель, Владелец) и статус активности. Также указывается время последнего входа (например, «1 d ago» или «2 h ago»), что помогает отслеживать активность. Этот модуль позволяет администратору добавлять, редактировать или удалять пользователей, а также управлять их правами, что соответствует требованиям безопасности и многопользовательской работы, описанным ранее.

В качестве отправной точки для анализа, разработки и тестирования использовалась платформа «АРГУС AMS» (рисунок 7), позволяющая создавать гибкие проектные решения под самые разные архитектуры предприятий и их бизнес-процессов за счет сформированной на принципах low-code инфраструктуры и возможностей JMIX.

AMS-компонент включает 6 базовых сущностей (средний слой AMS-компонент). Выделение таких сущностей позволяет реализовывать различные сценарии управленческого учета, придавая этим понятиям различный бизнес-смысл. Эти объекты являются самостоятельными, их можно настраивать независимо.

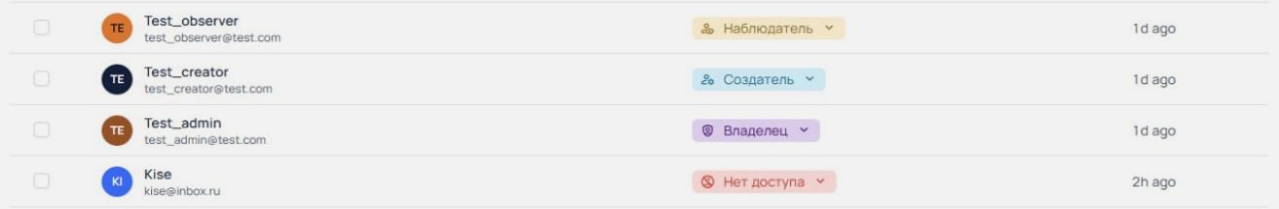


Рис. 6. Интерфейс управления пользователями

Fig. 6. User's Management Interface

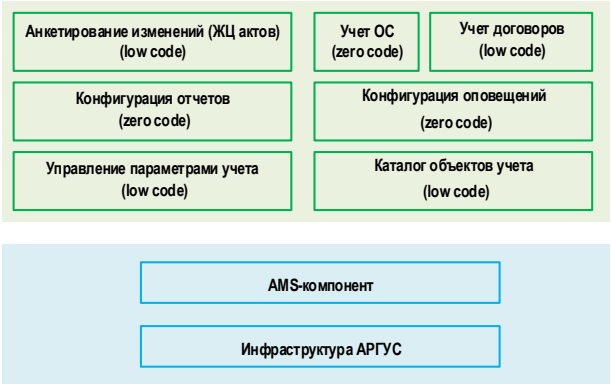


Рис. 7. Платформа «АРГУС AMS»

Fig. 7. «ARGUS AMS» Software Platform

Сущности AMS-компонента реализованы по технологии «low code», что не потребовало и не потребует писать большого количества строк кода для адаптации системы под конкретные задачи университета. Это позволит в дальнейшем не нести больших затрат на программирование и программистов. Необходимые доработки под конкретный проект и сценарии можно будет реализовывать по технологии «low code». Верхний слой платформы AMS содержит сущности, которые настраиваются и взаимоувязываются в режиме «zero-code», когда не требуется знание языков программирования.

Заключение

В результате разработана модель системы управления активами (AMS) для университета, основанная на новейшем фреймворке – открытой цифровой архитектуры (ODA). Система решает ключевые проблемы традиционного бумажного учета, такие как неэффективность, высокий риск ошибок и отсутствие аналитических возможностей, обеспечивая автоматизацию процессов, централизованное хранение данных и интеграцию с существующей IT-инфраструктурой через стандартизированные API.

Разработанные функциональные требования, включая автоматизацию списания оборудования, генерацию инвентарных номеров и управление справочниками, а также нефункциональные требования (производительность, безопасность, масштабируемость), позволили создать гибкое и устойчивое решение. Применение компонентов ODA, таких как TMFC014 Location Management и TMFC039 Agreement Management, обеспечило модульность системы и возможность ее дальнейшего масштабирования. Использование современных технологий (Docker/Kubernetes, PostgreSQL, Grafana) и подходов к безопасности (zero trust, шифрование данных) гарантирует надежность и защиту данных на всех этапах эксплуатации.

Новизна работы заключается в предложенном подходе к декомпозиции «монолитной» AMS на компоненты ODA с учетом специфики управления активами, что отличает решение от традиционных систем. Теоретическая значимость исследования состоит в установлении зависимости между гибкостью системы и применением ODA, а практическая – в предоставлении инструмента для автоматизации процессов, улучшения аналитики и поддержки принятия решений на основе данных.

Перспективы дальнейших исследований включают внедрение и тестирование прототипа системы в реальных условиях университета, а также расширение функциональности AMS за счет добавления модулей для прогнозирования потребностей и управления проектами с партнерами.

ODA позволяет разрабатывать системы, автоматизирующие любой бизнес, так как именно компонентный подход вкупе с открытыми или стандартными API (прикладными программными интерфейсами) дает максимальную гибкость в архитектуре и функциональности. Если за основу разработки взять платформу JMIX, то это позволит в дальнейшем не нести больших затрат на программирование и программистов. Необходимые доработки под конкретный проект и сценарии можно будет реализовывать по технологии «low code».

Список источников

1. Febriyanto E., Naufal R.S., Sulistiawati S. Planning of the Web-based E-Raport Assessment System // Aptisi Transactions on Technopreneurship. 2020. Vol. 2. Iss. 1. PP. 34–44. DOI:10.34306/att.v2i1.27

2. Кисляков С.В., Майоров В.В. Разработка бизнес-процесса подключения услуги на основе TM Forum Open Digital Architecture // XI Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (АПИНО 2022, Санкт-Петербург, Российская Федерация, 15–16 февраля 2022 г.). СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2022. Т. 1. С. 551–556. EDN:FFGRMD

3. Iluore O.E., Onose A.M., Emetere M. Development of asset management model using real-time equipment monitoring (RTEM): case study of an industrial company // Cogent Business & Management. 2020. Vol. 7. Iss. 1. DOI:10.1080/23311975.2020.1763649

4. Гольдштейн А.Б., Кисляков С.В. Современные подходы к автоматизации бизнес-процессов операторов связи. СПб.: СПбГУТ, 2020. 84 с.

5. Гольдштейн А.Б., Кисляков С.В. Концепция открытой цифровой архитектуры: эволюция или революция? // Вестник связи. 2022. № 6. С. 21–25. EDN:GVAFPF

6. Гольдштейн А.Б., Кисляков С.В., Феноменов М.А. Открытая цифровая архитектура для разработки систем управления инфокоммуникациями. СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2024. 77 с. EDN:AOKPJR

References

1. Febriyanto E., Naufal R.S., Sulistiawati S. Planning of the Web-based E-Raport Assessment System. *Aptisi Transactions on Technopreneurship*. 2020;2(1):34–44. DOI:10.34306/att.v2i1.27

2. Kislyakov S., Mayorov V. Development of a Business Process for Service Activation Based on TM Forum Open Digital Architecture. *Proceedings of the XIth International Conference on Infotelecommunications in Science and Education, 1–2 March 2017, St. Petersburg, Russian Federation, vol.1*. St. Petersburg: The Bonch-Bruevich Saint Petersburg State University of Telecommunications Publ.; 2022. p.551–556. (in Russ.) EDN:FFGRMD

3. Iluore O.E., Onose A.M., Emetere M. Development of asset management model using real-time equipment monitoring (RTEM): case study of an industrial company. *Cogent Business & Management*. 2020;7(1). DOI:10.1080/23311975.2020.1763649

4. Goldstein A.B., Kislyakov S.V. *Modern Approaches to Automation of Business Processes of Telecom Operators*. St. Petersburg: The Bonch-Bruevich Saint Petersburg State University of Telecommunications Publ.; 2020. 84 p. (in Russ.)

5. Goldstein A.B., Kislyakov S.V. The concept of open digital architecture: evolution or revolution? *Vestnik svyazi*. 2022;6:21–25. (in Russ.) EDN:GVAFPF

6. Goldstein A.B., Kislyakov S.V., Fenomenov M.A. *Open Digital Architecture for the Development of Infocommunication Management Systems*. St. Petersburg: The Bonch-Bruevich Saint Petersburg State University of Telecommunications Publ.; 2024. 77 p. (in Russ.) EDN:AOKPJR

Статья поступила в редакцию 08.04.2025; одобрена после рецензирования 05.06.2025; принята к публикации 10.06.2025.
The article was submitted 08.04.2025; approved after reviewing 05.06.2025; accepted for publication 10.06.2025.

Информация об авторах:

ГОЛЬДШТЕЙН Александр Борисович — доктор технических наук, профессор, профессор кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, директор ООО «НТЦ АРГУС»
https://orcid.org/0000-0002-4136-4703

КИСЛЯКОВ Сергей Викторович — кандидат технических наук, доцент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, аналитик ООО «НТЦ АРГУС»
https://orcid.org/0000-0001-8842-7903

КУЗНЕЦОВ Артём Алексеевич — инженер АО «Селектел»
https://orcid.org/0009-0001-6624-2868

ЛОЧКАРЕВ Егор Андреевич — инженер ООО «placeholder»
https://orcid.org/0009-0009-1418-0018

РЫБАКОВ Илья Андреевич — инженер ООО «НТЦ ПРОТЕЙ»
https://orcid.org/0009-0006-4173-087X

СУХОМЛИНОВ Даниил Игоревич — инженер ООО «placeholder»
https://orcid.org/0009-0008-7304-270X

Авторы сообщают об отсутствии конфликтов интересов.
The authors declare no conflicts of interests.

Научная статья
УДК 656.254.1
https://doi.org/10.31854/1813-324X-2025-11-3-37-46
EDN:IZBJBW

Расчет затухания сигнала в системах видеонаблюдения на железнодорожных переездах, в соответствии с модернизированной моделью COST-231 Hata

Елена Владимировна Казакевич[1], kev-pgups@yandex.ru
Анна Андреевна Маслова[1], bloodyelis@yandex.ru
Артем Игоревич Алексеев[1], alekseevartem-i@yandex.ru
Илья Сергеевич Гришанов[1], ilia911119@gmail.com
Федор Алексеевич Прошин[1], fedorproshin@gmail.com
Сергей Викторович Дворников[2] ✉, practicdsv@yandex.ru

[1]Петербургский государственный университет путей сообщения Императора Александра I, Санкт-Петербург, 190031, Российская Федерация
[2]Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, 190000, Российская Федерация

Аннотация

Актуальность. *Необходимость интеллектуального видеонаблюдения обусловлена нехваткой контроля отсутствия автотранспорта со стороны дежурного по переезду, из-за чего существует риск несвоевременного обнаружения препятствия машинистом. Для построения системы интеллектуального видеонаблюдения на неохраняемых переездах предлагается использовать систему стандарта 4G в выделенном для ОАО «РЖД» диапазоне частот от 1785 до 1805 МГц.*
Цель: *создание модели, позволяющей исследовать и моделировать зависимость затухания от дальности связи для систем интеллектуального видеонаблюдения на неохраняемых железнодорожных переездах.*
Методы: *использование математической модели COST-231 Hata, основанной на эмпирических соотношениях, учитывающих тип местности, частоту радиосигнала, абсолютные размеры объектов, перекрывающих трассу, расстояние между ними, а также высоты мачт базовых станций и антенн мобильных абонентов.*
Результаты: *полученное уточненное выражение модели для рассматриваемых условий определяет зависимость затухания на трассе радиоканала от расстояния между базовой станцией и пользовательским оборудованием платформ видеонаблюдений на основе сетей 4G для неохраняемых переездов, находящихся на перегоне вне городской застройки. В модели учитываются время реакции машиниста и длина тормозного пути для подвижного состава различных типов.*
Практическая значимость: *результаты работы могут использоваться в проектировании систем видеонаблюдения на железнодорожном транспорте на неохраняемых переездах с учетом скорости движения поездов на рассматриваемом участке.*

Ключевые слова: *модель COST-231 Hata, затухание сигнала, платформа видеонаблюдения, неохраняемый железнодорожный переезд, тормозной путь подвижного состава*

Ссылка для цитирования: Казакевич Е.В., Маслова А.А., Алексеев А.И., Гришанов И.С., Прошин Ф.А., Дворников С.В. Расчет затухания сигнала в системах видеонаблюдения на железнодорожных переездах, в соответствии с модернизированной моделью COST-231 Hata // Труды учебных заведений связи. 2025. Т. 11. № 3. С. 37–46. DOI:10.31854/1813-324X-2025-11-3-37-46. EDN:IZBJBW

Original research
https://doi.org/10.31854/1813-324X-2025-11-3-37-46
EDN:IZBJBW

Calculation of Signal Attenuation in Video Surveillance Systems at Railway Crossings, in Accordance with the Modernized COST-231 Hata Model

Elena V. Kazakevich[1], kev-pgups@yandex.ru
Anna A. Maslova[1], bloodyelis@yandex.ru
Artem I. Alekseev[1], alekseevartem-i@yandex.ru
Ilya S. Grishanov[1], ilia911119@gmail.com
Fedor A. Proshin[1], fedorproshin@gmail.com
Sergey V. Dvornikov[2] ✉, practicdsv@yandex.ru

[1]Emperor Alexander I St. Petersburg State Transport University,
St. Petersburg, 190031, Russian Federation
[2]Saint Petersburg State University of Aerospace Instrumentation,
St. Petersburg, 190000, Russian Federation

Annotation

Relevance*. The need for intelligent video surveillance is due to the lack of control over the situation at unguarded crossings. For this purpose, it is proposed to use a 4G standard system in the frequency range from 1785 to 1805 MHz allocated to Russian Railways.*
Objective*: to create a model that allows us to study and simulate the dependence of attenuation on the communication range for intelligent video surveillance systems at unguarded railway crossings.*
Methods: *using the COST-231 Hata mathematical model based on empirical relationships that take into account the type of terrain, the frequency of the radio signal, the size of objects blocking the route, the distance between them, as well as the heights of base station masts and mobile subscriber antennas.*
Results: *the obtained refined expression of the model for the conditions under consideration determines the dependence of attenuation on the radio channel route on the distance between the base station and the user equipment of video surveillance platforms based on 4G networks for unguarded crossings located on a section outside urban development. The model takes into account the driver's reaction time and the length of the braking distance for rolling stock of various types.*
Practical significance: *the results of the work can be used in the design of video surveillance systems on railway transport at unguarded crossings, taking into account the speed of trains on the section under consideration.*

Keywords: *model COST-231 Hata, signal attenuation, CCTV platform, unguarded railway crossing, braking distance of rolling stock*

For citation: Kazakevich E.V., Maslova A.A., Alekseev A.I., Grishanov I.S., Proshin F.A., Dvornikov S.V. Calculation of Signal Attenuation in Video Surveillance Systems at Railway Crossings, in Accordance with the Modernized COST-231 Hata Model. *Proceedings of Telecommunication Universities.* 2025;11(3):37–46. (in Russ.) DOI:10.31854/1813-324X-2025-11-3-37-46. EDN:IZBJBW

Введение

В настоящее время системы видеонаблюдения внедряются и эксплуатируются в различных областях железнодорожного транспорта: в системах обеспечения транспортной безопасности, охраны, для проведения аттестации в центрах повышения квалификации, а также для видеорегистрации проведения работ сотрудников в целях проверки на со-

блюдение правил охраны труда и при аварийно-восстановительных работах. Одним из наиболее приоритетных направлений применения систем видеонаблюдения является мониторинг и контроль железнодорожных переездов, составляющий основу систем обеспечения безопасности на участках с интенсивным движением поездов и автотранспорта. Особенностью данной области применения, с точки зрения беспроводных систем связи, является повышенная нагрузка на канал, которая обусловлена большим объемом передаваемого трафика. Так как во многих системах видеонаблюдения доступ к общему каналу связи осуществляется посредством радиоканала, то при выборе устройств видеофиксации, необходимых для обеспечения требуемого качества видеозаписи и последующего интеллектуального анализа поступающих данных, возникает следующее противоречие.

С одной стороны, необходим выбор устройств с высоким качеством изображения, способных осуществлять автоматический анализ изображения, обеспечивая увеличение вероятности своевременного обнаружения событий, происходящих на переезде, тем самым повышая оперативность принятия решения ответственными сотрудниками. А с другой стороны, применение таких устройств приводит к существенному увеличению объема передаваемого трафика по радиоканалу, что, в свою очередь, снижает вероятность своевременной доставки данных, т. е. в конечном итоге снижает результирующую эффективность применения систем контроля и мониторинга.

В целях устранения данного противоречия при организации технологических сетей связи ОАО «РЖД» предлагается использовать технологию стандарта LTE в выделенном диапазоне от 1785 до 1805 МГц. Переход к указанным технологиям позволит при минимальной скорости загрузки 25 Мбит/с обеспечить передачу видеоконтента разрешением 4К. Такой подход открывает возможность развертывания систем видеонаблюдения на всех переездах без выделения дополнительных каналов. При этом данные от устройств видеофиксации и от приемопередающего оборудования на локомотиве подвижного состава будут рассматриваться как данные, сформированные пользовательским оборудованием (UE, *аббр. от англ.* User Equipment) в радиусе действия базовой станции eNB (*аббр. от англ.* evolved Node B).

Кроме того, производительность систем видеофиксации может быть повышена, если обеспечить переход построения сети к пикосотовой и фемтосотовой структуры, а также – за счет использования репитеров в качестве единой системы беспроводной связи. Вместе с тем проведенный анализ показал, что в настоящее время отсутствуют относительно простые модели, позволяющие исследовать и моделировать зависимость затухания от дальности связи для систем видеотрансляции на железнодорожных переездах, а также прогнозировать влияние этих факторов на оперативность доставки данных. Таким образом, задача разработки моделей затухания сигналов в радиолиниях стандарта 4G, позволяющих оперативно прогнозировать требуемые скорости передачи данных в сетях беспроводной связи с учетом объема поставляемого трафика в системах видеонаблюдения, используемых на железнодорожных переездах, является актуальной.

Общий подход к организации видеонаблюдения на железнодорожных переездах

Как правило, железнодорожные переезды бывают двух основных типов: охраняемые и неохраняемые. На неохраняемых переездах необходимость интеллектуального видеонаблюдения обусловлена отсутствием контроля со стороны дежурного по переезду наличия или отсутствия препятствий на пути следования подвижного состава [1]. В свою очередь, это приводит к несвоевременному обнаружению транспортных средств со стороны машиниста (когда расстояние до переезда будет меньше необходимой длины тормозного пути). Для реализации системы интеллектуального видеонаблюдения требуется устройство видеофиксации, связанное с сетью передачи данных общетехнологического назначения (СПД ОТН). Локомотив оснащен приемопередатчиком стандарта 4G [2], устанавливающим канал передачи с ближайшей базовой станцией, и дисплеем для трансляции видеоизображения. В случае фиксации на переезде объекта, находящегося дольше установленного времени, система видеонаблюдения начинает трансляцию на дисплей в кабине машиниста [3]. При этом необходимо обеспечить доставку видеосигнала машинисту на расстоянии не менее 2 км на участках обращения скоростных и высокоскоростных пассажирских поездов со скоростью от 140 до 250 км/ч, а с учетом скорости до 400 км/ч на перегонах строящейся высокоскоростной магистрали, – не менее 8 км от железнодорожного переезда [4]. Данное требование обусловлено длиной тормозного пути подвижного состава, которая зависит от средней скорости в расчетном интервале, удельной тормозной силы и сопротивления движению [5]. Иллюстрация к рассматриваемому подходу представлена на рисунке 1.

Высота антенны приемопередатчика стандарта 4G, расположенного на подвижном составе, равна 5 м (данное значение выбрано, исходя из средней высоты локомотива, которое составляет для: поездов «Сапсан» – 4,400 м, «Ласточка» – 4,850 м, 2ТЭ116 – 5,104 м).

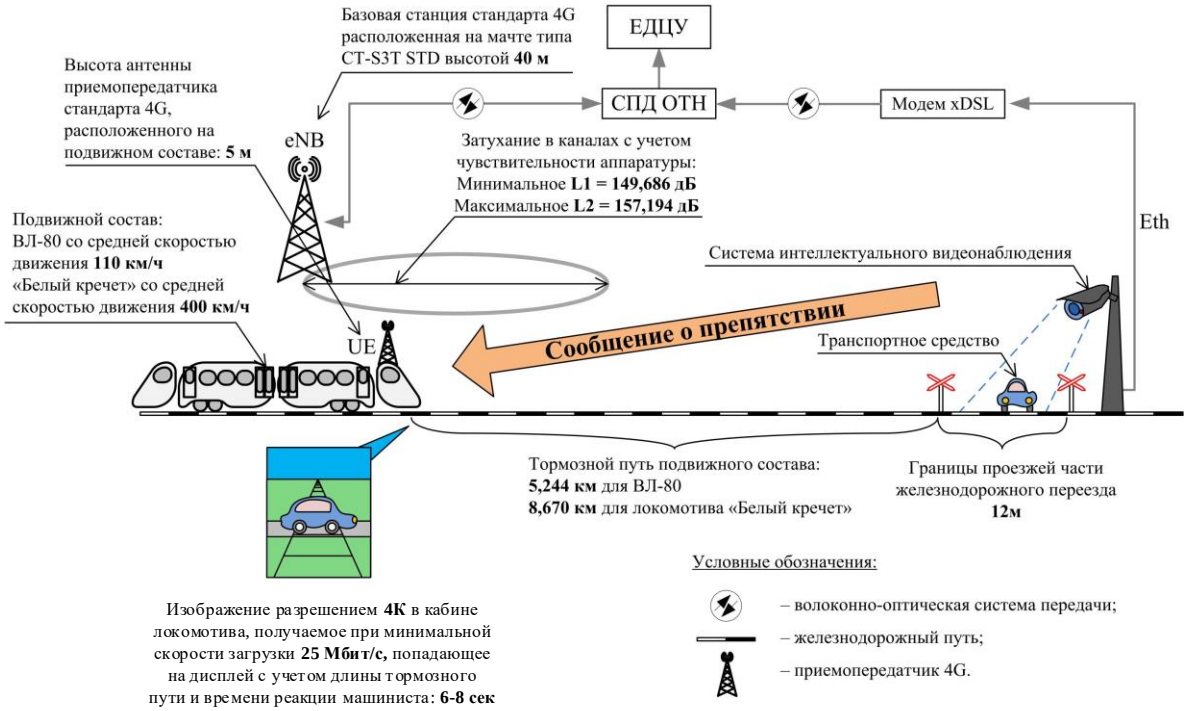


Рис. 1. Общий подход к организации видеонаблюдения на железнодорожном переезде с использованием предлагаемых технологий

Fig. 1. General Approach to Organizing Video Surveillance at a Railway Crossing Using the Proposed Technologies

Высота антенны приемопередатчика стандарта 4G, расположенного на подвижном составе, равна 5 м (данное значение выбрано, исходя из средней высоты локомотива, которое составляет для: поездов «Сапсан» – 4,400 м, «Ласточка» – 4,850 м, 2ТЭ116 – 5,104 м).

Последовательность технических операций, реализуемых в соответствии с моделью, представлена на рисунке 2, который представляет собой временну́ю диаграмму. Она позволяет оценить масштаб временны́х затрат [6], характеризующих работу платформы систем видеонаблюдения на переездах на основе сетей стандарта 4G, при обнаружении посторонних объектов на неохраняемом железнодорожном переезде[1].

Следует понимать, что для успешного функционирования разрабатываемой платформы на основе сетей 4G, уровни сигнала должны соответствовать нормам, определяемым Приказами Министерства связи и массовых коммуникаций Российской Федерации [2,3]. Параметры приемника и базовых станций представлена в таблице 1.

ТАБЛИЦА 1. Параметры приемника и базовых станций согласно Приказам № 128 и № 572

TABLE 1. Requirements for the Parameters of the Receiver and Base Stations According to Orders No. 128 and No. 572

Типы устройств	Технические требования к предельно допустимой максимальной мощности передатчиков для всех диапазонов и частотных каналов стандарта LTE	Значения величины эталонной чувствительности приемника (дБм) для полосы частот 20 МГц
Мобильные терминалы[2]	Не более 23 дБм; допустимое отклонение максимальной мощности – не более 2..3 дБ на интервале измерения не менее одного субкадра (1 мс).	Не более –94
Базовые станции[3]	Не более 24 дБм для одной передающей антенны базовой станции локального радиуса действия	Не более –101,5

[1] Борискин Д.В. Проектно-изыскательские работы Определение оптимального технического решения для переработки структуры и состава оборудования транспортных сетей передачи данных в рамках комплексного инвестиционного проекта «Внедрение системы управления движением электропоездов ЭС2Г «Ласточка» на Московском центральном кольце в автоматическом режиме» с учетом санкционных ограничений.

[2] Приказ Министерства связи и массовых коммуникаций Российской Федерации от 6 июня 2011 года № 128 «Об утверждении правил применения абонентских терминалов сетей подвижной радиотелефонной связи стандарта LTE».

[3] Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 29 октября 2018 года № 572 «Об утверждении Правил применения базовых станций и ретрансляторов сетей подвижной радиотелефонной связи. Часть VI. Правила применения базовых станций и ретрансляторов сетей подвижной радиотелефонной связи стандарта LTE и его модификации LTE-Advanced».

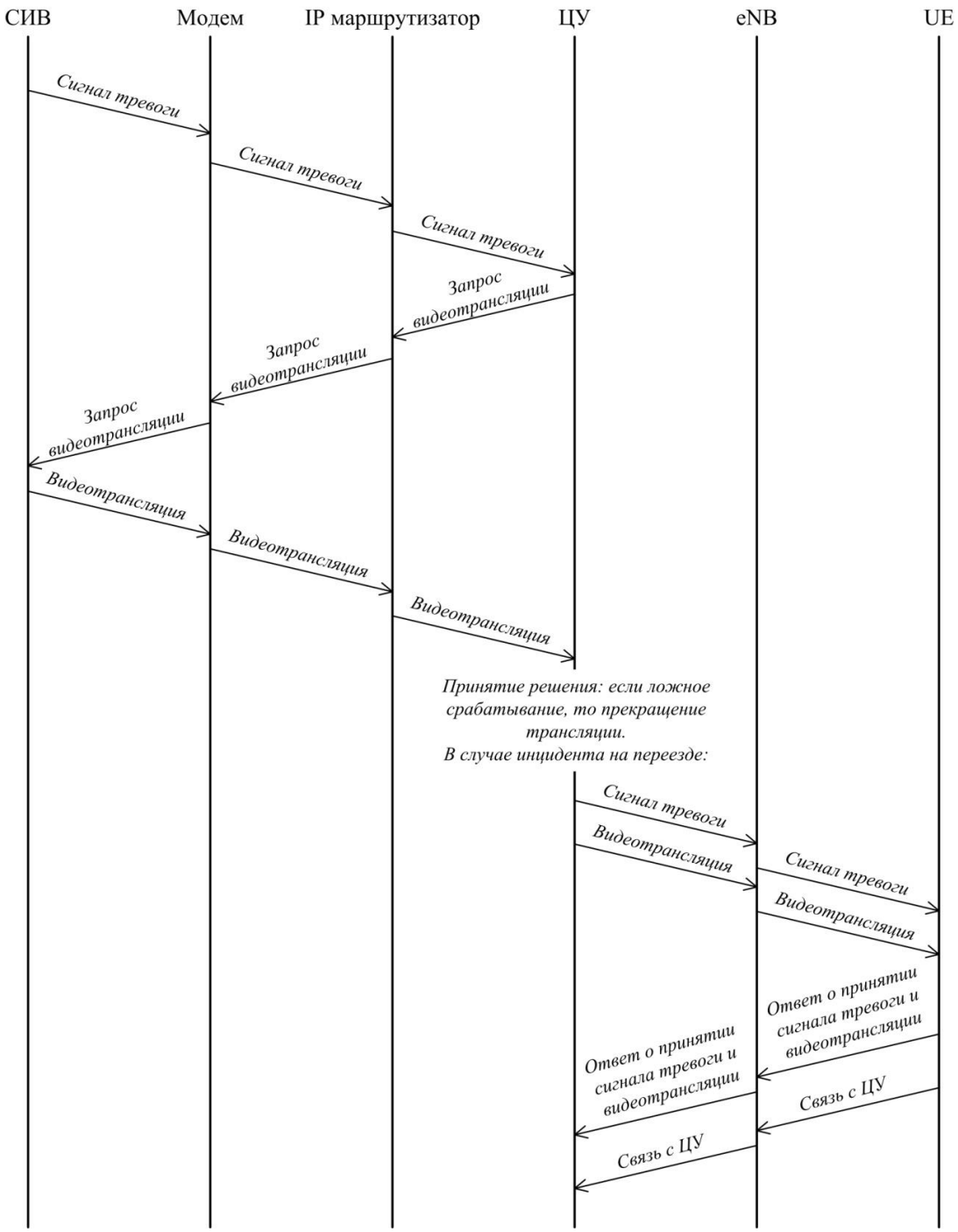


Рис. 2. Последовательность технических операций, реализуемых в соответствии с моделью

Fig. 2. Sequence of Technical Operations Implemented in Accordance with the Model

Модель COST-231 Hata и начальные условия для рассматриваемого случая

В настоящее время для расчета затуханий на трассах радиоканалов сетей LTE наиболее широкое применение получила модель COST-231 Hata, расширяющая функционал более ранних моделей для высокочастотных диапазонов (от 1,5 до 2 ГГц), что позволяет ее практическое применение сообразно к рассматриваемой проблематике [7, 8].

В основе модели COST-231 Hata используются эмпирические соотношения, рассчитанные для множественных трасс радиоканалов, находящихся в условиях различной степени урбанизации местности [9]. Данная модель учитывает следующие параметры: тип местности, частота радиосигнала, абсолютные размеры объектов, перекрывающих трассу, расстояние между ними, а также высоты мачт базовых станций и антенн мобильных абонентов.

В общем виде уравнение затухания в рамках модели COST-231 Hata определяется выражением:

$$L_b = 46{,}3 + 33{,}9\lg f - 13{,}82\lg h_B - a(h_R, f) + \\ +(44{,}9 - 6{,}55\lg h_B)\lg d + C_m, \quad (1)$$

где L_b – среднее затухание радиосигнала на трассе, дБ; f – частота сигнала, МГц; h_B – высота базовой станции, м; h_R – высота мобильной станции, м; d – расстояние между станциями, км; $a(h_R, f)$ – коэффициент коррекции высоты антенны мобильной станции, дБ, который определяется отдельно для городской и пригородной местности; C_m – постоянное смещение, дБ, также зависящее от типа местности.

Расчет значения коэффициента $a(h_R, f)$ для пригородной местности производится согласно выражению:

$$a(h_R, f) = (1{,}1\lg f - 0{,}7)h_R - (1{,}56\lg f - 0{,}8). \quad (2)$$

В свою очередь [10], для городской местности с высоким уровнем урбанизации, коэффициент $a(h_R, f)$ находится, исходя из условий (3). Величина смещения C_m выбирается, исходя из условия (4).

$$a(h_R, f) = \begin{cases} 8{,}29(\lg 1{,}54h_R)^2 - 1{,}1, & \text{если 150 МГц} \le f \le \text{200 МГц;} \\ 3{,}2(\lg 11{,}75h_R)^2 - 4{,}97, & \text{если 200 МГц} < f \le \text{2000 МГц.} \end{cases} \quad (3)$$

$$C_m = \begin{cases} 0 \text{ дБ} & \text{для средних городов и пригородов;} \\ 3 \text{ дБ} & \text{для крупных городов.} \end{cases} \quad (4)$$

Для рассматриваемых условий функционирования платформы видеонаблюдения на основе сетей 4G, устанавливаемых на железнодорожных переездах, параметры в выражениях (1–3) будут определяться следующими значениями:

– $f = 1800$ МГц (диапазон частот, выделенный для сетей 4G на железнодорожном транспорте, в соответствии с Решением ГКРЧ № 18-46-02[4]);

– $h_B = 40$ м (высота мачты базовой станции тип CT-S3T STD, определен спецификацией[5]);

– $h_R = 4{,}78$ м (среднее значение высоты размещения антенны на локомотивах типа «Сапсан», «Ласточка», 2ТЭ116);

– значение коэффициента $a(h_R, f)$ определяется согласно выражению (2), т. к. в исследовании полагалось рассмотрение неохраняемых переездов на перегоне вне городской застройки;

– $C_m = 0$ дБ (соответствует значению местности с низкой степенью урбанизации).

Анализ уравнения указывает на его структурную сложность, которая может быть упрощена с учетом исходных данных, используемых для исследования [11, 12].

Уточненная модель COST-231 Hata для условий проводимого исследования

Учитывая ограниченность частотного диапазона, в исследовании открывается возможность для слагаемых выражения (1), имеющих в своем составе характеристики номиналов частоты, получить расчетные величины, которые будут выступать в качестве постоянных значений.

Коэффициент, учитывающий величину частоты, соответствует следующему значению:

$$33{,}9\lg f = 33{,}9\lg 1800 = 110{,}354.$$

Т. к. высота базовой станции является постоянной, то содержащие ее слагаемые выражения (1) могут быть также предварительно рассчитаны:

$$13{,}82\lg h_B = 13{,}82\lg 40 = 22{,}237;$$
$$44{,}9 - 6{,}55\lg h_B = 44{,}9 - 6{,}55\lg 40 = 34{,}407.$$

Значение коэффициента $a(h_R, f)$ также будет постоянной величиной для последующих расчетов, поскольку оно определяется высотой антенны абонентских терминалов и значением частоты:

$$a(h_R, f) = (1{,}1\lg f - 0{,}7)h_R - (1{,}56\lg f - 0{,}8) = \\ = (1{,}1\lg 1800 - 0{,}7)\cdot 4{,}78 - \\ - (1{,}56\lg 1800 - 0{,}8) = 9{,}492.$$

Для рассматриваемых условий величина C будет равна 0.

Далее, подставляя расчетные коэффициенты, определяемые условиями применения платформы видеонаблюдения на основе сетей 4G, модель COST-231 Hata может быть упрощена следующим образом:

$$L_b = 124{,}925 + 34{,}407\lg d. \quad (5)$$

Представленное уточненное выражение модели (5) для рассматриваемых условий определяет зависимость затухания на трассе радиоканала от расстояния между базовой станцией и пользовательским оборудованием платформ видеонаблюдений

[4] Решение Государственной комиссии по радиочастотам Министерства связи и массовых коммуникаций Российской Федерации от 11 сентября 2018 года № 18-46-02 «О выделении полосы радиочастот 1785–1805 МГц для радиоэлектронных средств сухопутной подвижной службы для создания технологических сетей связи на железнодорожном транспорте».

[5] https://comtech.ru/produktsiya/machtovye-konstruktsii/stalnye-machty/seriya-ct-s3t-std/?ysclid=mbbu6bqcet167210791

на основе сетей 4G для неохраняемых переездов, находящихся на перегоне вне городской застройки.

График затухания сигнала для рабочей частоты 1800 МГц, рассчитанный в соответствии с вышеуказанной моделью (5), представлен на рисунке 3.

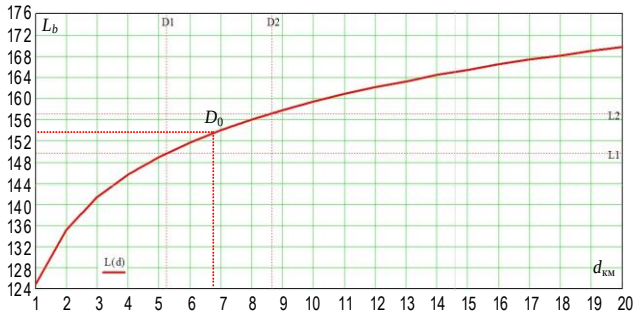


Рис. 3. График затухания сигнала для платформ видеонаблюдений на основе сетей 4G для неохраняемых переездов в условиях с низкой урбанизацией местности

Fig. 3. Signal Attenuation Graph for 4G-Based Video Surveillance Platforms for Unguarded Crossings in Low-Urbanization Areas

Ось абсцисс (см. рисунок 3), характеризующая дальность дистанции связи, представлена в км, а ось ординат, характеризующая уровень затухания на трассе, – в дБ. Величина $D1 = 5{,}244$ км – дальность, определяемая временем реакции машиниста (6–8 сек) и тормозному пути для локомотивов типа ВЛ-80 со средней скоростью движения 110 км/ч, соответствующая минимальному затуханию, получаемому в каналах с учетом чувствительности аппаратуры $L1 = 149{,}686$ дБ; $D2 = 8{,}670$ км – дальность, определяемая временем реакции машиниста (6–8 сек) и тормозному пути для локомотива «Белый кречет» со средней скоростью движения 400 км/ч, соответствующая максимальному затуханию $L2 = 157{,}194$ дБ.

Функциональное обозначение платформ видеонаблюдений на основе сетей 4G определяется своевременным информированием машинистов подвижных составов о ситуации на неохраняемых переездах для принятия ими соответствующих мер в случае возникновения внештатных ситуаций. При этом следует понимать, что скорость движения современного подвижного состава достигает 400 км/ч.

При расчетах тормозного пути учитывалась тяговая характеристика локомотива, тип тормозных колодок, виды систем торможения и другие параметры, определяемые в [13]. Известные математические модели тормозного пути рассчитываются персонально для каждого вида подвижного состава. Поэтому в рамках проведенного исследования представлено обобщенное значение.

Кроме того, необходимо учитывать, что длина тормозного пути представляет результат суммирования двух составляющих: подготовительного тормозного пути и действительного. Первый характеризует собой расстояние, которое проходит подвижной состав за время от нажатия крана машинистом, до запуска тормозной системы, а второй – путь, проходимый подвижным составом от начала действия тормозов до полной остановки. Общий тормозной путь рассчитывался в соответствии с выражением [14]:

$$S = 0{,}278 \cdot V_{НТ} \cdot \frac{a - d \cdot i}{b_Т} + S_Д, \qquad (6)$$

где $V_{НТ}$ – скорость начала торможения, км/ч; a, d – коэффициенты, значения которых для грузовых поездов определяются числом осей, а для пассажирских – наличием электропневматических тормозов; i – значение уклона на тормозном пути, ‰ (при спуске значение берется со знаком «минус»); $S_Д$ – действительный тормозной путь, пройденный поездом за время действия тормозов и определяемый путем решения основных уравнений движения поезда графическим методом, в соответствии с методикой, представленной в [15].

При расчете тормозного пути подвижного состава учитывалась его скорость, расстояние, которое он проходит за время реакции машиниста, и фактическое расстояние подготовительного и действительного тормозного пути. Таким образом, тормозной путь для типового пассажирского состава («Сапсан», «Ласточка») будет составлять порядка 8 км (с учетом реакции машиниста не более 6–8 сек, согласно требованиям[6]). За такое время подвижной состав при скорости 400 км/ч пройдет 666–888 м. С учетом тормозного пути общая дистанция срабатывания системы оповещения будет составлять порядка 8,67–8,89 км.

Вместе с тем в известном обзоре технологии LTE [16] указано, что для диапазона 1800 МГц, как наиболее широко используемого в мире, радиус действия оборудования базовых станций LTE ограничивается значением 6,8 км. То есть для расчетных дальностей 8,67–8,89 км как минимум потребуется составная радиолиния. Заметим, что предельная дальность, отмеченная на рисунке 3 как точка $D_0 = 6{,}8$ км, позволяет оценить уровень допустимых затуханий, равный порядка $L_b = 30$ дБ, что позволяет определить требования к оборудованию по эффективной изотропной излучаемой мощности.

В частности, ориентируясь на результаты [17], можно полагать, что для наихудших условий, при которых обеспечивается устойчивая передача данных в формате OFDM для сигналов BPSK (реализующих наилучшую помехоустойчивость приема) с

[6] Система ТСКБМ. Руководство по эксплуатации. Книга 1 НКРМ.424313.003 РЭ.

вероятностью битовой ошибки p_b = 0,001, допустимое значение отношения сигнал / шум (ОСШ) составляет 17,6 дБ. Следовательно, величина ОСШ на выходе передающего тракта оборудования LTE должна составлять порядка 48 дБ. Тогда, зная предельные дальности и требования по вероятности битовой ошибки, можно построить зависимость p_b как функция дальности (рисунок 4).

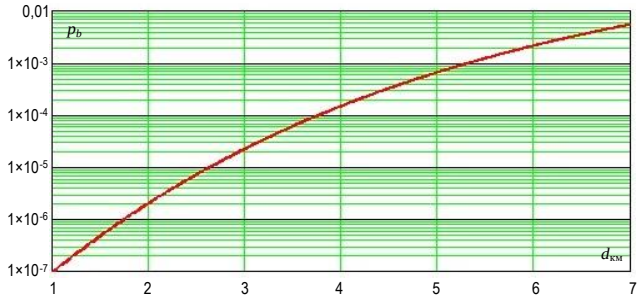


Рис. 4. График зависимости вероятности битовой ошибки в канале от дистанции связи

Fig. 4. Graph of the Dependence of Bit Error Probability in the Channel on the Communication Distance

График (см. рисунок 4) построен для условий, представленных в [17], при использовании сверточного кодера RSC с мягким принятием решения при демодуляции [18].

В ходе исследования, для лучшего раскрытия полученных результатов, было проведено дополнительное моделирование для частот 1000, 1500 и 2000 МГц. При этом высоты размещения антенн полагались равными 30, 100 и 200 м. Дополнительные расчеты были проведены для модели Окумуры – Хаты, в интересах их сравнения с COST-231 Hata. Результаты моделирования показали, что графики потерь для этих моделей внешне совпадают лишь на первый взгляд, особенно на частотах 1000 и 1500 МГц. Однако более детальный анализ показал, что при высоте антенны, равной 200 м, траектория функции потери для модели COST-231 Hata ниже, чем Окумура – Хата. Установлено, что функция потерь для модели COST-231 Hata дает более точные результаты значения коэффициента в условиях городской среды, что коррелирует с результатами, представленными в материалах Всемирного инженерного конгресса, прошедшего в 2014 г. [19]. Согласно опубликованным в научном сборнике исследованиям в условиях прямой видимости, обеспечивающих прямое распространение радиоволн, модель COST-231 Hata рекомендована для использования в стандарте LTE, с расширением диапазона частот расширяется до 2000 МГц. При том, что на высотах антенн базовых станций менее 50 м, в урбанизированных районах ошибка в расчете затухания по модели COST-231 Hata становится значительной.

Кроме того, следует понимать и основные проблемы модели COST-231 Hata для ее дальнейшего использования при планировании сетей LTE. В частности, в настоящее время активно развивается технология LTE с временны́м разделением каналов (*от англ.* Time Division Duplex) – LTE-TDD, разработанная международной коалицией компаний, включая China Mobile, Datang Telecom, Huawei, ZTE, Nokia Solutions and Networks, Qualcomm, Samsung и ST-Ericsson. Технология LTE-TDD отличается не только способом загрузки и выгрузки данных, но и диапазоном частотного спектра, который варьируется от 1850 до 3800 МГц. Но модель COST-231 Hata не адаптирована для расчетов в указанных границах, поэтому необходима разработка новой концепции для расчета затуханий сигнала в более высоких диапазонах частот.

Заключение

По результатам проведенного исследования можно сделать следующие выводы. Мощности типового передатчика базовой станции сети стандарта LTE для предлагаемой платформы видеонаблюдения на основе сетей 4G, устанавливаемых на железнодорожных переездах, недостаточна для обеспечения необходимой дальности, определяемой требованиями безопасности. При этом следует отметить, что в представленных расчетах не учитывались значения коэффициента усиления антенн базовой станции и антенн приемника, а также их чувствительности. Следует также понимать, что выбор типовых устройств не позволит получить желаемый результат. Это обусловлено тем, что для высокоскоростных объектов (при скорости подвижного состава порядка 400 км/ч) выбор оборудования должен производиться с учетом его работы в условиях проявления эффекта Доплера, который при таких скоростях будет существенным. Данные аспекты авторы планируют учесть в дальнейшем исследовании.

Список источников

1. ПНСТ 828-2023 Устройства и системы электросвязи для систем управления железнодорожным подвижным составом в автоматическом и дистанционном режимах. Общие технические требования. 2023.

2. Журавлёва Л.М., Журавлёв О.Е., Лошкарёв В.Л., Курьянцев Д.Г. Видеонаблюдение на базе сети мобильной связи // Автоматика, связь, информатика. 2019. № 9. С. 19–22. EDN:PRSEVE

3. СП 227.1326000.2014 Пересечения железнодорожных линий с линиями транспорта и инженерными сетями. 2014.

4. Журавлёва Л.М., Журавлёв О.Е., Лошкарёв В.Л., Курьянцев Д.Г. Сетевая архитектура систем видеонаблюдения на железнодорожном транспорте // Автоматика, связь, информатика. 2018. № 8. С. 14–18. EDN:LXSTVR

5. Буйносов А.П., Федоров Е.В. Совершенствование метода расчета длины тормозного пути железнодорожного подвижного состава // Известия Транссиба. 2018. № 1(33). С. 13–22. EDN:XQXUXB

6. Прошин Ф.А., Сторожук М.Н., Сторожук Н.Л. Методы синхронизации в сетях связи // Первая миля. 2024. № 2(118). С. 62–69. DOI:10.22184/2070-8963.2024.118.2.62.69. EDN:BQBPFX

7. Дворников С.В., Балыков А.А., Котов А.А. Упрощенная модель расчета потерь сигнала в радиолинии, полученная путем сравнения квадратичной формулы Введенского с существующими эмпирическими моделями // Системы управления, связи и безопасности. 2019. № 2. С. 87–99. DOI:10.24411/2410-9916-2019-10204. EDN:MAFQIB

8. Дворников С.В., Крячко А.Ф., Тимашов П.В. Аппроксимация функций затухания сигналов в эмпирических моделях // Успехи современной радиоэлектроники. 2019. № 11. С. 55–63. DOI:10.18127/j20700784-201911-09. EDN:AVHCQD

9. Аюков Б.А., Дворников С.В., Крячко А.Ф., Левин Я.Я. Вероятностная оценка характеристик системы подвижной радиосвязи стандарта DMR // Успехи современной радиоэлектроники. 2019. № 12. С. 84–94. DOI:10.18127/j20700784-201912-13. EDN:VOUHIW

10. Чикрин Д.Е. Сети и системы телекоммуникаций: курс лекций. Казань: Казанский университет, 2013. 146 с.

11. Дворников С.В., Литкевич Г.Ю., Романенко П.Г., Царелунго А.Б., Дворовой М.О., Федоренко И.В. и др. Эмпирический подход к расчёту зон покрытия цифровых телевизионных передатчиков // Вопросы радиоэлектроники. Серия: Техника телевидения. 2017. № 3. С. 70–75. EDN:ZTCABH

12. Дворников С.В., Власенко В.И., Царелунго А.Б., Балыков А.А., Борисов В.В., Тимашов П.В. Упрощенный подход к расчету затухания сигналов в сетях широкополосного доступа // Вопросы радиоэлектроники. Серия: Техника телевидения. 2019. № 3. С. 93–100. EDN:KMYLBJ

13. Лакин И.И., Семченко В.В. Применение теории массового обслуживания и сетей Петри при анализе параметров системы обслуживания тягового подвижного состава методом математического моделирования // Современные технологии. Системный анализ. Моделирование. 2023. № 4(80). С. 65–77. DOI:10.26731/1813-9108.2023.4(80).65-77. EDN:UNTGVS

14. Фролов Н.О., Ветлугина О.В., Пышный И.М. Тяга поездов: конспект лекций. Екатеринбург: УрГУПС, 2020. 50 с.

15. Корбан В.В., Жебанов А.В. Математические модели для автоматизированной подготовки режимных карт ведения поезда // Наука и образование транспорту. 2019. № 1. С. 36–38. EDN:UPGGYY

16. Cox C. An Introduction to LTE. LTE, LTE-Advanced, SAE, VoLTE and 4G Mobile Communications. Wiley, 2014.

17. Sabir Z., Babar M.I., Shah S.W. Performance enhancement of wireless mobile adhoc networks through improved error correction and ICI cancellation // EURASIP Journal on Advances in Signal Processing. 2012. P. 216. DOI:10.1186/1687-6180-2012-216

18. Дворников С.В., Осадчий А.И., Дворников С.С., Родин Д.В. Демодуляция сигналов на основе обработки их модифицированных распределений // Контроль. Диагностика. 2010. № 10. С. 46–54. EDN:NBEXTJ

19. Ao S.I., Gelman L., Hukins D.W.L., Hunter A., Korsunsky A.M. (Eds.) Proceedings Book of World Congress on Engineering 2014 (WCE 2014, U.K., London, 2–4 July 2014). 2014.

References

1. PNST 828-2023 *Telecommunication devices and systems for railway rolling stock control systems in automatic and remote modes. General technical requirements*. 2023. (in Russ.)

2. Zhuravleva L., Zhuravlev O., Loshkarev V., Kuryantsev J. Video Surveillance on the Basis of a Mobile Communication Network. *Automation, Communications, Informatics*. 2019;9:19–22. (in Russ.) EDN:PRSEVE

3. SP 227.1326000.2014 *Intersections of Railway Lines with Transport Lines and Utility Networks*. 2014. (in Russ.)

4. Zhuravleva L., Zhuravlev O., Loshkarev V., Kuryantsev J. Network Architecture of Video Surveillance Systems in Railway Transport. *Automation, Communications, Informatics*. 2018;8:14–18. (in Russ.) EDN:LXSTVR

5. Buinosov A.P., Fedorov E.V. Improvement of the Method of Calculating the Lengthof the Braking Path of Railway Rolling Stock. *Journal of Transsib Railway Studies*. 2018;1(33):13–22. (in Russ.) EDN:XQXUXB

6. Proshin F.A., Storozhuk M.N., Storozhuk N.L. Methods of Synchronisationin Communication Networks. *Last Mile*. 2024; 2(118):62–69. (in Russ.) DOI:10.22184/2070-8963.2024.118.2.62.69. EDN:BQBPFX

7. Dvornikov S.V., Balykov A.A., Kotov A.A The Simplified Model for Radio Signal Path Loss Computation, Which Was Developed by Comparing the Vvedensky Quadratic Equation with Existing Empirical Models. *Systems of Control, Communication and Security*. 2019;2:87–99. DOI:10.24411/2410-9916-2019-10204. (in Russ.) EDN:MAFQIB

8. Dvornikov S.V., Kraychko A.V., Timashov P.V. Approximation of Signal Attenuation Functions in Empirical Models. *Journal Achievements of Modern Radioelectronics*. 2019;11:55–63. (in Russ.) DOI:10.18127/j20700784-201911-09

9. Ayukov B.A., Dvornikov S.V., Kryachko A.F., Levin Ya.Ya. Probability Evaluation of DMR Mobile Radio Communication System Characteristics. *Journal Achievements of Modern Radioelectronics*. 2019;12:84–94. DOI:10.18127/j20700784-201912-13. (in Russ.) EDN:VOUHIW

10. Chikrin D.E. *Networks and Systems of Telecommunications: Course of Lectures*. Kazan: Kazan University Publ.; 2013. 146 p. (in Russ.)

11. Dvornikov S.V., Litkevich G.Yu., Romanenko P.G., Tsarelungo A.B., Dvorovoy M.O., Fedorenko I.V., et al. Empirical Approach to Calculating the Coverage Areas of Digital Television Transmitters. *Voprosy radioelektroniki. Seriia: Tekhnika televideniia*. 2017;3:70–75. (in Russ.) EDN:ZTCABH

12. Dvornikov S.V., Vlasenko V.I., Tsarelungo F.B., Balykov A.A., Borisov V.V., Timashev P.V. A Simple Approach to Calculating the Drop of Signals in the Networks of Broadband Access. *Voprosy radioelektroniki. Seriia: Tekhnika televideniia*. 2019;3:93–100. (in Russ.) EDN:KMYLBJ

13. Lakin I.I., Semchenko V.V. Application of Queuing Theory and Petri Nets in the Analysis of Traction Rolling Stock Maintenance Parameters by Mathematical Modeling. *Modern Technologies. System analysis. Modeling*. 2023;4(80):65–77. (in Russ.) DOI:10.26731/1813-9108.2023.4(80).65-77. EDN:UNTGVS
14. Frolov N.O., Vetlugina O.V., Pyshny I.M. *Train Traction: Lecture Notes*. Ekaterinburg: Ural State University of Railway Transport Publ.; 2020. 50 p. (in Russ.)
15. Korban V.V., Zhebanov A.V. Mathematical models for automated preparation of train control regime maps. *Nauka i obrazovanie transportu*. 2019;1:36–38. (in Russ.) EDN:UPGGYY
16. Cox C. An Introduction to LTE. LTE, LTE-Advanced, SAE, VoLTE and 4G Mobile Communications. Wiley, 2014.
17. Sabir Z., Babar M.I., Shah S.W. Performance enhancement of wireless mobile adhoc networks through improved error correction and ICI cancellation. *EURASIP Journal on Advances in Signal Processing*. 2012:216. DOI:10.1186/1687-6180-2012-216
18. Dvornikov S.V., Osadchy A.I., Dvornikov S.S., Rodin D.V. Demodulation Based on Processing the Modified Distributions. *Testing. Diagnostics*. 2010;10:46–54. (in Russ.) EDN:NBEXTJ
19. Ao S.I., Gelman L., Hukins D.W.L., Hunter A., Korsunsky A.M. (Eds.) *Proceedings Book of World Congress on Engineering 2014, WCE 2014, 2–4 July 2014, U.K., London*. 2014.

Статья поступила в редакцию 27.03.2025; одобрена после рецензирования 16.04.2025; принята к публикации 22.05.2025.
The article was submitted 27.03.2025; approved after reviewing 16.04.2025; accepted for publication 22.05.2025.

Информация об авторах:

КАЗАКЕВИЧ Елена Владимировна — кандидат технических наук, доцент, заведующий кафедрой «Электрическая связь» Петербургского государственного университета путей сообщения Императора Александра I
https://orcid.org/0000-0002-4549-787X

МАСЛОВА Анна Андреевна — аспирант кафедры «Электрическая связь» Петербургского государственного университета путей сообщения Императора Александра I
https://orcid.org/0009-0001-1573-6171

АЛЕКСЕЕВ Артем Игоревич — аспирант кафедры «Электрическая связь» Петербургского государственного университета путей сообщения Императора Александра I
https://orcid.org/0000-0002-6595-2024

ГРИШАНОВ Илья Сергеевич — аспирант кафедры «Электрическая связь» Петербургского государственного университета путей сообщения Императора Александра I
https://orcid.org/0009-0006-8573-6333

ПРОШИН Федор Алексеевич — ассистент кафедры «Электрическая связь» Петербургского государственного университета путей сообщения Императора Александра I
https://orcid.org/0009-0009-5513-9302

ДВОРНИКОВ Сергей Викторович — доктор технических наук, профессор, профессор института радиотехники, электроники и связи (институт 2) Санкт-Петербургского государственного университета аэрокосмического приборостроения, профессор кафедры Военной академии связи имени Маршала Советского Союза С.М. Буденного
https://orcid.org/0000-0002-4889-0001

Дворников С.В. 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 авторы не заявляли.

Dvornikov S.V. has been a member of the journal "Proceedings of Telecommunication Universities" Editorial Council 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 authors have not declared any other conflicts of interest.

Научная статья
УДК 621.391.8
https://doi.org/10.31854/1813-324X-2025-11-3-47-58
EDN:OJBGGT

Распределение комплексной огибающей сигналов, принятых из канала в условиях «сложной» сигнально-помеховой обстановки

Михаил Леонидович Маслаков, maslakov.ml@yandex.ru

ООО «Специальный Технологический Центр»,
Санкт-Петербург, 195220, Российская Федерация
Санкт-Петербургский государственный университет аэрокосмического приборостроения,
Санкт-Петербург, 190000, Российская Федерация

Аннотация

Аннотация. *При статистическом анализе комплексных огибающих модулированных сигналов, принимаемых из канала связи, в качестве модели плотности распределения вероятностей общепринято полагают нормальную плотность распределения. Однако в канале с глубокими замираниями, а также при наличии помех, т. е. в случае «сложной» сигнально-помеховой обстановки, интерес могут представлять модели распределений, обладающие более тяжелыми хвостами. В качестве таковых в работе рассматриваются логистическое распределение и распределение гиперболического секанса. В работе приведены выражения для соответствующих двумерных плотностей распределения вероятностей.*

Цель работы: *показать, что при определенных условиях в реальном канале связи могут наблюдаться модели распределения комплексной огибающей, отличные от нормального. Учет данного обстоятельства может позволить улучшить характеристики системы связи в задачах адаптации и оценки надежности решений демодулятора.*

Методы исследования: *для проверки принадлежности комплексной огибающей соответствующему закону распределения применяется критерий Хи-квадрат. В статье предложена реализация критерия Хи-квадрат для случая двумерной плотности распределения.*

В качестве ***результатов*** *в работе представлен анализ статистической обработки сигналов, принятых из реального канала связи в различных условиях.*

Новизна *состоит в экспериментальном исследовании факта, что в реальных каналах в случае глубоких замираний и сложной сигнально-помеховой обстановки более предпочтительными могут оказаться логистическое распределение или распределение гиперболического секанса.*

Практическая значимость *заключается в том, что учет модели распределения позволяет получить более адекватную оценку среднего квадратичного отклонения шумовой составляющей и отношения сигнал / шум, что имеет существенное значение для функционирования адаптивных систем радиосвязи, а также в задаче оценки мягких решений демодуляции.*

Ключевые слова: *комплексная огибающая, двумерное нормальное распределение, двумерное логистическое распределение, двумерное распределение гиперболического секанса, критерий Хи-квадрат, отношение сигнал / шум*

Ссылка для цитирования: Маслаков М.Л. Распределение комплексной огибающей сигналов, принятых из канала в условиях «сложной» сигнально-помеховой обстановки // Труды учебных заведений связи. 2025. Т. 11. № 3. С. 47–58. DOI:10.31854/1813-324X-2025-11-3-47-58. EDN:OJBGGT

Original research
https://doi.org/10.31854/1813-324X-2025-11-3-47-58
EDN:OJBGGT

Distribution of the Complex Envelope for Signals Received from a Channel with a "Complex" Signal-Noise Environment

Mikhail L. Maslakov, maslakov.ml@yandex.ru

LLC Special Technology Center,
St. Petersburg, 195220, Russian Federation
Saint-Petersburg State University of Aerospace Instrumentation,
St. Petersburg, 190000, Russian Federation

Annotation

Relevance*. In statistical analysis of complex envelopes of modulated signals received from a communication channel, the normal distribution density is generally assumed to be the probability density model. However, in a channel with deep fading and in the presence of interference, i.e. in the case of a "complex" signal-interference environment in the channel, distribution models with heavier tails may be of interest. The logistic distribution and the hyperbolic secant distribution are considered as such in the work. Expressions for the corresponding two-dimensional probability distribution densities are presented.*
The aim *of the work is to show that, under certain conditions, models of the distribution of the complex envelope that other than normal one can be observed in a real communication channel. Taking this into account may allow to improve the characteristics of the communication system in the tasks of adaptation and evaluation of the reliability of demodulator solutions.*
Research methods: *To check whether the complex envelope belongs to the corresponding distribution law, the Chi-square criterion is used. The implementation of the Chi-square criterion for the case of a two-dimensional distribution density is proposed in article.*
As results*, the paper presents the analysis of statistical processing of signals received from a real communication channel under various conditions.*
The novelty *lies in the experimental study of the fact that in real channels, in the case of deep fading and complex signal-interference conditions, the logistic distribution or the hyperbolic secant distribution may be more preferable.*
The practical significance *lies in the fact that taking into account the distribution model makes it possible to obtain a more adequate estimate of the mean square deviation of the noise component and the signal-to-noise ratio, which is essential for the functioning of adaptive radio communication systems, as well as in the task of evaluating soft demodulation solutions.*

Keywords: *complex envelope, 2-dimensional normal distribution, 2-dimensional logistic distribution, 2-dimensional hyperbolic secant distribution, chi-squared test, signal-to-noise ratio*

For citation: Maslakov M.L. Distribution of the Complex Envelope for Signals Received from a Channel with a "Complex" Signal-Noise Environment. *Proceedings of Telecommunication Universities.* 2025;11(3):47–58. (in Russ.) DOI:10.31854/1813-324X-2025-11-3-47-58. EDN:OJBGGT

1. Введение

Оценка канала является важнейшей задачей в адаптивных системах радиосвязи. При статистическом анализе принимаемых сигналов для оценки параметров каналов, характеризующих качество распространения или, другими словами, текущее состояние радиоканала – отношение сигнал / шум (ОСШ) и вероятность ошибки на бит, часто используют параметрические методы оценивания [1–4]. При этом обычно переходят к рассмотрению комплексных огибающих принимаемых модулированных сигналов [3]. Известно большое число методов,

основанных на статистическом анализе комплексных огибающих, позволяющих получить оценки ОСШ [3–5] и вероятности ошибки на бит [6].

Обозначим комплексную огибающую принимаемого сигнала в форме:

$$\hat{u}_k = \hat{A}_k = \exp(j\hat{\varphi}_k) = \hat{I}_k + j\hat{Q}_k, \quad k = 1, 2, \ldots, \qquad (1)$$

где $\hat{A}_k$ – модуль комплексной огибающей принятого символа; $\hat{\varphi}_k$ – фаза принятого символа; $\hat{I}_k$, $\hat{Q}_k$ – синфазная и квадратурная составляющие принятого символа; k – номер принятого символа.

При этом:

$$\hat{A}_k = \sqrt{\hat{I}_k^2 + j\hat{Q}_k^2} = \sqrt{\left(I_k + \xi_{I,k}\right)^2 + \left(Q_k + \xi_{Q,k}\right)^2}, \quad k = 1, 2, \ldots, \qquad (2)$$

где I_k, Q_k – истинные значения синфазной и квадратурной составляющей; $\xi_{I,k}$, $\xi_{Q,k}$ – соответствующие шумовые составляющие.

В предположении нормальности $\xi_{I,k}$, $\xi_{Q,k}$ в (2) часто переходят к рассмотрению закона Райса, Накагами или в частном случае закона Рэлея [6–8] для амплитуды – модуля комплексной огибающей, что удобно в случае, например, фазовой манипуляции (PSK, *аббр. от англ.* Phase-Shift-Keying). В свою очередь для оценки статистики фазы [9] могут быть использованы модели кругового нормального распределения или распределения Мизеса [10, 11] – что, однако, имеет место быть лишь при больших значениях ОСШ.

Рассмотрим общепринятую модель, применительно к задаче статистического анализа сигналов. Запишем выражение для двумерной нормальной случайной величины [12]:

$$W_N(x, y, \sigma_x, \sigma_y, a_x, a_y) = \\ = \frac{1}{2\pi\sigma_x\sigma_y}\exp\left(-\left(\frac{(x-a_x)^2}{2{\sigma_x}^2} + \frac{(y-a_y)^2}{2{\sigma_y}^2}\right)\right), \qquad (3)$$

где σ_x, σ_y – средне-квадратичные отклонения (СКО) случайных величин x и y; a_x, a_y – математические ожидания случайных величин x и y, соответственно.

Приняв случайные величины x и y синфазной и квадратурной составляющими $\hat{I}$ и $\hat{Q}$, с равными дисперсиями и, следовательно, с равными СКО, т. е.:

$$\sigma_x = \sigma_y = \sigma, \qquad (4)$$

а также приняв математические ожидания a_x, a_y точками сигнального созвездия, запишем выражение для описания комплексной огибающей принятого сигнала в виде двумерной плотности распределения, где:

$$W_N(\hat{I}, \hat{Q}, \sigma, I_m, Q_m) = W_N(\hat{I}, \hat{Q}, \sigma_x = \sigma, \sigma_y = \sigma, I_m, Q_m);$$

I_m, Q_m – точки сигнального созвездия, соответствующие m-му символу; M – число точек сигнального созвездия или порядок модуляции:

$$W_{N,M}(\hat{u}, \sigma) = W_{N,M}(\hat{I}, \hat{Q}, \sigma) = \\ = \frac{1}{M}\sum_{m=0}^{M-1} W_N(\hat{u}, \sigma, I_m, Q_m) = \\ = \frac{1}{M}\sum_{m=0}^{M-1} W_N(\hat{I}, \hat{Q}, \sigma, I_m, Q_m). \qquad (5)$$

Приведенная модель используется в известных моделях и оценщиках ОСШ [5, 13–15] и, как будет показано в работе, является подходящей для большого числа реальных случаев. Однако в случае глубоких замираний в канале связи, а также при наличии помех, или, другими словами, в случае «сложной» сигнально-помеховой обстановки в канале, более адекватным может быть применение других моделей плотностей распределения вероятностей [16], в частности обладающих более тяжелыми хвостами. Также отметим работы [17–20], в которых рассматривается проблема получения оценки ОСШ в канале со сложной сигнально-помеховой обстановкой, а для решения задачи предлагаются достаточно сложные в вычислительном плане подходы, основанные на итеративных процедурах или получении прогнозов с использованием методов машинного обучения.

В работе приведены результаты статистического анализа распределения огибающей, полученные при анализе сигналов, принятых из реального канала связи в условиях глубоких замираний и сложной помеховой обстановки. Цель работы – показать, что в подобных условиях в канале могут наблюдаться модели распределения комплексной огибающей отличные от нормального распределения.

2. Альтернативные модели распределений

В данном разделе кратко рассмотрим модели распределений, принадлежность к которой будет проверяться для имеющейся выборки.

Двумерное нормальное распределение

Нормальное или гауссовское распределение общепринято применяется в качестве модели шумовой составляющей. На основе данной модели получены аналитические выражения для вероятностей ошибки на бит для различных видов модуляции [8].

Выражение для двумерной нормальное плотности для общего случая (3) применительно к рассматриваемой задаче, а также с учетом (1), запишем в следующем виде:

$$W_N(\hat{u}, \sigma, I_m, Q_m) = \\ = \frac{1}{2\pi\sigma^2}\exp\left(-\frac{(\hat{I}-I_m)^2 + (\hat{Q}-Q_m)^2}{2\sigma^2}\right). \qquad (6)$$

В силу того, что значения I_m, Q_m – это точки сигнального созвездия и, соответственно, являются известными, то все плотности вида (6), входящие в (5), могут быть центрированы. Кроме того, как будет показано в разделе 2, при вычислении статистики Хи-квадрат будет осуществлен переход к одномерному случаю, поэтому функцию распределения, называемую также кумулятивной функцией распределения (CDF, *аббр. от англ.* Cumulative Distribution Function), здесь и далее будем записывать для одномерного случая.

Функция распределения для одномерного нормального распределения в случае нулевого математического ожидания определяется выражением:

$$CDF_N(x) = \frac{1}{2}\left(1 + \mathrm{erf}\left(\frac{x}{\sqrt{2}\sigma}\right)\right), \qquad (7)$$

где erf(x) – функция ошибок или интеграл вероятности.

Двумерное логистическое распределение

Логистическое распределение часто рассматривают в качестве альтернативного нормальному распределению при статистическом анализе случайных данных [21]. Отличительной чертой логистического распределения является более тяжелые хвосты функции плотности распределения вероятностей, а также несколько больший коэффициент эксцесса.

Плотность распределения вероятностей одномерного логистического распределения определяется выражением [22]:

$$W_L(x, \sigma, \mu) = \frac{\pi}{4\sqrt{3}\sigma}\mathrm{sech}^2\left(\frac{\pi}{2\sqrt{3}}\frac{(x-\mu)^2}{\sigma}\right), \qquad (8)$$

где μ – математическое ожидание; σ – СКО случайной величины x.

Выбранная в (8) параметризация позволяет приравнять дисперсию для нормального и логистического распределений значению σ^2.

Как известно [23], плотность распределения вероятностей многомерной случайной величины равна произведению одномерных плотностей распределения вероятностей. Таким образом, необходимо перемножить две плотности (8), подставив в них вместо (x, μ), соответственно $(\hat{I}, I_m)$ и $(\hat{Q}, Q_m)$.

В результате выражение для плотности двумерного логистического распределения с учетом принятых обозначений имеет вид:

$$W_L(\hat{u}, \sigma, I_m, Q_m) = \\ = \frac{\pi^2}{48\sigma^2}\mathrm{sech}^2\left(\frac{\pi}{2\sqrt{3}}\frac{(\hat{I}-I_m)^2}{\sigma}\right)\mathrm{sech}^2\left(\frac{\pi}{2\sqrt{3}}\frac{(\hat{Q}-Q_m)^2}{\sigma}\right). \qquad (9)$$

При этом, как и ранее, полагаем равенство значений σ для синфазной и квадратурной составляющих, а также их некоррелированность, что позволяет обойтись без введения коэффициента корреляции и матрицы ковариации в выражении (9).

Функция распределения логистического распределения при нулевом математическом ожидании определяется выражением [22]:

$$CDF_L(x) = \frac{1}{2}\left(1 + \tanh\left(\frac{\pi}{2\sqrt{3}\sigma}x\right)\right). \qquad (10)$$

Двумерное распределение гиперболического секанса

Распределение гиперболического секанса является еще одной альтернативой нормального распределения. Оно обладает рядом схожих свойств с нормальным (см. подробнее в [24]) и логистическим законами распределения [25]. Его часто используют при статистическом анализе случайных величин, принадлежащим близкому, однако отличному от нормального, закону распределения. Утяжеление хвостов отражает наличие выбросов, а применительно к рассматриваемому в статье случаю отражает наличие помех.

Плотность распределения вероятностей одномерного распределения гиперболического секанса определяется выражением [26]:

$$W_{\mathrm{H}}(x, \sigma, \mu) = \frac{1}{2\sigma}\mathrm{sech}\left(\frac{\pi}{2\sigma}(x-\mu)\right) = \\ = \frac{1}{2\sigma\cosh\left(\frac{\pi}{2\sigma}(x-\mu)\right)}, \qquad (11)$$

где μ – математическое ожидание; σ – СКО случайной величины x.

По аналогии с получением (9) выражение для двумерной плотности распределения гиперболического секанса с учетом параметризации для приравнивания σ и принятых обозначений примет вид:

$$W_{\mathrm{H}}(\hat{u}, \sigma, I_m, Q_m) = \frac{1}{4\sigma^2}\mathrm{sech}\left(\frac{\pi}{2\sigma}(\hat{I}-I_m)\right) \times \\ \times \mathrm{sech}\left(\frac{\pi}{2\sigma}(\hat{Q}-Q_m)\right) = \\ = \frac{1}{4\sigma^2\cosh\left(\frac{\pi}{2\sigma}(\hat{I}-I_m)\right)\cosh\left(\frac{\pi}{2\sigma}(\hat{Q}-Q_m)\right)}. \qquad (12)$$

Соответствующая функция распределения для закона гиперболического секанса определяется выражением:

$$CDF_{\mathrm{H}}(x) = \frac{2}{\pi}\arctan\left(\exp\left(\frac{\pi}{2\sigma}x\right)\right). \qquad (13)$$

Другие альтернативные распределения

Потенциально можно было рассмотреть и некоторые другие законы распределений, в частности распределения Коши и Лапласа [27]. Однако эти

распределения являются более «непохожими» на нормальное распределение. Так, распределение Коши обладает более тяжелыми хвостами, по сравнению с рассмотренными выше распределениями. Кроме того, для распределения Коши не так удобно сопоставить значение СКО с нормальным распределением для последующей оценки ОСШ. Распределение Лапласа обладает самым большим коэффициентом эксцесса, что характеризует большую вероятность «попадания» значений случайной величины в область, близкой к математическому ожиданию. По указанной причине это распределение не подходит для рассматриваемого в работе случая анализа сигналов, принимаемых из канала в условиях глубоких замираний и сложной помеховой обстановки.

3. Критерий согласия типа Хи-квадрат для случая двумерной плотности распределения

При статистическом анализе для проверки принадлежности имеющейся выборки (а точнее эмпирического распределения, полученного на основе этой выборки) заданному закону распределения применяют критерии согласия. Одним из наиболее употребительных критериев является критерий согласия Хи-квадрат [21, 28–30].

Отметим, что выбор используемого критерия согласия должен осуществляться в зависимости от типа анализируемых данных и вида предполагаемого распределения. Критерий Хи-квадрат представляется подходящим для исследования принадлежности выборки к нормальному или близкому к нормальному конкурирующему распределению – см., например, [21, 28]. Отличительной чертой рассматриваемой задачи является необходимость исследования выборок, состоящих из комплексных чисел, что приводит к использованию двумерных распределений. Вопросы применения и реализации критериев согласия, в том числе критерия Хи-квадрат, для случая двумерных случайных величин практически не освещены как в отечественных, так и зарубежных источниках. Можно отметить работы [31–32], носящие больше теоретический характер. В данном разделе приведем вариант реализации критерия согласия Хи-квадрат в случае его применения для двумерных плотностей распределения.

Как говорилось выше, считаем, что значения σ для реальной и мнимой составляющих равны (4). Кроме того, для удобства описания реализации применительно к двумерной случайной величине математическое ожидание положим равным 0. Как известно [33], в случае одномерных случайных величин осуществляют разбиение на r столбцов (бинов), подсчитывая частоты попадания элементов выборки в соответствующий столбец. Фактически получают гистограммную оценку плотности распределения.

Статистику критерия Хи-квадрат вычисляют из выражения:

$$\chi^2 = \sum_{k=1}^{r} \frac{N(\hat{p}_k - p_k)^2}{p_k} = \sum_{k=1}^{r} \frac{(\hat{n}_k - Np_k)^2}{Np_k}, \qquad (14)$$

где N – объем выборки; $\hat{p}_k$ – измеренные частоты (оценки вероятностей) попадания в k-й столбец; p_k – ожидаемые значения вероятностей; $\hat{n}_k$ – количество попаданий в k-й столбец.

При гистограммной оценке двумерной плотности столбцы обычно ограничивают квадратными областями. Однако при таком разбиении несколько проблематично получить значения p_k, которые должны быть получены на основе функции распределения. Поэтому вместо квадратного разбиения разделим комплексную область на кольца, ограниченные окружностями с радиусами $\{R_0, R_1, R_2, \ldots, R_r\}$ как показано на рисунке 1.

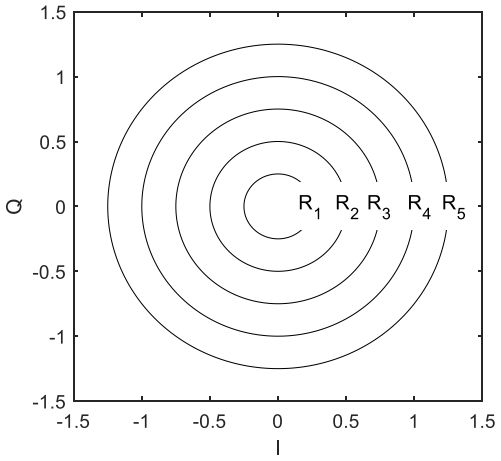


Рис. 1. Пример разбиения комплексной плоскости

Fig. 1. An Example of Splitting a Complex Plane

Для общности внутренний круг также будем называть *кольцом*, ограниченным окружностями R_1 и $R_0 = 0$.

Обозначим шаг увеличения радиусов ΔR, тогда значения радиусов определяются следующим образом:

$$R_k = R_{k-1} + \Delta R = k\Delta R. \qquad (15)$$

Площади колец A_k определяются из выражения:

$$A_k = \pi R_k^2 - \pi R_{k-1}^2 = \pi(R_k^2 - R_{k-1}^2) = \\ = \pi(R_k - R_{k-1})(R_k + R_{k-1}) = (2k-1)\pi\Delta R^2. \qquad (16)$$

Так как площади колец (бинов) различны, получаемые частости не будут соответствовать вероятностям предполагаемого распределения при «движении» по направлению от центра координат. Для решения указанной проблемы произведем нормализацию числа попаданий с учетом площади колец:

$$\hat{n}_k^n = A_1 \frac{n_k}{A_k}. \qquad (17)$$

Кроме того, для корректного вычисления частостей $\hat{p}_k$ необходимо также нормализовать объем выборки, в результате получим:

$$N^n = 2\sum_{k}^{r} \hat{n}_k^n, \qquad (18)$$

а соответствующие нормализованные частости определяются в виде:

$$\hat{p}_k^n = \frac{\hat{n}_k^n}{N^n}. \qquad (19)$$

Множитель 2 в выражении (18) возникает из-за того, что при подсчете числа попаданий элементов выборки в соответствующие кольца данные частости «сворачиваются» в бины, ограниченные интервалами $[R_0; R_1)$, $[R_1; R_2)$, $[R_2; R_3)$ и т. д. При этом границы интервалов $R_k \geq 0$, $k = 0, 1, 2, \ldots$, поэтому отрицательные значения случайных величин «попадают» в положительные интервалы. Таким образом, фактически от двумерной плотности распределения перешли («свернули») к одномерной односторонней плотности распределения.

Значения (17, 18 и 19) будем называть, соответственно, нормализованными числом попаданий в соответствующие бины, нормализованным объемом выборки и нормализованными частостями или ожидаемыми вероятностями.

В результате, вместо (14) получаем следующее выражение для значения статистики критерия Хи-квадрат:

$$\chi_n^2 = \sum_{k=1}^{r} \frac{N^n(\hat{p}_k^n - p_k)^2}{p_k} = \sum_{k=1}^{r} \frac{(\hat{n}_k^n - N^n p_k)^2}{N^n p_k}. \qquad (20)$$

В случае сложной гипотезы, а именно при неизвестном значении σ, будем рассматривать статистику вида:

$$\chi_n^2(\hat{\sigma}) = \sum_{k=1}^{r} \frac{N^n\left(\hat{p}_k^n - p_k(\hat{\sigma})\right)^2}{p_k(\hat{\sigma})} = \sum_{k=1}^{r} \frac{\left(\hat{n}_k^n - N^n p_k(\hat{\sigma})\right)^2}{N^n p_k(\hat{\sigma})} \qquad (21)$$

с r-3 степенями свободы.

При этом совместно с вычислением статистики Хи-квадрат может быть получена и оценка σ. Подробнее о вычислении статистики критерия согласия Хи-квадрат в случае сложной гипотезы см. в [21, 28].

Представленная реализация позволяет свести двумерный случай к одномерному одностороннему, что позволяет воспользоваться выражениями (7, 10 и 13) для вычисления ожидаемых вероятностей p_k для соответствующих гипотетических моделей распределений.

Далее, для получения оценки Хи-квадрат на основе отсчетов комплексной огибающей модулированного сигнала необходимо воспользоваться выражением (5), приняв математические ожидания точками сигнального созвездия и заменив нормальную плотность на альтернативные (9 и 12). Фактически данный подход аналогичен способу оценки ОСШ методом максимального правдоподобия, представленному, например, в [3, 13, 14].

4. Результаты

В данном разделе представлены результаты, полученные при статистическом анализе реальных сигналов, принятых из радиоканала. В рамках работы рассматривались однотональные сигналы системы связи КВ диапазона с модуляцией BPSK, QPSK и PSK8 при символьной скорости 2400 симв/с. Для формирования символов используется фильтр типа приподнятый косинус.

Для примера на рисунках 2–4 представлены фрагменты спектрограмм для пояснения различных условий в канале связи. Так, спектрограммы на рисунке 2 соответствуют сигналам, принятым из канала с замираниями. Несмотря на наличие замираний (более отчетливо видно на нижней спектрограмме рисунка 2), связанных с многолучевым распространением в канале, «качество» подобных записей можно считать «хорошим» – ОСШ составляет 13–20 дБ, а распределение комплексной огибающей соответствует двумерному нормальному распределению.

Основное внимание в статье уделено случаям сигналов, принятых из канала с глубокими замираниями и / или при наличии помех, что контрастно отличает их от приведенных на рисунках 3, 4 случаев. Так, сигналы с характерными спектрограммами вида, представленного на рисунке 3, соответствуют случаю канала с глубокими замираниями, что «контрастно» выделяется, сопоставляя эти спектрограммы со случаями, показанными на рисунке 2. Оценки ОСШ для таких сигналов, полученные в предположении нормальности функции плотности распределения вероятностей комплексной огибающей [3–5], составляют 3–9 дБ.

Второй рассматриваемый случай предполагает наличие помех. Характерный вид спектрограмм для таких сигналов показан на рисунке 4. Приведенные здесь спектрограммы «близки» к случаям, показанным на рисунке 2, с тем отличием, что в рассматриваемой полосе наблюдаются «сторонние» сигналы, отличные по виду (иная модуляция и ширина спектра) от полезного сигнала. В случае наличия сторонних помех значения ОСШ, также полученные оценщиком [13, 17], предполагающим нормальность распределения, составляют 3–6 дБ. Как будет показано далее, в подобных случаях такая оценка часто является заниженной.

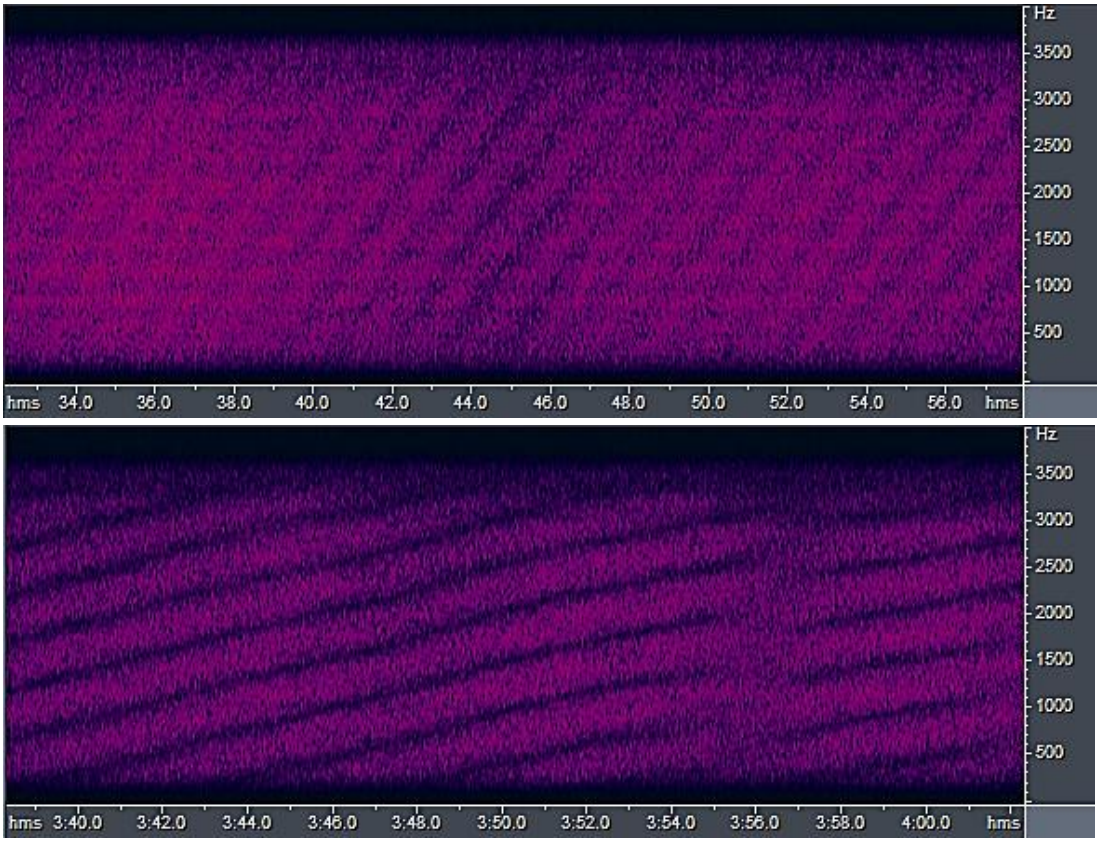


Рис. 2. Характерные спектрограммы сигналов

Fig. 2. Typical Spectrograms of Signals Received from a Fading Channel

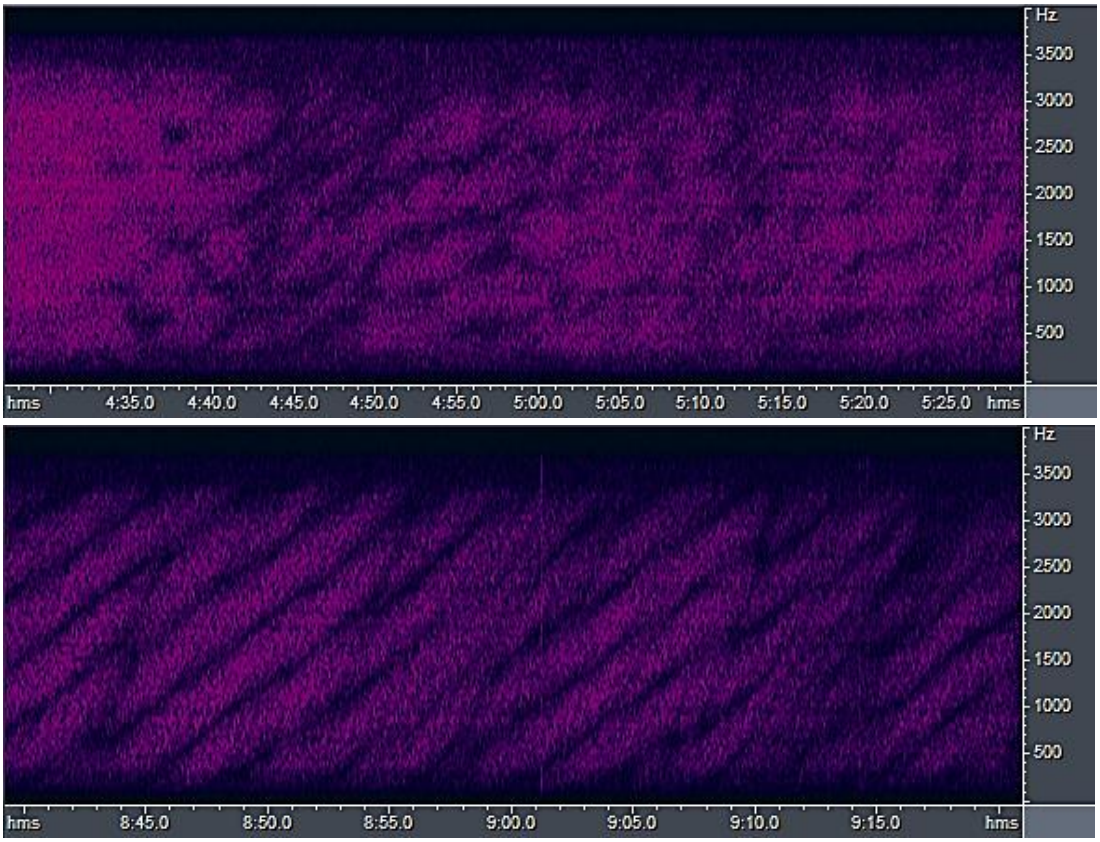


Рис. 3. Характерные спектрограммы сигналов из канала с «глубокими» замираниями

Fig. 3. Typical Spectrograms of Signals Received from a Channel with "Deep" Fading

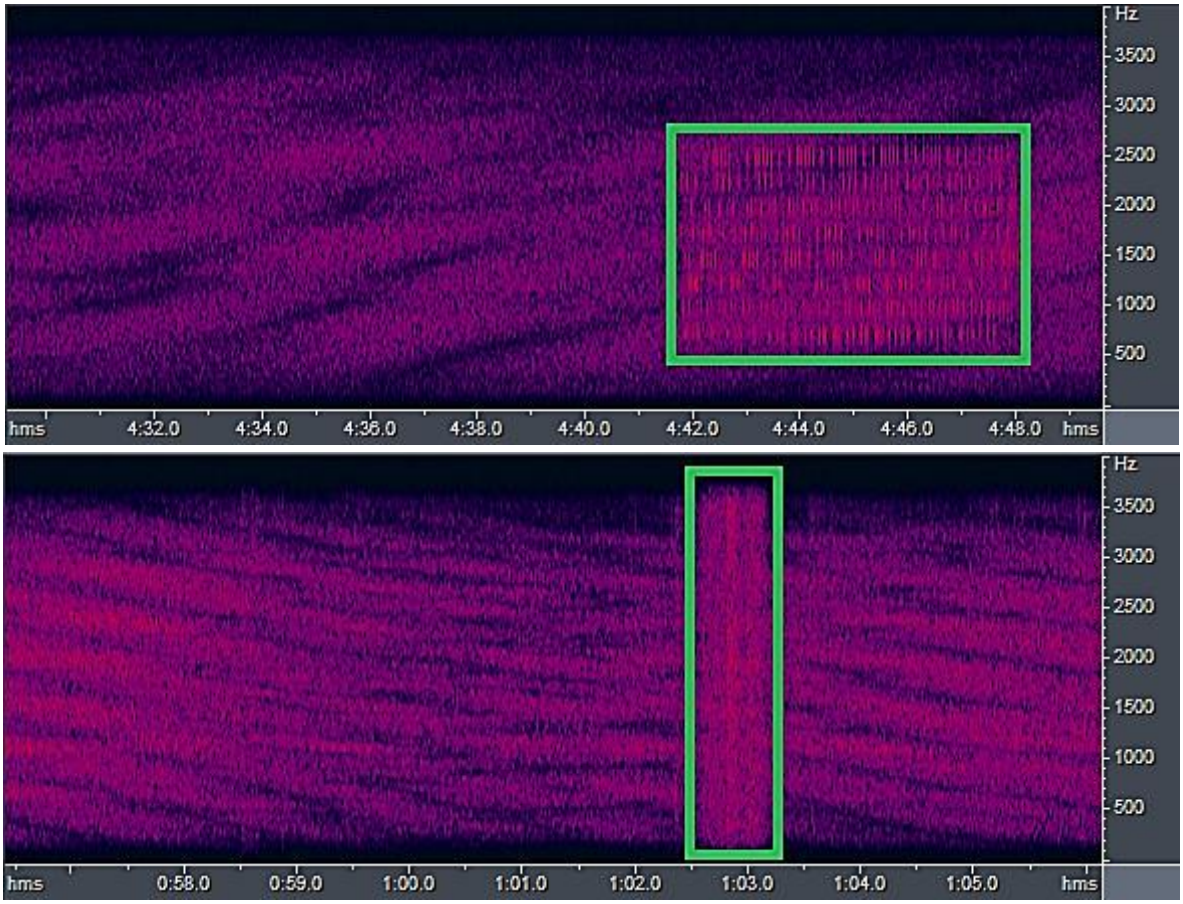


Рис. 4. Характерные спектрограммы сигналов, принятые из замирающего канала при наличии помех (выделены зеленым)

Fig. 4. Typical Spectrograms of Signals Received from a Fading Channel in the Presence of Interference (Highlighted in Green)

Очевидно, что длительность помехи составляет от нескольких сотен миллисекунд до нескольких секунд. Аналогично, в случае замираний в канале ОСШ меняется (иногда периодически) и, как следствие, наблюдаются сегменты с низким значением ОСШ.

В данной работе рассматриваются сигналы с фазовой манипуляцией (BPSK, QPSK и PSK8). В этом случае оценка ОСШ однозначно определяется на основе получаемой оценки σ следующим образом:

$$SNR = \frac{1}{2\hat{\sigma}^2}, \qquad (22)$$

где $\hat{\sigma}$ – оценка значения σ, входящего в выражение для соответствующего распределения (см. выражения (6, 9, 12)).

Оценки ОСШ и принадлежности комплексной огибающей к предполагаемым распределениям, указанным в разделе 2, будут осуществляться на длительности 500 мс, что соответствует 1200 символам. Также сделаем важное замечание: все представленные здесь оценки осуществляются на основе символов, получаемых на выходе адаптивного эквалайзера.

Далее приведем частные выборочные результаты статистического анализа принятых сигналов. При отсутствии помех в условиях неглубоких замираниях для подавляющего количества случаев распределение комплексной огибающей соответствует нормальной плотности распределения. В таблице 1 приведены частные выборочные результаты, показывающие в процентном соотношении количество случаев, когда распределение комплексной огибающей соответствует определенной модельной плотности распределения. Полученные частные выборочные оценки ОСШ здесь и далее определяются с учетом значения σ, оценку которой берем для распределения соответствующего принятой гипотезе.

ТАБЛИЦА 1. Частота соответствия распределения комплексной огибающей принятого сигнала модельной плотности распределения

TABLE 1. The Matching Frequency of the Complex Envelope Distribution of the Received Signal to the Model Distribution Density

ОСШ в канале, дБ	Модель распределения		
	Нормальное	Логистическое	Гиперболического секанса
более 15	100	0	0
12–15	98	2	0
9–12	90	10	0

Структурировать подобным образом результаты для записей с характерными глубокими замираниями и / или при наличии помех весьма затруднительно, так как ОСШ в пределах одной записи относительно небольшой длительности (порядка нескольких десятков секунд) часто изменяется в широких пределах. Поэтому далее представим характерные примеры зависимостей статистики Хи-квадрат, полученные при обработке принятых сигналов в различных условиях. На рисунках 5a и 5b приведены примеры зависимостей статистики Хи-квадрат для двух образцов сигналов, принятых из канала в условиях глубоких замираний. Здесь же представлены оценки ОСШ, полученные в предположении нормального распределения комплексной огибающей и для случая преобладающей в данный момент модели распределения в соответствии с текущим значением Хи-квадрат. Как можно заметить, в случае соответствия выборки отсчетов комплексной огибающей распределению, отличному от нормального оценки, ОСШ получаются несколько заниженными. Аналогичные результаты (рисунки 5a и 5b) можно наблюдать и для случая наличия помехи в канале связи.

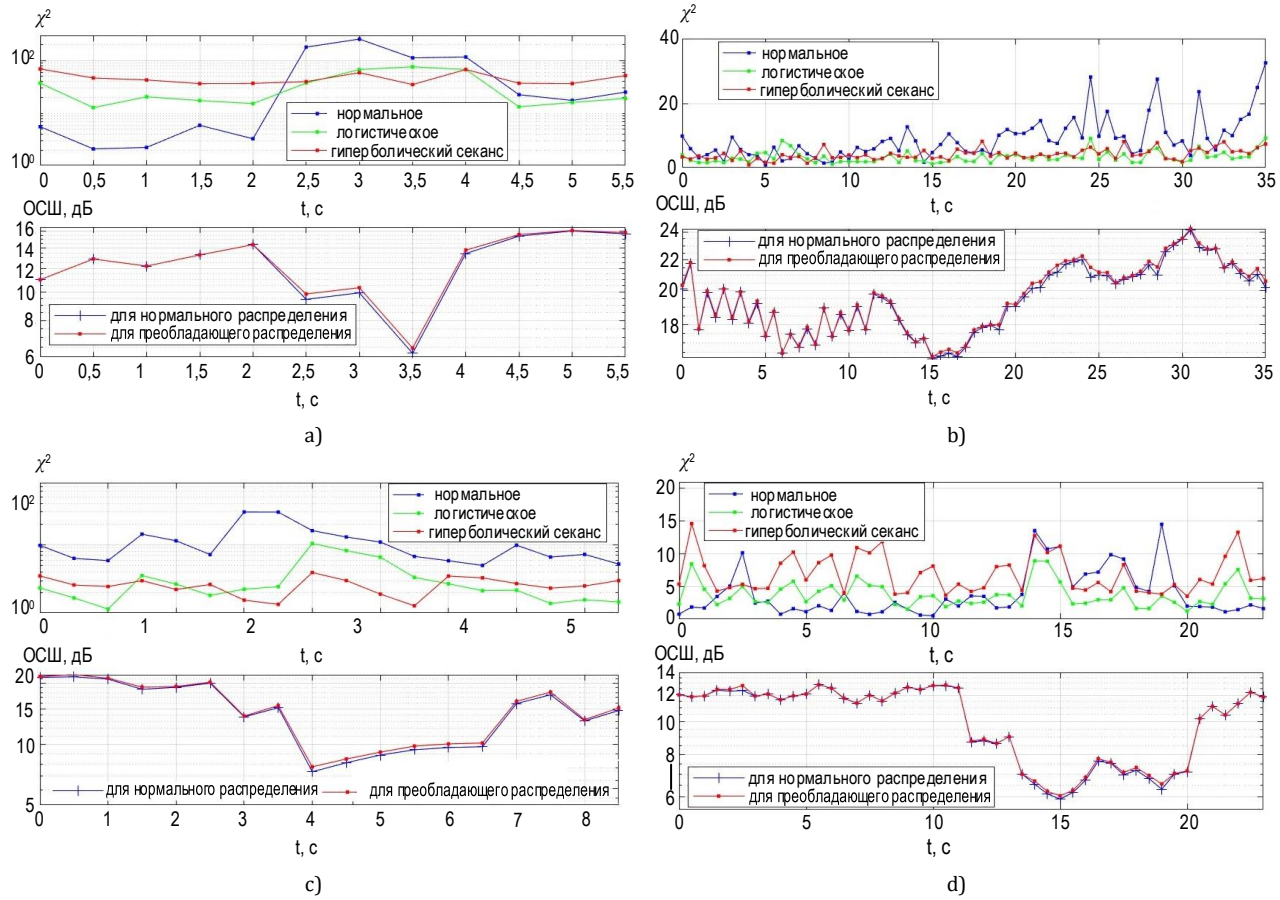


Рис. 5. Примеры зависимостей статистики Хи-квадрат на длительности сигнала для гипотез различных распределений и соответствующие оценки ОСШ в условиях глубоких замираний (a, b) и помехи в канале (c, d)

Fig. 5. Examples of Chi-Square Statistics Dependencies on Signal Duration for Hypotheses of Various Distributions and SNR Estimations in Case Fading (a, b) and Channel Interference (c, d)

Соответствие модели распределения отличному от нормального является полезным критерием при оценке текущего состояния канала. Несмотря на незначительное отличие оценок ОСШ (до 0,5 дБ), полученные результаты могут быть полезны для функционирования адаптивных систем радиосвязи при выборе оптимального режима работы, в частности, оптимальной сигнально-кодовой конструкции. Так, продолжительность помехи часто значительно меньше длительности передаваемого пакета, а значит изменение текущего режима может не соответствовать реальной обстановке в канале. Необходимо отметить, что заниженная оценка ОСШ приведет к использованию сигнально-кодовой конструкции, соответствующей более низким информационным скоростям. Напротив, при вычислении логарифма отношения правдоподобия (см. подробнее в [34]) завышенные значения СКО приведут к заниженным оценкам надежности демодулированных бит в задаче получения мягких решений демодуляции, что может негативно сказаться при декодировании.

Также важно отметить, что для значительного числа анализируемых сигналов распределение комплексной огибающей соответствует нормальному распределению. Даже для каналов с существенно глубокими замираниями и / или при наличии помех число случаев соответствия распределения комплексной огибающей нормальному закону составляло около 80 %. Тем не менее, достаточно частой альтернативой является логистическое распределение (порядка 14 %), а в случае наличия помех в канале – распределение гиперболического косинуса.

Заключение

В работе представлены результаты статистического анализа комплексных огибающих сигналов, принятых из канала связи в условиях замираний и / или при наличии помех – иначе говоря, в условиях сложной сигнально-помеховой обстановки. Для демонстрации результатов статистической обработки в работе представлен алгоритм оценки статистики критерия Хи-квадрат для случая двумерных плотностей распределения вероятностей комплексных случайных величин – синфазной и квадратурной составляющих.

Показано, что в условиях сложной сигнально-помеховой обстановки в канале связи достаточно часто наблюдаются случаи плотности распределения комплексной огибающей, отличной от нормального закона. В качестве альтернативных распределений могут быть использованы логистическое распределение и распределение гиперболического секанса. Указанные модели распределений отличны от нормального несколько более тяжелыми хвостами. Как следствие, оценки ОСШ (в предположении нормальности распределения) будут несколько занижены, напротив оценки значения σ будут немного завышены. При этом стоит отметить, что, несмотря на незначительное расхождение этих оценок, это может быть немаловажным в отдельных случаях, например, при выборе оптимального режима функционирования адаптивной системы радиосвязи в задаче выбора сигнально-кодовой конструкции. Также это имеет важное значение при оценках надежности мягких решений демодулятора при вычислении логарифма отношения правдоподобия.

При этом отметим, что целью данной работы не являлось опровергнуть общепринятую модель о нормальности шумовой составляющей и распределении комплексной огибающей сигнала и, как следствие, теоретическим основам оптимального приема и помехоустойчивости. Напротив, для подавляющего количества случаев это является наиболее верной моделью. Тем не менее, в некоторых случаях наблюдается отличие от модели нормального распределения и учет данного обстоятельства может позволить улучшить характеристики системы связи.

Список источников

1. Levy B.C. Principles of Signal Detection and Parameter Estimation. New York: Springer, 2008. DOI:10.1007/978-0-387-76544-0

2. Barkat M. Signal Detection and Estimation. Boston: Artech, 2005.

3. Серкин Ф.Б., Важенин Н.А., Вейцель В.В. Сравнительный анализ алгоритмов оценки отношения сигнал-шум на основе квадратурных компонент принимаемого сигнала // Труды МАИ. 2015. № 83. С. 19. EDN:UNWXRT

4. Beaulieu N.C., Toms A.S., Pauluzzi D.R. Comparison of four SNR estimators for QPSK modulations // IEEE Communications Letters. 2000. Vol. 4. Iss. 2. PP. 43–45. DOI:10.1109/4234.824751

5. Pauluzzi D.R., Beaulieu N. A comparison of SNR estimation techniques in the AWGN channel // Proceedings of the Pacific Rim Conference on Communications, Computers, and Signal Processing (Victoria, Canada, 17–19 May 1995). IEEE, 1995. DOI:10.1109/PACRIM.1995.519404

6. Cavers J.K. Mobile Channel Characteristics. New York: Kluwer, 2002.

7. Тихонов В.И. Статистическая радиотехника. М.: Советское радио, 1966.

8. Simon M.K., Alouini M.S. Digital Communication over Fading Channels: A Unified Approach to Performance Analysis. New York: John Wiley & Sons, 2000.

9. Патюков В.Г., Патюков Е.В., Силантьев А.А. Оценка отношения сигнал/шум на основе фазовых флуктуаций сигнала // Журнал радиоэлектроники. 2013. № 4. С. 1. EDN:PZZBWL

10. Jammalamadaka S.R., Sengupta A. Topics in Circular Statistics. Singapore: World Scientific, 2001.

11. Mardia K.V., Jupp P.E. Directional Statistics. John Wiley & Sons, Inc, 2000.

12. Tong Y.L. The Multivariate Normal Distribution. New-York: Springer-Verlag, 1990.

13. Thomas C.M. Maximum Likelihood Estimation of Signal-to-Noise Ratio. Ph.D. Thesis. Los Angeles: University of Southern California, 1967.

14. Bellili F., Meftehi R., Affes S., Stephenne A. Maximum likelihood SNR estimation over time-varying flat-fading SIMO channels // Proceedings of the International Conference on Acoustics, Speech and Signal Processing (ICASSP, Florence, Italy, 04-09 May 2014). IEEE, 2014. PP. 6523–6527. DOI:10.1109/ICASSP.2014.6854861

15. Treviño J.C., Benammar M., Roque D. A Hybrid Envelope-IQ Moment-Based Non-Data-Aided SNR Estimator for QPSK // IEEE Communications Letters. 2024. Vol. 28. Iss. 6. PP. 1382–386. DOI:10.1109/LCOMM.2024.3386188

16. Силантьев А.А., Шатров В.А., Патюков В.Г., Рябушкин С.А. Метод оценки отношения сигнал/шум на основе статистических характеристик выбросов случайных процессов применительно к командно-измерительной системе спутниковой связи // Исследования Наукограда. 2014. № 4(10). С. 4–8. EDN:TBSMSV

17. Агеев Ф.И., Вознюк В.В., Куценко Е.В. Методика расчета вероятности ошибки оптимального посимвольного когерентного приема MPSK сигналов при наличии в канале радиосвязи узкополосной шумовой помехи // Труды МАИ. 2024. № 139. С. 15. EDN:QBDQJZ

18. Bakkali M., Stephenne A., Affes S. Iterative SNR Estimation for MPSK Modulation Over AWGN Channels // Proceedings of the Vehicular Technology Conference (Montreal, Canada, 25–28 September 2006). IEEE, 2006. DOI:10.1109/VTCF.2006.350

19. Jiang L., Zheng G., Zhang B. A Noise Estimation Method Based on Envelope Pseudo-measurement System in Adaptive Kalman Filter // Proceedings of the 43rd Chinese Control Conference (CCC, Kunming, China, 28–31 July 2024). IEEE, 2024. PP. 208–213. DOI:10.23919/CCC63176.2024.10661809

20. Türkben Ö.Ü.A.K., Al-Akraa V. S.A. SNR Estimation in Communication Systems Using Cognitive Radio // Proceedings of the 5th International Conference on Engineering Technology and its Applications (IICETA, Al-Najaf, Iraq, 31 May – 01 June 2022). IEEE, 2022. PP. 477–481. DOI:10.1109/IICETA54559.2022.9888467

21. Лемешко Б.Ю., Лемешко С.Б., Постовалов С.Н., Чимитова Е.В. Статистический анализ данных, моделирование и исследование вероятностных закономерностей. Компьютерный подход. Новосибирск: Изд-во НГТУ, 2011. EDN:TZNHMX

22. Balakrishnan N. Handbook of the Logistic Distribution. Boca Raton: CRC Press, 1991. 624 p. DOI:10.1201/9781482277098

23. Giri N.C. Multivariate Statistical Analysis. Boca Raton: Marcel Dekker, 2003. 550 p. DOI:10.1201/9781482276374

24. Fischer M.J. Generalized Hyperbolic Secant Distributions. New York: Springer, 2014. DOI:10.1007/978-3-642-45138-6

25. Капля Е.В. Обобщение закона гиперболического секанса и логистического закона распределения в единый закон распределения с варьируемым коэффициентом эксцесса // Дальневосточный математический журнал. 2020. Т. 20. № 1. С. 74–81. DOI:10.47910/FEMJ202008. EDN:NLRAHN

26. Ding P. Three Occurrences of the Hyperbolic-Secant Distribution // The American Statistician. 2014. Vol. 68. Iss. 1. PP. 32–35. DOI:10.1080/00031305.2013.867902

27. Forbes C., Evans M., Hastings N., Peacock B. Statistical Distributions. New Jersey: John Wiley & Sons, 2011. 230 p.

28. Greenwood P.E., Nikulin M.S. A Guide to Chi-Squared testing. New York: John Wiley & Sons, 1996. 304 p.

29. Никулин М.С. О критерии согласия Хи-квадрат для непрерывных распределений с параметрами сдвига и масштаба // Теория вероятностей и ее применение. 1973. Т. 18. № 3. С. 583–591.

30. Watson G.S. On Chi-Square Goodness-of-Fit Tests for Continuous Distributions // Journal of the Royal Statistical Society: Series B. 1958. Vol. 20. Iss. 1. PP. 44–61. DOI:10.1111/j.2517-6161.1958.tb00274.x

31. Мирвалиев М. Критерии согласия Хи-квадрат для одного семейства многомерных дискретных распределений // Теория вероятностей и ее применение. 1989. Т. 34. № 4. С. 794–799.

32. Воинов В.Г., Никулин М.С. Критерий согласия Хи-квадрат для одномерных и многомерных дискретных распределений // Записки научных семинаров ЛОМИ. 1990. Т. 184. С. 62–79.

33. Лемешко Б.Ю., Чимитова Е.В. О выборе числа интервалов в критериях согласия типа С2 // Заводская лаборатория. Диагностика материалов. 2003. Т. 69. № 1. С. 61–67. EDN:SDJQIF

34. Hasan A.A., Marsland I.D. Low Complexity LLR Metrics for Polar Coded QAM // Proceedings of the 30th Canadian Conference on Electrical and Computer Engineering (CCECE, Windsor, Canada, 30 April – 03 May 2017). IEEE, 2017. DOI:10.1109/CCECE.2017.7946778

References

1. Levy B.C. *Principles of Signal Detection and Parameter Estimation*. New York: Springer; 2008. DOI:10.1007/978-0-387-76544-0

2. Barkat M. *Signal Detection and Estimation*. Boston: Artech; 2005.

3. Serkin F.B., Vazhenin N.A., Veytsel V.V. Analysis of signal-to-noise ratio estimation algorithms based on inphase and quadrature components of the received signal. *Trudy MAI*. 2015;83:19. (in Russ.) EDN:UNWXRT

4. Beaulieu N.C., Toms A.S., Pauluzzi D.R. Comparison of four SNR estimators for QPSK modulations. *IEEE Communications Letters.* 2000;4(2):43–45. DOI:10.1109/4234.824751

5. Pauluzzi D.R., Beaulieu N. A comparison of SNR estimation techniques in the AWGN channel. *Proceedings of the Pacific Rim Conference on Communications, Computers, and Signal Processing, 17–19 May 1995, Victoria, Canada*. IEEE; 1995. DOI:10.1109/PACRIM.1995.519404

6. Cavers J.K. *Mobile Channel Characteristics*. New York: Kluwer; 2002.

7. Tikhonov V.I. *Statisticheskaya radiotekhnika*. Moscow: Sovetskoe radio Publ.; 1966. (in Russ.)

8. Simon M.K., Alouini M.S. Digital Communication over Fading Channels: A Unified Approach to Performance Analysis. New York: John Wiley & Sons; 2000.

9. Patyukov V.G., Patyukov E.V., Silantiev A.A. Measurement of the attitude a signal/noise on the basis of phase fluctuations of a signal. *Journal of Radio Electronics*. 2013;4:1. (in Russ.) EDN:PZZBWL

10. Jammalamadaka S.R., Sengupta A. *Topics in Circular Statistics*. Singapore: World Scientific; 2001.

11. Mardia K.V., Jupp P.E. *Directional Statistics*. John Wiley & Sons, Inc; 2000.

12. Tong Y.L. *The Multivariate Normal Distribution*. New-York: Springer-Verlag; 1990.

13. Thomas C.M. *Maximum Likelihood Estimation of Signal-to-Noise Ratio*. Ph.D. Thesis. Los Angeles: University of Southern California; 1967.

14. Bellili F., Meftehi R., Affes S., Stephenne A. Maximum likelihood SNR estimation over time-varying flat-fading SIMO channels. *Proceedings of the International Conference on Acoustics, Speech and Signal Processing, ICASSP, 04–09 May 2014, Florence, Italy*. IEEE; 2014. p.6523–6527. DOI:10.1109/ICASSP.2014.6854861

15. Treviño J.C., Benammar M., Roque D. A Hybrid Envelope-IQ Moment-Based Non-Data-Aided SNR Estimator for QPSK. *IEEE Communications Letters*. 2024;28(6):1382–1386. DOI:10.1109/LCOMM.2024.3386188

16. Silantyev A.A., Shatrov V.A., Patyukov V.G., Ryabushkin S.A. Method of estimation of the signal/noise ratio, based on the statistical characteristics of the emission of stochastic processes, as applied to the telemetry, commandand ranging system of satellite communication. *Issledovaniya Naukograda*. 2014;4(10):4–8. (in Russ.) EDN:TBSMSV

17. Ageev F.I., Voznuk V.V., Kutsenko E.V. A method for calculating the probability of a bit error of optimal character-by-character coherent reception of multiple phase-manipulated signals in the presence of narrowband noise interference in the radio communication channe. *Trudy MAI*. 2024;139:15. (in Russ.) EDN:QBDQJZ

18. Bakkali M., Stephenne A., Affes S. Iterative SNR Estimation for MPSK Modulation Over AWGN Channels. *Proceedings of the Vehicular Technology Conference, 25–28 September 2006, Montreal, Canada*. IEEE; 2006. DOI:10.1109/VTCF.2006.350

19. Jiang L., Zheng G., Zhang B. A Noise Estimation Method Based on Envelope Pseudo-measurement System in Adaptive Kalman Filter. *Proceedings of the 43rd Chinese Control Conference, CCC, 28–31 July 2024, Kunming, China*. IEEE; 2024. p.208–213. DOI:10.23919/CCC63176.2024.10661809

20. Türkben Ö.Ü.A.K., Al-Akraa V. S.A. SNR Estimation in Communication Systems Using Cognitive Radio. *Proceedings of the 5th International Conference on Engineering Technology and its Applications, IICETA, 31 May – 01 June 2022, Al-Najaf, Iraq*. IEEE; 2022. p.477–481. DOI:10.1109/IICETA54559.2022.9888467

21. Lemeshko B.Yu., Lemeshko S.B., Postovalov S.N., Chimitova E.V. *Statistical data Analysis, Simulation and Study of Probability Regularities. Computer Approach*. Novosibirsk: NSTU Publ.; 2011. (in Russ.) EDN:TZNHMX

22. Balakrishnan N. *Handbook of the Logistic Distribution*. Boca Raton: CRC Press; 1991. 624 p. DOI:10.1201/9781482277098

23. Giri N.C. *Multivariate Statistical Analysis*. Boca Raton: Marcel Dekker; 2003. 550 p. DOI:10.1201/9781482276374

24. Fischer M.J. *Generalized Hyperbolic Secant Distributions*. New York: Springer; 2014. DOI:10.1007/978-3-642-45138-6

25. Kaplya E.V. The generalization of the hyperbolic secant distribution and the logistic distribution in the single dostribution with variable kurtosis. *Far Eastern Mathematical Journal*. 2020;20(1):74–81. (in Russ.) DOI:10.47910/FEMJ202008. EDN:NLRAHN

26. Ding P. Three Occurrences of the Hyperbolic-Secant Distribution. *The American Statistician*. 2014;68(1):32–35. DOI:10.1080/00031305.2013.867902

27. Forbes C., Evans M., Hastings N., Peacock B. *Statistical Distributions*. New Jersey: John Wiley & Sons; 2011. 230 p.

28. Greenwood P.E., Nikulin M.S. *A Guide to Chi-Squared testing*. New York: John Wiley & Sons; 1996. 304 p.

29. Nikulin M.S. Chi-Square Test for Continuous Distributions with Shift and Scale Parameters *Theory of Probability and its Applications*. 1974;18(3):559–568. DOI:10.1137/1118069

30. Watson G.S. On Chi-square goodness-of-fit tests for continuous distributions. *Journal of the Royal Statistical Society: Series B*. 1958;20(1):44–61. DOI:10.1111/j.2517-6161.1958.tb00274.x

31. Mirvaliev M. Chi-Square Goodness-of-Fit Tests for a Family of Multidimensional Discrete Distributions. *Theory of Probability and its Applications*. 1989;34(4):728–732. DOI:10.1137/1134094

32. Voinov V.G., Nikulin M.S. Chi-square goodness-of-fit test for one- and multidimensional discrete distributions. *Journal of Mathematical Sciences.* 1994;68:438–450. DOI:10.1007/BF01254268

33. Lemeshko B.Yu., Chimitova E.V. On the choice of the number of intervals in Type C2 Good-Affirmation Criteria. *Zavodskaya laboratoriya. Diagnostika materialov.* 2003:69(1):61–67. (in Russ.) EDN:SDJQIF

34. Hasan A.A., Marsland I.D. Low Complexity LLR Metrics for Polar Coded QAM. *Proceedings of the 30th Canadian Conference on Electrical and Computer Engineering, CCECE, 30 April – 03 May 2017, Windsor, Canada*. IEEE; 2017. DOI:10.1109/CCECE.2017.7946778

Статья поступила в редакцию 31.03.2025; одобрена после рецензирования 13.05.2025; принята к публикации 03.06.2025.
The article was submitted 31.03.2025; approved after reviewing 13.05.2025; accepted for publication 03.06.2025.

Информация об авторе:

МАСЛАКОВ Михаил Леонидович

кандидат технических наук, старший научный сотрудник отдела РМ ВЧ ООО «Специальный технологический центр», доцент кафедры инфокоммуникационных технологий и систем связи Санкт-Петербургского государственного университета аэрокосмического приборостроения

https://orcid.org/0000-0002-8989-8122

Автор сообщает об отсутствии конфликтов интересов.
The author declares no conflicts of interests.

Научная статья
УДК 621.391.1
https://doi.org/10.31854/1813-324X-2025-11-3-59-70
EDN:XTSWWS

Исследование и разработка алгоритмов обработки сигналов в системах MIMO с применением пространственно-временных кодов

Конг Куен Фам ✉, fam.kk@sut.ru
Евгений Иванович Глушанков, glushankov.ei@sut.ru

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

Аннотация

Актуальность. *С развитием цифровых радиотехнических систем передачи информации возрастают требования к спектральной эффективности мобильных и гибридных систем и сетей радиосвязи. Для удовлетворения этих требований в современных системах радиосвязи широко применяется технология многоканальных антенных систем (MIMO, аббр. от англ. Multiple-Input Multiple-Output). Использование нескольких передающих и приемных антенн в системах MIMO предъявляет повышенные требования по производительности алгоритмов обработки сигналов. В связи с этим задача разработки быстрых и эффективных алгоритмов обработки сигналов приобретает актуальность.*

Цель *исследования заключается в анализе и оптимизации пространственно-временны́х методов кодирования, а также алгоритмов обработки сигналов в системах MIMO. Разработан алгоритм обработки сигналов, обеспечивающий необходимую спектральную эффективность, при существенно сниженной вычислительной сложности. В настоящем исследовании применяются* ***методы*** *численного моделирования в среде MATLAB для сравнения эффективности различных алгоритмов обработки сигналов в системах MIMO в канале с замираниями.*

В ходе ***решения*** *поставленных задач рассмотрены принципы построения пространственно-временны́х кодовых матриц для методов кодирования, а также проанализированы методы когерентной демодуляции сигналов, на основе чего предложен алгоритм, обладающий пониженной вычислительной сложностью. Вычисление обратной матрицы канала в алгоритмах когерентной демодуляции, особенно для матриц высокой размерности, является вычислительно затратной операцией. В связи с этим научная* ***новизна*** *работы заключается в разработке и применении нового подхода к аппроксимации обратной матрицы, основанного на совместном использовании итерационного метода Якоби и разложения в ряд Неймана.*

Практическая значимость. *Разработанный алгоритм может быть использован при построении систем MIMO с большим числом передающих и приемных антенн, а также при применении методов кодирования с неортогональной структурой для увеличения скорости кодирования. В таких системах использование методов демодуляции требует значительных вычислительных ресурсов для нахождения обратной матрицы, что ограничивает производительность в реальных условиях.*

Ключевые слова: *система MIMO, пространственно-временны́е методы кодирования, метод максимального правдоподобия, метод декоррелятора, метод минимизации среднеквадратичной ошибки*

Ссылка для цитирования: Фам К.К., Глушанков Е.И. Исследование и разработка алгоритмов обработки сигналов в системах MIMO с применением пространственно-временных кодов // Труды учебных заведений связи. 2025. Т. 11. № 3. С. 59–70. DOI:10.31854/1813-324X-2025-11-3-59-70. EDN:XTSWWS

Original research
https://doi.org/10.31854/1813-324X-2025-11-3-59-70
EDN:XTSWWS

Research and Development of Signal Processing Algorithms in MIMO Systems Using Space-Time Codes

Kong K. Fam ✉, fam.kk@sut.ru
Evgeniy I. Glushankov, glushankov.ei@sut.ru

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

Annotation

Abstract: *With the advancement of digital radio communication systems, there is a growing demand for enhanced spectral efficiency in mobile and hybrid radio systems and networks. To meet these requirements, Multiple-Input Multiple-Output (MIMO) technology is extensively employed in modern radio communication systems. The use of multiple transmitting and receiving antennas in MIMO systems imposes stringent performance requirements on signal processing algorithms. Consequently, the development of fast and efficient signal processing algorithms is a task of significant relevance.*

The aim of this study *is to analyze and optimize space-time coding techniques and signal processing algorithms for MIMO systems. The research focuses on developing an algorithm that ensures the required level of performance while significantly reducing computational complexity.*

Methods*. This study utilizes numerical simulation methods within the MATLAB environment to compare the performance of various signal processing algorithms in MIMO systems over a fading channel.*

Results. *In addressing the research objectives, the principles of constructing space-time code matrices for different coding methods were examined, and coherent signal demodulation techniques were analyzed. Based on this analysis, an algorithm with reduced computational complexity is proposed. A key element of* ***scientific novelty*** *of this work lies in the development and application of a novel approach to approximate the inverse channel matrix, which is a computationally expensive operation, particularly for high-dimensional matrices in coherent demodulation algorithms. This new approach is based on the combined use of the iterative Jacobi method and the Neumann series expansion for the approximation of the matrix inverse.*

Practical significance. *The developed algorithm can be utilized in the design of MIMO systems with a large number of transmitting and receiving antennas, as well as in the application of non-orthogonal coding schemes to increase the coding rate. In such systems, conventional demodulation methods require significant computational resources for inverting the channel matrix, which limits real-world performance. The proposed algorithm mitigates this bottleneck, enabling more practical implementations.*

Keywords: *MIMO system, space-time coding techniques, Maximum Likelihood method, Zero Forcing detector, Minimum Mean Squared Error method*

For citation: Fam K.K., Glushankov E.I. Research and Development of Signal Processing Algorithms in MIMO Systems Using Space-Time Codes. *Proceedings of Telecommunication Universities.* 2025;11(3):59–70. (in Russ.) DOI:10.31854/1813-324X-2025-11-3-59-70. EDN:XTSWWS

Введение

С развитием современных цифровых систем связи постоянно возрастают требования к повышению их энергетической и спектральной эффективности [1, 2]. В настоящее время известно множество решений данной задачи, основанных на следующих подходах: разработке адаптивных систем с обратной связью с целью оптимального выбора схем модуляции и кодирования [3, 4];

использовании ортогонального частотного мультиплексирования (OFDM, *аббр. от англ.* Orthogonal Frequency-Division Multiplexing) [5, 6]; а также применении технологий многоантенных систем связи (MIMO, *аббр. от англ.* Multiple Input, Multiple Output) [7–9].

Данная работа посвящена исследованию последней из вышеуказанных технологий – технологии MIMO, включая методы пространственно-временно́го блочного кодирования, а также описание различных подходов к обработке сигналов на приемной стороне в данной системе. Рассмотрим систему MIMO с N передающими и M приемными антеннами.

В этом случае модель принимаемого сигнала может быть представлена следующим образом:

$$y = \mathbf{H}s + \mathbf{n}, \quad (1)$$

где s – вектор переданных сигналов размерности $M \times 1$; $\mathbf{H}$ – матрица комплексных коэффициентов передачи канала MIMO размерности $M \times N$; $\mathbf{n}$ – гауссовский случайный вектор шума размерности $M \times 1$.

В системах MIMO применяются различные методы демодуляции, отличающиеся уровнем вычислительной сложности и эффективностью. Среди них можно выделить методы: максимального правдоподобия (ML, *аббр. от англ.* Maximum Likelihood); декоррелятора (ZF, *аббр. от англ.* Zero Forcing); метод минимизации среднеквадратичной ошибки (MMSE, *аббр. от англ.* Minimum Mean Squared Error).

Выражения, используемые для оценки переданных сигналов в рамках указанных методов демодуляции, описываются следующими формулами:

$$\hat{s}_{ML} = \underset{s \in \Theta^I}{\operatorname{argmin}} \|y - \mathbf{H}s\|^2,$$

$$\hat{s}_{ZF} = (\mathbf{H}'\mathbf{H})^{-1}\mathbf{H}'y, \quad (2)$$

$$\hat{s}_{MMSE} = (\mathbf{H}'\mathbf{H} + 2\sigma_n^2\mathbf{I})^{-1}\mathbf{H}'y, \quad (3)$$

где Θ^I – дискретное множество значений I-мерного вектора s комплексных информационных символов, определяемое выбранным методом модуляции; матрица $\mathbf{H'}$ – комплексно-сопряженная и транспонированная матрица $\mathbf{H}$.

Как известно, применение метода ML на практике затруднено из-за его чрезвычайно высокой вычислительной сложности, особенно при использовании модуляции высокого порядка или большом числе передающих антенн N. Из выражений (2 и 3) следует, что для реализации методов ZF и MMSE необходимо вычисление обратной матрицы, что представляет собой достаточно трудоемкую операцию с вычислительной точки зрения [10, 11].

Основная идея предложенного в данной статье решения заключается в использовании приближенных методов для вычисления обратной матрицы с целью снижения вычислительной сложности при сохранении эффективности рассматриваемых методов. Кроме того, предлагается приближенное вычисление обратной матрицы, направленное на оптимизацию как точности, так и вычислительной сложности.

Ортогональные пространственно-временны́е блочные коды OSTBC

К наиболее простым схемам кодирования относятся ортогональные пространственно-временные блочные коды (OSTBC, *аббр. от англ.* Orthogonal Space-Time Block Code), в частности схема, предложенная Аламоути для случая двух передающих антенн [12], пространственно-временна́я кодовая матрица (ПВКМ) $\mathbf{S_{N,R}}$, которая имеет следующий вид:

$$\mathbf{S_{N,R}} = \mathbf{S_{2,1}} = \begin{pmatrix} s_1 & -s_2^* \\ s_2 & s_1^* \end{pmatrix},$$

где s_i* – комплексно-сопряженное значение символа s_i.

Основной принцип работы схемы Аламоути заключается в следующем [13]: символы используемого модуляционного алфавита (s_1 и s_2) передаются одновременно с двух антенн (разнесение по пространству) в течение двух временны́х интервалов (разнесение по времени). В представленной схеме скорость пространственно-временно́го кода R, определяемая как отношение числа передаваемых модулированных информационных символов k к числу временны́х интервалов p, необходимых для их передачи, составляет $R = \frac{k}{p} = 1$. При этом достигаемая степень разнесения равна $2M$. С целью повышения степени разнесения в работах В. Тароха [13], Г. Ганесана [14] и М.К. Арти [15] были предложены методы построения пространственно-временны́х кодов, обеспечивающих степень разнесения, равную NM, однако характеризующихся пониженной скоростью кодирования $R < 1$.

Ниже представлены варианты построения ПВКМ со скоростью кодирования $R = \frac{1}{2}$ и $R = \frac{3}{4}$ для случая использования трех ($\mathbf{S}_{3,\frac{1}{2}}, \mathbf{S}_{3,\frac{3}{4}}$) и четырех передающих антенн ($\mathbf{S}_{4,\frac{1}{2}}, \mathbf{S}_{4,\frac{3}{4}}$):

$$\mathbf{S}_{3,\frac{1}{2}} = \begin{pmatrix} s_1 & -s_2 & -s_3 & -s_4 & s_1^* & -s_2^* & -s_3^* & -s_4^* \\ s_2 & s_1 & s_4 & -s_3 & s_2^* & s_1^* & s_4^* & -s_3^* \\ s_3 & -s_4 & s_1 & -s_2 & s_3^* & s_4^* & s_1^* & -s_2^* \end{pmatrix},$$

$$\mathbf{S}_{3,\frac{3}{4}} = \begin{pmatrix} s_1 & -s_2 & s_3 & 0 \\ s_2 & s_1 & 0 & s_3 \\ s_3 & 0 & -s_1 & -s_2 \end{pmatrix},$$

$$\mathbf{S}_{4,\frac{1}{2}} = \begin{pmatrix} s_1 & -s_2 & -s_3 & -s_4 & s_1^* & -s_2^* & -s_3^* & -s_4^* \\ s_2 & s_1 & s_4 & -s_3 & s_2^* & s_1^* & s_4^* & -s_3^* \\ s_3 & -s_4 & s_1 & s_2 & s_3^* & -s_4^* & s_1^* & s_2^* \\ s_4 & s_3 & -s_2 & s_1 & s_4^* & s_3^* & -s_2^* & s_2^* \end{pmatrix},$$

$$\mathbf{S}_{4,\frac{3}{4}} = \begin{pmatrix} s_1 & s_2 & s_3 & 0 \\ -s_2^* & s_1^* & 0 & s_3 \\ s_3^* & 0 & -s_1^* & s_2 \\ 0 & s_3^* & -s_2^* & -s_1 \end{pmatrix}.$$

Квазиортогональные пространственно-временны́е блочные коды

Проведенный выше анализ методов OSTBC показывает, что увеличение числа передающих антенн более двух позволяет повысить степень разнесения. Однако при этом скорость кодирования R становится меньше единицы, что приводит к снижению спектральной эффективности при передаче информации. В связи с этим далее рассматривается альтернативный подход – квазиортогональные пространственно-временны́е блочные коды (QOSTBC, *аббр. от англ.* Quasi-Orthogonal Space-Time Block Codes), обладающие рядом привлекательных свойств, присущих рассмотренным выше ортогональным кодам.

Рассмотрим пример построения ПВКМ по методу QOSTBC при использовании трех и четырех передающих антенн ($\mathbf{S}_{3,1}$ и $\mathbf{S}_{4,1}$) [16–19]:

$$\mathbf{S}_{3,1} = \begin{pmatrix} s_1 & -s_2^* & s_3 & -s_4^* \\ s_2 & s_1^* & s_4 & s_3^* \\ -s_3 & -s_4^* & s_1 & s_2^* \end{pmatrix},$$

$$\mathbf{S}_{4,1} = \begin{pmatrix} s_1 & s_2 & s_3 & s_4 \\ -s_2^* & s_1^* & -s_4^* & s_3^* \\ s_3 & s_4 & s_1 & s_2 \\ -s_4^* & s_3^* & -s_2^* & s_1^* \end{pmatrix}.$$

Нетрудно заметить, что в данном случае скорость кодирования составляет $R = 1$.

Неортогональные пространственно-временны́е блочные коды

Продолжим рассмотрение, обратив внимание на метод кодирования, обеспечивающий скорость ПВК R, превышающую единицу, а, следовательно, и более высокую спектральную эффективность системы связи. Речь идет о неортогональных пространственно-временны́х блочных кодах, которые в литературе часто обозначаются обобщенным термином STBC (*аббр. от англ.* Space-Time Block Code). В этом случае модулированные информационные символы s_i передаются одновременно через различные передающие антенны в течение нескольких временны́х интервалов, что приводит к ситуации, при которой число передаваемых модулированных символов k превышает количество временны́х интервалов p, необходимых для их передачи, то есть $R = \frac{k}{n} > 1$. Несмотря на то, что данный метод характеризуется повышенной вычислительной сложностью алгоритмов демодуляции, а также уступает по эффективности ранее рассмотренным ортогональным схемам, благодаря высокой скорости кодирования он продолжает находить применение в системах беспроводной связи, ориентированных на высокоскоростную передачу данных и повышенную спектральную эффективность.

Ниже приведены примеры построения ПВКМ по методу STBC при использовании трех и четырех передающих антенн со скоростью кодирования $R = 2$ ($\mathbf{S}_{3,2}$ и $\mathbf{S}_{4,2}$)[20, 21]:

$$\mathbf{S}_{3,2} = \begin{pmatrix} s_1 & -s_2^* & s_5 & -s_6^* \\ s_2 & s_1^* & s_6 & s_5^* \\ s_7 & -s_8^* & s_3 & s_4^* \end{pmatrix},$$

$$\mathbf{S}_{4,2} = \begin{pmatrix} s_1 & s_2 & s_3 & s_4 \\ -s_2^* & s_1^* & -s_4^* & s_3^* \\ s_5 & s_7 & s_6 & s_8 \\ -s_7^* & s_5^* & -s_8^* & s_6^* \end{pmatrix}.$$

Алгоритмы демодуляции

Из выражений (2 и 3) следует, что точность и вычислительная сложность алгоритмов демодуляции ZF и MMSE в значительной степени определяются операциями умножения матриц $\mathbf{H}'\mathbf{H}$, а также вычислением обратной матрицы к полученному произведению. К сожалению, операция инверсии матрицы в большинстве случаев является вычислительно затратной. Далее будет проведен анализ методов вычисления обратной матрицы $\mathbf{H}'\mathbf{H}$ на примере классической схемы пространственно-временно́го кодирования Аламоути для системы MIMO конфигурации 2×2. Как уже было изложено ранее, в соответствии с методом Аламоути, модулированные символы s_1 и s_2 передаются одновременно с двух передающих антенн в течение двух временны́х интервалов t_1 и t_2.

Таким образом, выражение (1), а также ПВКМ $\mathbf{S}_{2,1}$ и структура принимаемых сигналов на двух приемных антеннах могут быть представлены в следующем виде [22–24]:

$$y_1 = h_1 s_1 + h_2 s_2 + n_1, \quad (4)$$

$$y_2 = -h_1 s_2^* + h_2 s_1^* + n_2 = h_2 s_1^* - h_1 s_2^* + n_2. \quad (5)$$

Выражения (4 и 5) можно объединить:

$$\begin{bmatrix} y_1 \\ y_2^* \end{bmatrix} = \begin{bmatrix} h_1 & h_2 \\ -h_2^* & h_1^* \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} + \begin{bmatrix} n_1 \\ n_2^* \end{bmatrix}. \quad (6)$$

Из матрицы $\mathbf{H}$, полученной в выражении (6), можно получить следующий результат:

$$(\mathbf{H}'\mathbf{H})_{\mathbf{N,R}} = (\mathbf{H}'\mathbf{H})_{\mathbf{2,1}} = \begin{bmatrix} h_1^* & -h_2 \\ h_2^* & h_1 \end{bmatrix}\begin{bmatrix} h_1 & h_2 \\ -h_2^* & h_1^* \end{bmatrix} = \\ = \begin{bmatrix} |h_1|^2 + |h_2|^2 & 0 \\ 0 & |h_1|^2 + |h_2|^2 \end{bmatrix} = \\ = (|h_1|^2 + |h_2|^2)\mathbf{I}. \quad (7)$$

Аналогичным образом, для случая использования метода OSTBC с тремя и четырьмя передающими антеннами, можно получить следующий результат:

$$(\mathbf{H}'\mathbf{H})_{\mathbf{3},\frac{\mathbf{1}}{\mathbf{2}}} = \left(2\sum_{i=1}^{3}|h_i|^2\right)\mathbf{I},$$
$$(\mathbf{H}'\mathbf{H})_{\mathbf{3},\frac{\mathbf{3}}{\mathbf{4}}} = \left(\sum_{i=1}^{3}|h_i|^2\right)\mathbf{I},$$
$$(\mathbf{H}'\mathbf{H})_{\mathbf{4},\frac{\mathbf{1}}{\mathbf{2}}} = \left(2\sum_{i=1}^{4}|h_i|^2\right)\mathbf{I}, \quad (8)$$
$$(\mathbf{H}'\mathbf{H})_{\mathbf{4},\frac{\mathbf{3}}{\mathbf{4}}} = \left(\sum_{i=1}^{4}|h_i|^2\right)\mathbf{I}.$$

Как следует из уравнений (7 и 8), ключевой особенностью ортогональных пространственно-временны́х блочных кодов (OSTBC) является то, что соответствующая им матрица является диагональной $\mathbf{H}'\mathbf{H}$. Это свойство позволяет свести процедуру демодуляции по критериям ZF и MMSE к набору поэлементных скалярных делений, что значительно снижает общую вычислительную сложность. В отличие от этого, для неортогональных кодов, в частности, QOSTBC и STBC, описываемых в выражениях (9 и 10), матрица $\mathbf{H}'\mathbf{H}$ имеет недиагональную структуру. Это обусловливает необходимость выполнения полного матричного обращения, сложность которого критически зависит от числа передающих антенн и порядка модуляции [25, 26]. Таким образом, требуется разработка таких алгоритмов демодуляции, которые, с одной стороны, могли бы работать с высокоскоростными неортогональными кодами, а с другой - обладали бы значительно меньшей вычислительной сложностью по сравнению с методом прямого обращения матрицы. Решение этой задачи является ключом к практической реализации перспективных систем MIMO.

$$(\mathbf{H}'\mathbf{H})_{\mathbf{4.1}} = \begin{bmatrix} \sum_{i=1}^{4}|h_i|^2 & 0 & h_1h_3^* + h_3h_1^* + h_2h_4^* + h_4h_2^* & 0 \\ 0 & \sum_{i=1}^{4}|h_i|^2 & 0 & h_1h_3^* + h_3h_1^* + h_2h_4^* + h_4h_2^* \\ h_3h_1^* + h_1h_3^* + h_4h_2^* + h_2h_4^* & 0 & \sum_{i=1}^{4}|h_i|^2 & 0 \\ 0 & h_3h_1^* + h_1h_3^* + h_4h_2^* + h_2h_4^* & 0 & \sum_{i=1}^{4}|h_i|^2 \end{bmatrix} \quad (9)$$

$$(\mathbf{H}'\mathbf{H})_{\mathbf{4.2}} = \begin{bmatrix} |h_1|^2 & -h_1h_2^* & 0 & 0 & h_1h_3^* & 0 & -h_1h_4^* & 0 \\ -h_2h_1^* & |h_1|^2 + |h_2|^2 & 0 & 0 & 0 & 0 & h_2h_4^* + h_1h_3^* & 0 \\ 0 & 0 & |h_1|^2 & -h_1h_2^* & 0 & h_1h_3^* & 0 & -h_1h_4^* \\ 0 & 0 & -h_2h_1^* & |h_1|^2 + |h_2|^2 & 0 & -h_2h_3^* & 0 & 0 \\ h_3h_1^* & 0 & 0 & 0 & |h_3|^2 & 0 & -h_3h_4^* & 0 \\ 0 & 0 & h_3h_1^* & -h_3h_2^* & 0 & |h_3|^2 & 0 & -h_3h_4^* \\ -h_4h_1^* & h_4h_2^* + h_3h_1^* & 0 & 0 & -h_4h_3^* & 0 & |h_3|^2 + |h_4|^2 & 0 \\ 0 & 0 & -h_4h_1^* & 0 & 0 & -h_4h_3^* & 0 & |h_3|^2 + |h_4|^2 \end{bmatrix}. \quad (10)$$

Предлагаемый метод приближенного вычисления обратной матрицы

Основная идея заключается в следующем: сначала положим $\mathbf{A} = \mathbf{H}'\mathbf{H}$, затем, основываясь на идее итерационного метода Якоби [27], матрица $\mathbf{A}$ разлагается на две составляющие матрицы:

$$\mathbf{A} = \mathbf{H}'\mathbf{H} = \mathbf{D} + \mathbf{R} = \mathbf{D}(\mathbf{I} + \mathbf{D}^{-1}\mathbf{R}).$$

где $\mathbf{R} = \mathbf{A} - \mathbf{D}$ – матрица, содержащая остальные элементы матрицы $\mathbf{A}$; $\mathbf{D} = \mathrm{diag}(\mathbf{A})$ – диагональная матрица.

В этом случае вычисление $\mathbf{A}^{-1}$ сводится к вычислению $(\mathbf{I} + \mathbf{D}^{-1}\mathbf{R})^{-1}$:

$$\mathbf{A}^{-1} = \mathbf{D}^{-1}(\mathbf{I} + \mathbf{D}^{-1}\mathbf{R})^{-1}.$$

Применяя ряд Неймана $(\mathbf{I} - \mathbf{B})^{-1} = \sum_{k=0}^{\infty}(\mathbf{B})^k$ [28] для вычисления $(\mathbf{I} + \mathbf{D}^{-1}\mathbf{R})^{-1}$ при $\mathbf{B} = -\mathbf{D}^{-1}\mathbf{R}$, получаем:

$$(\mathbf{I} + \mathbf{D}^{-1}\mathbf{R})^{-1} = \\ = \sum_{k=0}^{\infty}(-\mathbf{D}^{-1}\mathbf{R})^k = \mathbf{I} - \mathbf{D}^{-1}\mathbf{R} + (\mathbf{D}^{-1}\mathbf{R})^2 - \ldots$$

При условии сходимости данного ряда (доказательство приводится ниже) матрица $\mathbf{A}^{-1}$ может быть представлена следующим образом:

$$\mathbf{A}^{-1} = \mathbf{D}^{-1}\sum_{k=0}^{\infty}(-\mathbf{D^{-1}R})^k = \mathbf{D}^{-1} - \mathbf{D^{-1}RD}^{-1} + \\ + (\mathbf{D^{-1}R})^2\mathbf{D}^{-1} - \cdots. \quad (11)$$

Чтобы доказать сходимость ряда Неймана, заданного выражением (11), необходимо показать, что существует такое натуральное число k, при котором погрешность между приближенным значением и исходным стремится к нулю. Из выражений (7 и 8) видно, что матрица $\mathbf{A} = \mathbf{H}'\mathbf{H} = \mathbf{D}$, следовательно, $\mathbf{A}^{-1} = \mathbf{D}^{-1}$, и ряд Неймана сходится уже при нулевом порядке ($k = 0$).

Докажем сходимость ряда Неймана для матрицы $(\mathbf{H}'\mathbf{H})_{\mathbf{4,1}}$, представленной в выражении (9) (доказательства для других случаев аналогичны). В этом случае ряд Неймана сходится, если выполняется следующее условие:

$$\rho(\mathbf{D^{-1}R}) = \frac{\max(|r_i|)}{|d|} = \frac{\max(|r_i|)}{\sum_i^4|h_i|^2} < 1,$$

где $\max(|r_i|)$ – это наибольшее значение элементов матрицы $\mathbf{R}$; $|d|$ – это величина элемента на главной диагонали матрицы $\mathbf{D}$.

Таким образом, чтобы доказать выполнение этого условия, необходимо доказать, что:

$$|h_1h_3^* + h_3h_1^* + h_2h_4^* + h_4h_2^*| < \\ < |h_1|^2 + |h_2|^2 + |h_3|^2 + |h_4|^2. \quad (12)$$

Предположим, что $h_i = a_i + b_ij$ и $h_j = a_j + b_jj$, тогда:

$$h_ih_j = (a_ia_j + b_ib_j) + (b_ia_j - a_ib_j)j,$$
$$\mathrm{Re}(h_ih_j^*) = a_ia_j + b_ib_j.$$

Поскольку коэффициент перехода для каждой антенны различен, применяя неравенство Коши – Буняковского, получаем:

$$\left|\mathrm{Re}(h_ih_j^*)\right| = \left|a_ia_j + b_ib_j\right| \leq \\ \leq \sqrt{a_i^2 + b_i^2}\sqrt{a_j^2 + b_j^2} = |h_i|\left|h_j\right| < \frac{|h_i|^2+|h_j|^2}{2}. \quad (13)$$

Преобразуем левую часть выражения (12) в следующий вид:

$$|h_1h_3^* + h_3h_1^* + h_2h_4^* + h_4h_2^*| = \\ = |2(\mathrm{Re}(h_1h_3^*) + \mathrm{Re}(h_2h_4^*))| = \\ = 2|\mathrm{Re}(h_1h_3^*) + \mathrm{Re}(h_2h_4^*)|. \quad (14)$$

Применив выражение (13) к выражению (14), получаем следующий результат:

$$|\mathrm{Re}(h_1h_3^*) + \mathrm{Re}(h_2h_4^*)| \leq |\mathrm{Re}(h_1h_3^*)| + \\ +|\mathrm{Re}(h_2h_4^*)| \leq |h_1||h_3| + |h_2||h_4| < \\ < \frac{|h_1|^2 + |h_2|^2 + |h_3|^2 + |h_4|^2}{2}. \quad (15)$$

Используя выражения (13 и 15), получим:

$$|h_1h_3^* + h_3h_1^* + h_2h_4^* + h_4h_2^*| < \\ < 2\frac{|h_1|^2 + |h_2|^2 + |h_3|^2 + |h_4|^2}{2} < \\ < |h_1|^2 + |h_2|^2 + |h_3|^2 + |h_4|^2.$$

Таким образом, можно утверждать, что выражение (12) верно, другими словами, $\rho(\mathbf{D^{-1}R}) < 1$, а следовательно, существует положительное число k, которое удовлетворяет условию $\mathbf{A}_k^{-1} \approx \mathbf{A}^{-1}$.

Для более наглядного сравнения между точным вычислением обратной матрицы $(\mathbf{H}'\mathbf{H})_{\mathbf{4,1}}$ и ее приближенным вычислением вышеописанным методом, подставим конкретные значения h_i, которые распределены по закону Рэлея [29] (рисунок 1), предполагая, что сигнал передается через канал с распределением Рэлея. Чтобы сравнить точность приближений, мы используем норму Фробениуса матрицы ошибки.

Для матрицы $\mathbf{E}$ норма Фробениуса $\|\mathbf{E}\|_F$ вычисляется как:

$$\|\mathbf{E}\|_F = \sqrt{\sum_{i,j}\left|e_{ij}\right|^2}.$$

где $\mathbf{E}$ – это матрица ошибки, которая равна разности между приближенной обратной матрицей и точной обратной матрицей.

Для обеспечения точности эксперимента процесс генерации значений h_i согласно распределению Рэлея, повторяется L раз (L = 1000), и при этом вычисляется матрица E. На рисунке 2 представлены средние значения элементов e_{ij} матрицы $\mathbf{E}$, а также среднее значение $\|\mathbf{E}\|_F$, которое обозначено как общая средняя ошибка после L испытаний. На рисунке 3 представлено значение $\|\mathbf{E}\|_F$ для первых ста испытаний при аппроксимации нулевого и первого порядка.

Из приведенного выше анализа следует, что предложенный метод приближенного вычисления обратной матрицы может быть применен в алгоритмах демодуляции, таких как ZF и MMSE, с целью снижения вычислительной сложности. Исходя из вопроса о том, какого порядка приближение следует выбрать в методе вычисления обратной матрицы для различных методов кодирования, следует отметить, что, как было доказано, для методов кодирования Аламоути и OSTBC приближение нулевого порядка может обеспечить достаточную точность (при высоком качестве принимаемого сигнала, то есть при высоком отношении сигнал / шум). Однако для других методов кодирования

при $R > 1$ это условие не выполняется. Предлагается идея построения алгоритма адаптивной демодуляции сигнала в системе MIMO, целью которого является обеспечение требуемой точности, а также учет вычислительной сложности. Общая структура данного алгоритма представлена на рисунке 4.

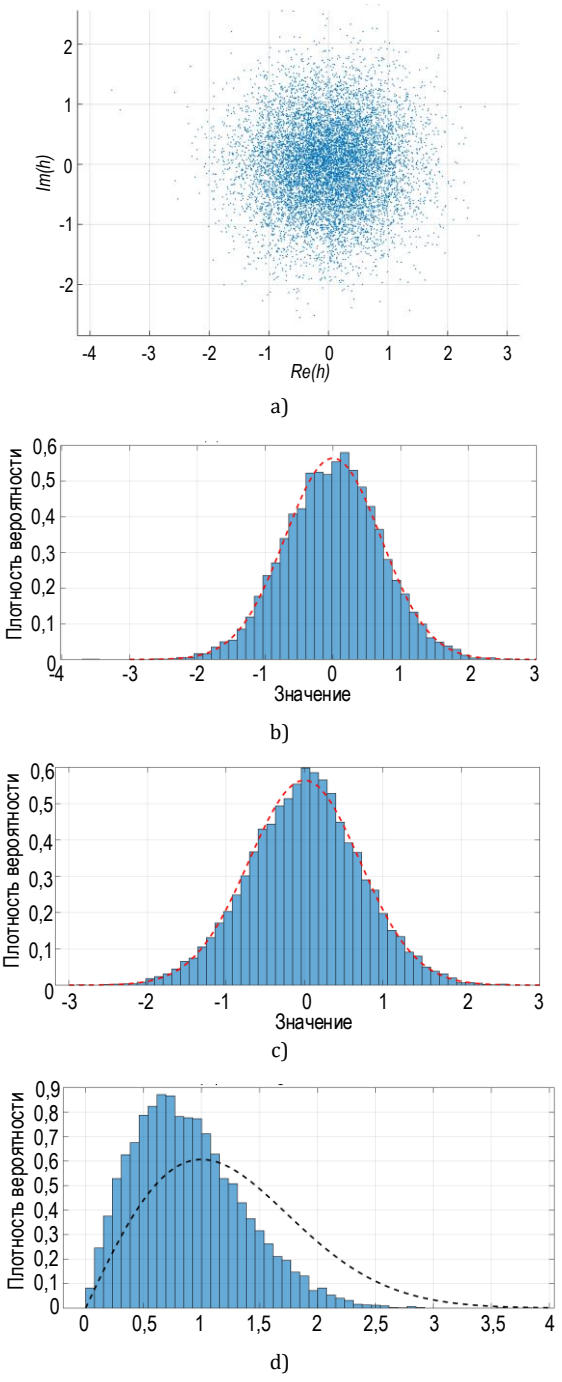


Рис. 1. Распределение значений коэффициентов передачи каналов h_i: a) комплексное распределение h_i; b) действительная часть h_i; c) мнимая часть h_i; d) распределение Рэлея

Fig. 1. Distribution of Channel Transfer Coefficient Values h_i: a) Complex Distribution; b) Real Part; c) Imaginary Part; d) Rayleigh Distribution

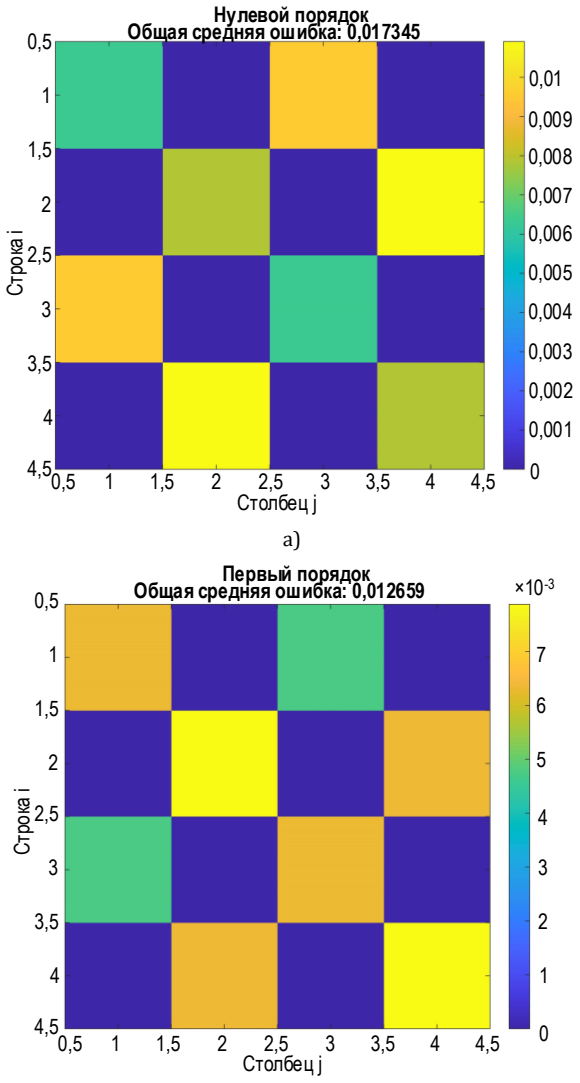


Рис. 2. Матрица ошибки между приближением нулевого (a) и первого (b) порядка и точным вычислением обратной матрицы

Fig. 2. Error Matrix between the Zero-Order (a) and First-Order (b) Approximation and the Exact Computation of the Inverse Matrix

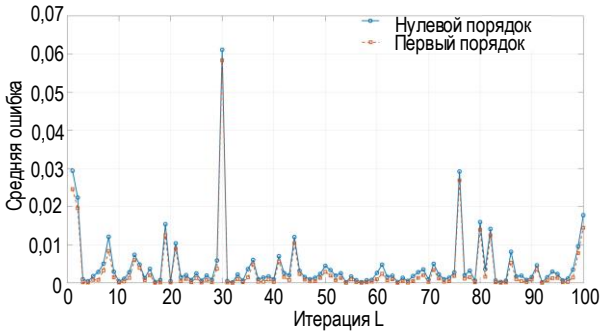


Рис. 3. Сравнение точности вычисления обратной матрицы при приближениях нулевого и первого порядка

Fig. 3. Comparison of the Accuracy of the Inverse Matrix Computation with Zero-Order and First-Order Approximations

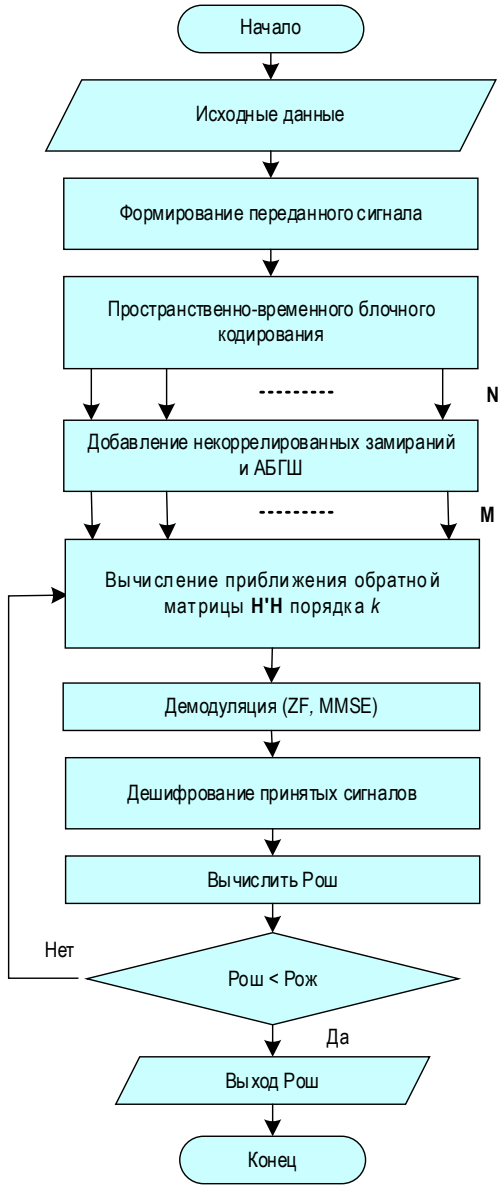


Рис. 4. Алгоритм предлагаемого метода демодуляции сигналов в системе MIMO

Fig. 4. Algorithm of the Proposed Signal Demodulation Method in the MIMO System

Основная идея предложенного алгоритма заключается в следующем: после обработки принятых сигналов от канала связи для вычисления матрицы **H'H**, применяется метод приближенного вычисления обратной матрицы, чтобы найти $(\mathbf{H}'\mathbf{H})^{-1}$порядка ноль ($k = 0$). Результат вычисления $(\mathbf{H}'\mathbf{H})^{-1}$ используется для демодуляции принятых сигналов с применением алгоритмов ZF, MMSE, после которых происходит дешифровка принятых сигналов с вычислением вероятности ошибки на каждом бите данных (Рош).

Затем полученное значение вероятности ошибки Рош сравнивается с ожидаемым значением Рож, которое, как правило, задается заранее (обычно Рож $= 10^{-5} - 10^{-6}$). Если полученное значение Рош соответствует требованию, алгоритм завершает вычисления обратной матрицы $(\mathbf{H}'\mathbf{H})^{-1}$ порядка ноль. В противном случае увеличивается значение k до $k = 1$ и повторяются процессы, как для $k = 0$. На основе экспериментальных данных (которые будут представлены позже) было установлено, что значение Рош, полученное при применении приближения порядка $k = 1$, не отличается значительно от значения Рош, полученного при точном вычислении обратной матрицы. Поэтому в предложенном алгоритме будет вычисляться обратная матрица с максимальным порядком, равным единице.

Результаты моделирования

Для оценки эффективности рассматриваемых методов было проведено численное моделирование в следующих условиях. Информационный сигнал без канального кодирования модулировался с использованием квадратурной фазовой манипуляции QPSK. Передача осуществлялась через канал с многолучевым распространением и рэлеевскими замираниями. Параметры канала были заданы следующим образом: разброс временны́х задержек многолучевых компонент находился в диапазоне от 10^{-9} до 10^{-6} с, а максимальный доплеровский сдвиг частоты составлял 100 Гц. На рисунке 5 представлены результаты сравнения помехоустойчивости методов демодуляции для системы MIMO с применением различных схем пространственно-временно́го кодирования.

Из представленных результатов (см. рисунок 5) можно сделать следующие выводы.

Во-первых, методы кодирования с ортогональной или квазиортогональной структурой, такие как OSTBC и QOSTBC, обеспечивают высокую эффективность в условиях сильных помех (низкое отношение сигнал / шум), несмотря на низкую скорость кодирования $R \leq 1$. При хорошем качестве канала передачи, а также в системах, предъявляющих высокие требования к скорости передачи данных, целесообразно применять методы STBC с повышенной скоростью кодирования ($R > 1$).

Во-вторых, наилучшими характеристиками среди рассмотренных методов демодуляции обладает метод ML, особенно в случае использования неортогональных методов кодирования STBC. Однако из-за высокой вычислительной сложности этот метод подходит только для систем с небольшим количеством передающих антенн, а также при использовании методов модуляции с низким порядком.

В-третьих, метод MMSE демонстрирует более высокую эффективность по сравнению с методом ZF, хотя при использовании кодирования OSTBC и QOSTBC это преимущество выражено менее явно.

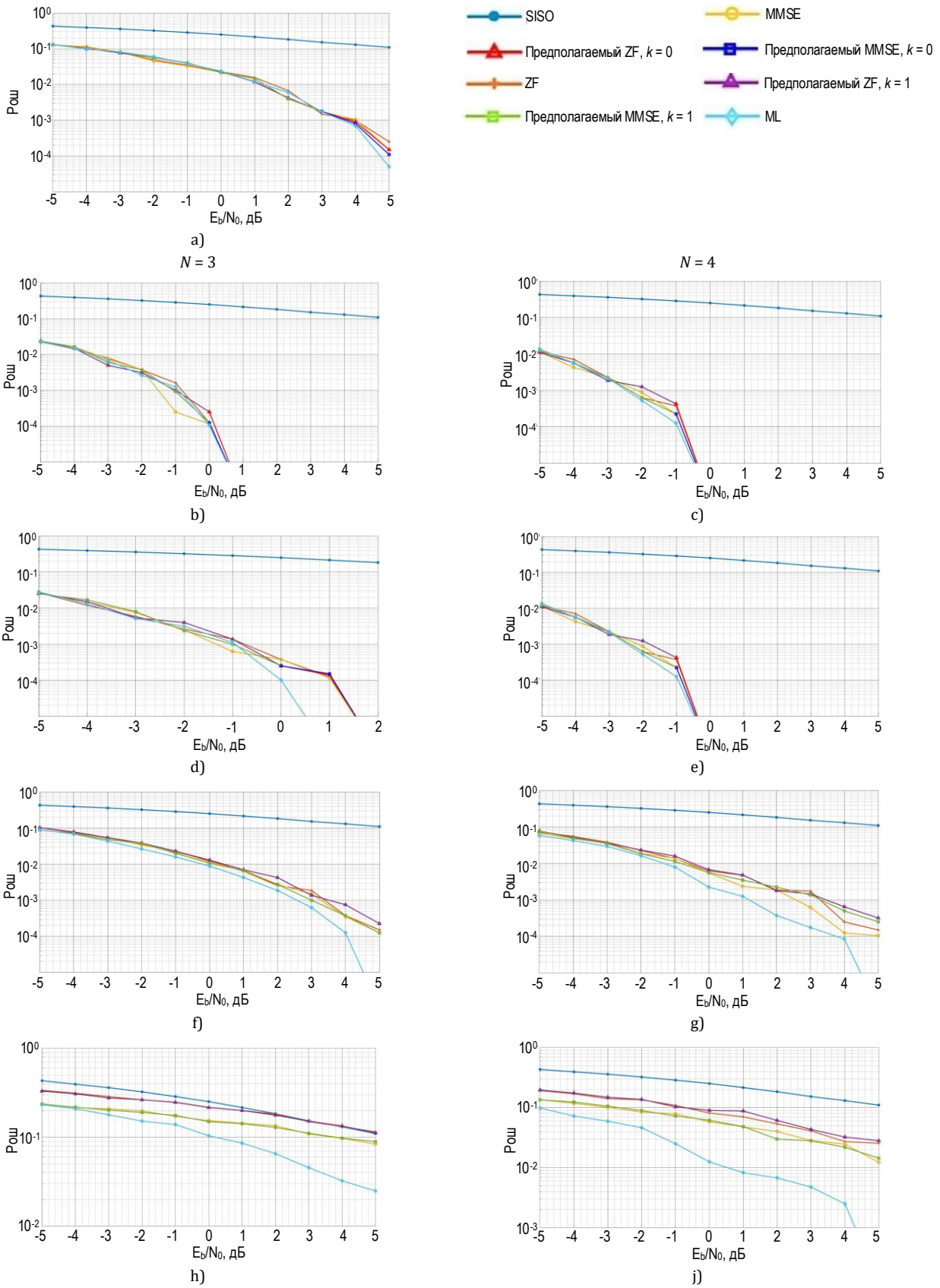


Рис. 5. Сравнение эффективности методов демодуляции сигналов системы MIMO с применением схемы Аламоути (a), OSTBC при скорости передачи R = 1/2 (b, c) и R = 3/4 (d, e), QOSTBC (f, g) и STBC при скорости передачи R = 2 (h, j)

Fig. 5. Performance Comparison of Demodulation Methods for a MIMO System Using the Alamouti Scheme (a), OSTBC at a Transmission Rate R = 1/2 (b, c) and R = 3/4 (d, e), QOSTBC (f, g), and STBC at a Transmission Rate R = 2 (h, j)

В-четвертых, предлагаемый алгоритм, направленный на снижение вычислительной сложности для методов ZF и MMSE, доказал свою эффективность, поскольку обеспечивает сопоставимую производительность по сравнению с точными реализациями этих методов, при этом значительно снижая объем вычислений при обработке сигналов.

По сравнению с классическими системами связи SISO, технологии MIMO обеспечивают существенное повышение надежности передачи данных и / или пропускной способности канала. В то же время, реализация многоантенных конфигураций сопряжена со значительным ростом вычислительной сложности алгоритмов обработки сигналов на приемной стороне.

Заключение

В работе рассмотрены методы пространственно-временно́го кодирования в системах MIMO. Представлены различные подходы к построению ПВКМ, направленные на максимизацию ортогональности методов OSTBC; на повышение скорости кодирования за счет утраты свойства ортогональности, как в случае применения методов STBC; а также методы, балансирующие между этими двумя критериями, такие как методы QOSTBC. Кроме того, в работе предложен алгоритм снижения вычислительной сложности существующих методов демодуляции сигналов ZF и MMSE в MIMO системах, основанный на применении аппроксимации обратной матрицы. Полученные результаты показывают, что предложенный алгоритм позволяет существенно сократить вычислительные затраты при сохранении высокой эффективности обработки сигнала.

Список источников

1. Варгаузин В.А., Цикин И.А. Методы повышения энергетической и спектральной эффективности цифровой радиосвязи. СПб.: БХВ-Петербург, 2013. 352 с. EDN SDSMUX

2. Быховский М.А. Гиперфазовая модуляция – оптимальный метод передачи сообщений в гауссовских каналах связи. М.: ТЕХНОСФЕРА, 2018. 310 с. EDN:IPVDXR

3. Лукьянчик Я.И., Левенец А.В., Чье Е.У. Модель системы передачи данных с обратной связью и адаптивным выбором кодирования по состоянию канала связи // Информационные технологии XXI века. 2015. С. 506–513. EDN:UDRXTH

4. Кульбида В.А. Способы помехоустойчивого кодирования и декодирования для построения систем связи с адаптацией этих способов к состоянию канала // Техника радиосвязи. 2006. № 11. С. 40–51. EDN:LTWRRX

5. Каменцев О.К. Алгоритмы обработки спектрально-эффективных сигналов с частотным мультиплексированием. Дис. … канд. физ.-мат. наук. Воронежский государственный университет, 2024. 131 с. EDN:JSKECY

6. Мальцев А.А., Рубцов А.Е. Исследование характеристик OFDM-систем радиосвязи с адаптивным отключением поднесущих // Вестник Нижегородского университета им. Н.И. Лобачевского. 2007. № 5. С. 43–49. EDN:JXCIBV

7. Бакулин М.Г., Крейнделин В.Б., Панкратов Д.Ю. Применение технологии MIMO в современных системах беспроводной связи разных поколений // T-Comm: Телекоммуникации и транспорт. 2021. Т. 15. № 4. С. 4–12. DOI:10.36724/2072-8735-2021-15-4-4-12. EDN:FPZEGW

8. Панкратов Д.Ю., Пахомова А.В. Применение технологии MIMO для улучшения характеристик физического уровня беспроводных сетей Wi-Fi // Наукоемкие технологии в космических исследованиях Земли. 2024. Т. 16. № 3. С. 55–61. DOI:10.36724/2409-5419-2024-16-3-55-61. EDN:UEAIEZ

9. Петров В.П., Якушев И.Ю. Современные технологии в системе MIMO // Вестник СибГУТИ. 2019. № 2. С. 94–108. EDN:HKRBBT

10. Комаров М.И., Панкратов Д.Ю., Степанова А.Г., Чуманов А.Е. Помехоустойчивость и вычислительная сложность алгоритмов демодуляции для систем MIMO с разным числом антенн // DSPA: Вопросы применения цифровой обработки сигналов. 2022. Т. 12. № 1. С. 39–47. EDN:ENKGOL

11. Крейнделин В.Б., Смирнов А.Э., Бен Режеб Т.Б.К. Эффективность методов обработки сигналов в системах MU-MIMO высоких порядков // T-Comm: Телекоммуникации и транспорт. 2016. Т. 10. № 12. С. 24–30. EDN:XKNRRJ

12. Alamouti S.M. A simple transmit diversity technique for wireless communications // IEEE Journal on Selected Areas in Communications. 1998. Vol. 16. Iss. 8. PP. 1451–1458. DOI:10.1109/49.730453

13. Tarokh V., Jafarkhani H., Calderbank R. Space-time block coding for wireless communications: performance results // IEEE Journal on Selected Areas in Communications. 1999. Vol. 17. Iss. 3. PP. 451–460. DOI:10.1109/49.753730

14. Ganesan G., Stoica P. Space-time block codes: A maximum SNR approach // IEEE Transactions on Information Theory. 2001. Vol. 47. Iss. 4. PP. 1650–1656. DOI:10.1109/18.923754

15. Arti M.K. OSTBC Transmission in Large MIMO Systems // IEEE Communications Letters. 2016. Vol. 20. Iss. 11. PP. 2308–2311. DOI:10.1109/LCOMM.2016.2597229

16. Ozbek B., Ruyet D., Bellanger M. Non-Orthogonal Space-Time Block Coding Design for 3 Transmit Antennas. 2003. URL: https://easytp.cnam.fr/leruyet/Publications/gretsi2003.pdf (Accessed 25.06.2025)

17. Dama Y., Abd-Alhameed R., Ghazaany T., Zhu S. A New Approach for OSTBC and QOSTBC // International Journal of Computer Applications. 2013. Vol. 67. Iss. 6. PP. 45–48. DOI:10.5120/11403-6719

18. Wu C., Yang S., Xiao Y., Xiao M. Quasi-Orthogonal Space-Time Block Coded Spatial Modulation // IEEE Transactions on Communications. 2022. Vol. 70. Iss. 12. PP. 7872–7885. DOI:10.1109/TCOMM.2022.3216805. EDN:JFXAGD

19. Seema S., Arti M.K., Reddy B. Data Detection in Large MIMO System with Reduced Computational Complexity for

QOSTBC Transmission // Proceedings of the 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE, Ghaziabad, India, 23–24 November 2023). IEEE, 2023. PP. 46–50. DOI:10.1109/AECE59614.2023.10428602

20. Jung Y.-H., Nam S.H., Chung J., Kim Y., Ko K., Chae C.-B., et al. Enhancement of Rate 2 STC with Antenna Grouping // IEEE 802.16 Broadband Wireless Access Working Group. 2004. URL: https://www.ieee802.org/16/tge/contrib/C80216e-04_555.pdf (Accessed 25.06.2025)

21. Chae C.-B., Roh W., Yun S.-R., Ko K., Jeong H., Oh J.T., et al. Enhancement of STC with Antenna Grouping // IEEE 802.16 Broadband Wireless Access Working Group. 2004. URL: https://ieee802.org/16/tge/contrib/C80216e-04_554r4.pdf (Accessed 25.06.2025)

22. Djemamar Y., Ibnyaich S., Zeroual A. Space-Time Block Coding Techniques for MIMO 2×2 System using Walsh-Hadamard Codes // Journal of International Conference on Electrical and Information Technologies. 2022. PP. 1–7. DOI:10.6109/jicce.2022.20.1.1

23. Mecklenbräuker C.F., Rupp M. Generalized Alamouti Codes for Trading Quality of Service Against Data Rate in MIMO UMTS // EURASIP Journal on Advances in Signal Processing. 2004. PP. 662–675. DOI:10.1155/S1110865704310061

24. Быховский М.А. Пространственно-временное кодирование в системах MISO // Электросвязь. 2020. № 1. С. 67–75. DOI:10.34832/ELSV.2020.2.1.010. EDN:LARTEL

25. Смирнов А.Э. Снижение порядка вычислительной сложности алгоритмов детектирования в многоантенных системах за счёт использования алгоритмов быстрого умножения матриц // Фундаментальные проблемы радиоэлектронного приборостроения. 2015. Т. 15. № 5. С. 267–270. EDN:VOUGPX

26. Панкратов Д.Ю., Степанова А.Г. Вычислительная сложность алгоритмов демодуляции систем MIMO с большим числом антенн // DSPA: Вопросы применения цифровой обработки сигналов. 2021. Т. 11. № 1. С. 11–20. EDN:QTSOZP

27. Khrapov P.V., Volkov N.S. Comparative analysis of Jacobi and Gauss-Seidel iterative methods // International Journal of Open Information Technologies. 2024. Vol. 12. Iss. 2. PP. 23–34. DOI:10.48550/arXiv.2307.09809. EDN:INYTHE

28. Björck, Å. Numerical Methods in Matrix Computations. Cham: Springer, 2015. 551 p. DOI:10.1007/978-3-319-05089-8

29. Cho Y.S., Kim J., Yang W.Y., Kang C.G. MIMO-OFDM Wireless Communications with MATLAB. John Wiley & Sons, 2010. 439 p. DOI:10.1002/9780470825631. EDN:SRQIDH

References

1. Vargauzin V.A., Tsikin I.A. *Methods for Improving Energy and Spectral Efficiency of Digital Radio Communication*. St. Petersburg: BHV-Peterburg Publ.; 2013. 352 p. (in Russ.) EDN:SDSMUX

2. Bykhovskii M. Hyperphase Modulation – the Optimal Method of Message Transmission in the Gaussian Communication Channels. Moscow: Tekhnosfera Publ.; 2018. 310 p. (in Russ.) EDN:IPVDXR

3. Lukyanchik Ya.I., Levenets A.V., Chye E.U. Model of a Data Transmission System with Feedback and Adaptive Coding Selection Based on Channel State. *Information Technologies of the 21st Century.* 2015:506–513. (in Russ.) EDN:UDRXTH

4. Kulbida V.A. Methods of Error-Resistant Coding and Decoding for Building Communication Systems with Adaptation to Channel State. *Tekhnika radiosvyazi*. 2006;11:40–51. (in Russ.) EDN:LTWRRX

5. Kamentsev O.K. *Algorithms for Processing Spectrally Efficient Signals with Frequency Multiplexing*. Ph.D. Thesis. Voronezh State University Publ.; 2024. 131 p. (in Russ.) EDN:JSKECY

6. Maltsev A.A., Rubtsov A.E. Investigation of Performance of OFDM Wireless Communication Systems with Adaptive Subcarrier Puncturing. *Vestnik Nizhegorodskogo universiteta im. N.I. Lobachevskogo.* 2007;5:43–49. (in Russ.) EDN:JXCIBV

7. Bakulin M.G., Kreindelin V.B., Pankratov D.Yu. Application of MIMO Technology in Modern Wireless Communication Systems of Different Generations. *T-Comm.* 2021;15(4):4–12. (in Russ.) DOI:10.36724/2072-8735-2021-15-4-4-12. EDN:FPZEGW

8. Pankratov D.Yu., Pakhomova A.V. Application of MIMO Technology to Improve Physical Layer Characteristics of Wi-Fi Wireless Networks. *H&ES Research.* 2024;16(3):55–61. (in Russ.) DOI:10.36724/2409-5419-2024-16-3-55-61. EDN:UEAIEZ

9. Petrov V.P., Yakushev I.Yu. Modern Technologies in MIMO Systems. *The Herald of the Siberian State University of Telecommunications and Information Science*. 2019;2:94–108. (in Russ.) EDN:HKRBBT

10. Komarov M.I., Pankratov D.Yu., Stepanova A.G., Chumanov A.E. Noise Immunity and Computational Complexity of Demodulation Algorithms for MIMO Systems with Different Numbers of Antennas. *Digital Signal Processing and Its Applications.* 2022;12(1):39–47. (in Russ.) EDN:ENKGOL

11. Kreindelin V.B., Smirnov A.E., Ben Rezheb T.B.K. Efficiency of Signal Processing Methods in High-Order MU-MIMO Systems. *T-Comm*. 2016;10(12):24–30. (in Russ.) EDN:XKNRRJ

12. Alamouti S.M. A simple transmit diversity technique for wireless communications. *IEEE Journal on Selected Areas in Communications*. 1998;16(8):1451–1458. DOI:10.1109/49.730453

13. Tarokh V., Jafarkhani H., Calderbank R. Space-time block coding for wireless communications: performance results. *IEEE Journal on Selected Areas in Communications*. 1999;17(3):451–460. DOI:10.1109/49.753730

14. Ganesan G., Stoica P. Space-time block codes: A maximum SNR approach. *IEEE Transactions on Information Theory*. 2001;47(4):1650–1656. DOI:10.1109/18.923754

15. Arti M.K. OSTBC Transmission in Large MIMO Systems. *IEEE Communications Letters*. 2016;20(11):2308–2311. DOI:10.1109/LCOMM.2016.2597229

16. Ozbek B., Ruyet D., Bellanger M. *Non-Orthogonal Space-Time Block Coding Design for 3 Transmit Antennas*. 2003. URL: https://easytp.cnam.fr/leruyet/Publications/gretsi2003.pdf [Accessed 25.06.2025]

17. Dama Y., Abd-Alhameed R., Ghazaany T., Zhu S. A new approach for OSTBC and QOSTBC. *International Journal of*

Computer Applications. 2013;67(6):45–48. DOI:10.5120/11403-6719
18. Wu C., Yang S., Xiao Y., Xiao M. Quasi-Orthogonal Space-Time Block Coded Spatial Modulation. *IEEE Transactions on Communications*. 2022;70(12):7872–7885. DOI:10.1109/TCOMM.2022.3216805. EDN:JFXAGD
19. Seema S., Arti M.K., Reddy B. Data Detection in Large MIMO System with Reduced Computational Complexity for QOSTBC Transmission. *Proceedings of the 3rd International Conference on Advancement in Electronics & Communication Engineering, AECE, 23–24 November 2023, Ghaziabad, India*. IEEE; 2023. p.46–50. DOI:10.1109/AECE59614.2023.10428602
20. Jung Y.-H., Nam S.H., Chung J., Kim Y., Ko K., Chae C.-B., et al. *Enhancement of Rate 2 STC with Antenna Grouping*. 2004. URL: https://www.ieee802.org/16/tge/contrib/C80216e-04_555.pdf [Accessed 25.06.2025]
21. Chae C.-B., Roh W., Yun S.-R., Ko K., Jeong H., Oh J.T., et al. *Enhancement of STC with Antenna Grouping*. 2004. URL: https://ieee802.org/16/tge/contrib/C80216e-04_554r4.pdf [Accessed 25.06.2025]
22. Djemamar Y., Ibnyaich S., Zeroual A. Space-Time Block Coding Techniques for MIMO 2×2 System using Walsh-Hadamard Codes. *Journal of International Conference on Electrical and Information Technologies*. 2022:1–7. DOI:10.6109/jicce.2022.20.1.1
23. Mecklenbräuker C.F., Rupp M. Generalized Alamouti Codes for Trading Quality of Service Against Data Rate in MIMO UMTS. *EURASIP Journal on Advances in Signal Processing*. 2004:662–675. DOI:10.1155/S1110865704310061
24. Bykhovskii M.A. Space-Time Coding In Miso Systems. *Elektrosvyaz.* 2020;1:67–75. (in Russ.) DOI:10.34832/ELSV.2020.2.1.010. EDN:LARTEL
25. Smirnov A.E. Reducing the Computational Complexity of Detection Algorithms in Multi-Antenna Systems Using Fast Matrix Multiplication Algorithms. *Fundamentalnye problemy radioelektronnogo priborostroeniya*. 2015;15(5):267–270. (in Russ.) EDN:VOUGPX
26. Pankratov D.Yu., Stepanova A.G. Computational Complexity of Demodulation Algorithms for MIMO Systems with a Large Number of Antennas*. Digital Signal Processing and Its Applications.* 2021;11(1):11–20. (in Russ.) EDN:QTSOZP
27. Khrapov P.V., Volkov N.S. Comparative analysis of Jacobi and Gauss-Seidel iterative methods. *International Journal of Open Information Technologies*. 2024;12(2):23–34. DOI:10.48550/arXiv.2307.09809. EDN:INYTHE
28. Björck Å. *Numerical Methods in Matrix Computations.* Cham: Springer; 2015. 551 p. DOI:10.1007/978-3-319-05089-8
29. Cho Y.S., Kim J., Yang W.Y., Kang C.G. *MIMO-OFDM Wireless Communications with MATLAB*. John Wiley & Sons; 2010. 439 p. DOI:10.1002/9780470825631. EDN:SRQIDH

Статья поступила в редакцию 19.05.2025; одобрена после рецензирования 03.06.2025; принята к публикации 10.06.2025.
The article was submitted 19.05.2025; approved after reviewing 03.06.2025; accepted for publication 10.06.2025.

Информация об авторах:

ФАМ Конг Куен — аспирант кафедры радиотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
https://orcid.org/0009-0005-5305-3872

ГЛУШАНКОВ Евгений Иванович — доктор технических наук, профессор, профессор кафедры радиотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
https://orcid.org/0000-0001-8842-7903

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

Review research
УДК 004.056
https://doi.org/10.31854/1813-324X-2025-11-3-72-86
EDN:HSXTLS

A Comprehensive Review of Deep Learning in Intrusion Detection Systems

Mokhalad M.A. Al-Tameemi[1], Almokhalad44@gmail.com
Abbas A.H. Alzaghir[2], a.a.h.alzagi@mtuci.ru
Malik A.M. Alsweity[3], al-sveiti.mam@sut.ru

[1]Saint Petersburg Electrotechnical University "LETI",
St. Petersburg, 197022, Russian Federation
[2]Moscow Technical University of Communication and Informatics,
Moscow, 123423, Russian Federation
[3]The Bonch-Bruevich Saint Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Annotation

Deep learning methods play a crucial role in enhancing the effectiveness of intrusion detection systems. This study presents a comparative analysis of seven deep learning models, including autoencoders, restricted Boltzmann machines, deep belief networks, convolutional and recurrent neural networks, generative adversarial networks, and deep neural networks. The primary focus is on accuracy, precision, and recall metrics, evaluated using the NSL-KDD dataset. The analysis demonstrated the high effectiveness of recurrent neural networks, which achieved an accuracy of 99.79 %, precision of 99.67 %, and recall of 99.86 %.

The objective of the study: *of this paper is to enhance the effectiveness of intrusion detection systems through a comparative analysis of the performance of various deep learning models and an assessment of their applicability in the context of dynamic network security threats.*

The proposed solution involves *a comparative analysis of seven deep learning models to identify the most effective ones for network security tasks. This analysis aids in selecting the optimal models for specific security requirements.*

The evaluation methodology *involves the use of the benchmark dataset NSL-KDD, which contains various types of attacks and normal connections. The key evaluation metrics are accuracy, precision, and recall.*

The system implementation *is based on deep learning frameworks such as TensorFlow. The results of the system's performance and their interpretation are presented in the paper.*

Experiments *with the NSL-KDD dataset demonstrated accuracy, precision, and recall for all the deep learning models considered.*

The scientific novelty *is the ability to obtain formal performance evaluations of various deep learning models for intrusion detection systems, taking into account their architectural features, the processing of temporal and spatial data, as well as the characteristics of network traffic and attack types.*

The theoretical significance *is the expansion of methods for evaluating the effectiveness of intrusion detection systems through the analysis and comparison of the performance of deep learning models in the context of processing complex and high-dimensional network data.*

The practical significance *is the application of the comparative analysis results for selecting the most effective solutions in intrusion detection systems and optimizing them for real-world operating conditions.*

Keywords: *deep learning, intrusion detection systems, autoencoders, restricted boltzmann machines, deep belief networks, convolutional neural networks, recurrent neural networks, generative adversarial networks, network security*

For citation: Al-Tameemi M.M.A., Alzaghir A.A.H., Alsweity M.A.M. A Comprehensive Review of Deep Learning in Intrusion Detection Systems. *Proceedings of Telecommunication Universities.* 2025;11(3):72–86. DOI:10.31854/1813-324X-2025-11-3-72-86. EDN:HSXTLS

Обзорная статья
https://doi.org/10.31854/1813-324X-2025-11-3-72-86
EDN:HSXTLS

Комплексный обзор глубокого обучения в системах обнаружения вторжений

Мохалад М.А. Аль-Тамими[1], Almokhalad44@gmail.com
Аббас А.Х. Алзагир[2], a.a.h.alzagi@mtuci.ru
Малик А.М. Аль-Свейти[3], al-sveiti.mam@sut.ru

[1]Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург, 197022, Российская Федерация
[2]Московский технический университет связи и информатики, Москва, 123423, Российская Федерация
[3]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация

Аннотация

Методы глубокого обучения играют ключевую роль в повышении эффективности систем обнаружения вторжений. В работе проведен сравнительный анализ семи моделей глубокого обучения, включая автоэнкодеры, ограниченные машины Больцмана, сети глубокого убеждения, сверточные и рекуррентные нейронные сети, генеративно-состязательные сети и глубокие нейронные сети. Основное внимание уделено метрикам точности, прецизионности и полноты на основе датасета NSL-KDD. Анализ показал высокую эффективность рекуррентных нейронных сетей, достигших точности 99,79 %, прецизионности 99,67 % и полноты 99,86 %. ***Цель статьи*** *– повышение эффективности систем обнаружения вторжений через сравнительный анализ производительности различных моделей глубокого обучения и оценку их применимости в условиях динамичных угроз сетевой безопасности.*

Предлагаемое решение состоит *в сравнительном анализе семи моделей глубокого обучения, чтобы выявить наиболее эффективные для задач защиты сети. Данный анализ помогает выбрать оптимальные модели для конкретных условий безопасности.* ***Методика оценки*** *включает использование эталонного набора данных NSL-KDD, который содержит различные типы атак и нормальных соединений. Ключевые метрики оценки – точность, прецизионность и полнота.* ***Реализация*** *системы выполнена на основе фреймворков глубокого обучения, таких как TensorFlow.* ***Эксперименты*** *с набором данных NSL-KDD показали точность, прецизионность и полноту для всех рассмотренных моделей глубокого обучения.*

Научная новизна *заключается в возможности получения формальных оценок производительности различных моделей глубокого обучения для систем обнаружения вторжений, с учетом их архитектурных особенностей, обработки временны́х и пространственных данных, а также характеристик сетевого трафика и типов атак.*

Теоретическая значимость *заключается в расширении методов оценки эффективности систем обнаружения вторжений путем анализа и сравнения производительности моделей глубокого обучения в условиях обработки сложных и высокоразмерных сетевых данных.*

Практическая значимость *заключается в применении результатов сравнительного анализа для выбора наиболее эффективных решений в системах обнаружения вторжений и их оптимизации для реальных условий эксплуатации.*

Ключевые слова: *глубокое обучение, системы обнаружения вторжений, автоэнкодеры, ограниченные машины Больцмана, сети глубоких убеждений, сверточные нейронные сети, рекуррентные нейронные сети, генеративно-состязательные сети, сетевая безопасность*

Ссылка для цитирования: Аль-Тамими М.М.А., Алзагир А.А.Х., Аль-Свейти М.А.М. Комплексный обзор глубокого обучения в системах обнаружения вторжений // Труды учебных заведений связи. 2025. Т. 11. № 3. С. 72–86. (in Russ.) DOI:10.31854/1813-324X-2025-11-3-72-86. EDN:HSXTLS

1. INTRODUCTION

Deep learning is widely used in computer or network security and we can define it as a type of machine learning methods based on artificial neural networks and the idea of learning representations. The term "deep" comes from the multilayered structure of the network. In general, deep learning models are of several types, including DNNs [1], CNNs [2], DBNs [3], and RNNs [4], which have been categorized under the different exemplars of the supervised learning model. Concurrently, restricted Boltzmann machines (RBMs) [5], autoencoders (AEs) [5,6], and generative adversarial networks (GANs) [7] are some of the models that can be used for unsupervised learning. In deep learning, features can be automatically extracted from raw data, like images and text and analyses the data [8, 9], this capability is particularly useful in intrusion detection systems, where deep learning models can process complex and high-dimensional data to identify potential threats [9, 10], so feature engineering by hand is not necessary. This skill allows the use of deep models on many kinds of data and gives it a considerable advantage over shallow models, mainly in dealing with vast datasets [11]. Deep learning techniques may be applied in the anomaly detection field for dimensionality reduction and classification tasks. Handcrafted feature engineering becomes insufficient for the increasingly larger, high-dimensional datasets; instead, deep learning models have been able to automatically capture complicated knowledge in these forms of data. At the same time, they may adapt to network behavior and dynamically varying attributes in attack scenarios [12]. Figure 1 shows the basic architecture for a deep learning-based IDS.

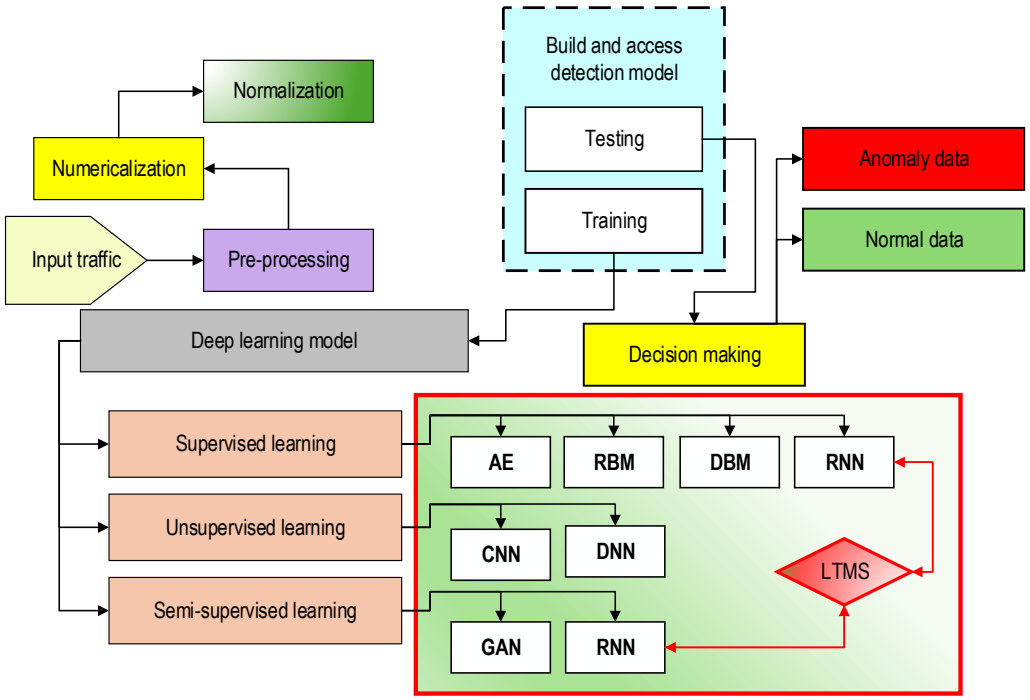


Fig. 1. Architecture of Deep Learning Based Intrusion Detection System

The use of deep learning techniques requires large and intensive computational resources during the training phase, involving many hidden layers with many elements, leading to high computational complexity. However, deep learning algorithms naturally involve large-scale matrix multiplication thanks to the development of modern processing technologies. In recent years, fast advancements in processing technologies enabled the improved availability of graphics processing units (GPUs) and artificial intelligence (AI) accelerators. Integration of these technologies into mobile devices and Internet of Things (IoT) devices has made it possible to deploy deep learning models on resource-constrained environments.

2. DEEP LEARNING MODELS

Deep learning models can be classified in to supervised learning, unsupervised learning and simi- supervised learning [13].

2.1. Supervised Learning

2.1.1. Autoencoder

An autoencoder is a specialized neural network architecture comprising two principal components the encoder and the decoder [14]. As illustrated in Figure 2, the encoder is responsible for extracting important features from the input data, while the decoder reconstructs the original data using these extracted features.

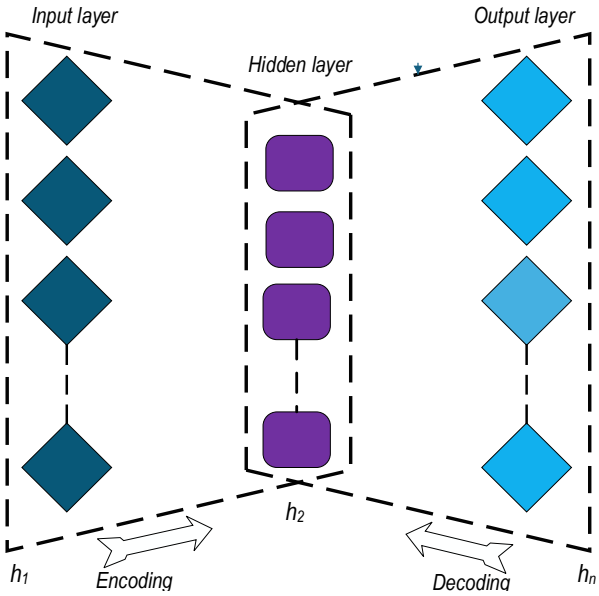


Fig. 2. Structural Model of the Auto-Encoder

This method is fundamentally similar to the traditional autoencoder framework [5, 15, 16], though it operates in a supervised manner. Throughout the training process, the gap between the encoder's input and the decoder's output narrows progressively, indicating that the features learned by the encoder accurately capture the significant information embedded in the original data, as evidenced by the decoder's ability to reconstruct the input data from these features. The encoder functions as a neural network with one or more hidden layers [14]. It transforms the input data, often noisy, into a compressed representation, or latent space, which contains fewer dimensions than the input data. This compression is achieved through the following equation:

$$h = f_{AE}(m) + W_{enc}M + b_{enc}\,, \qquad (1)$$

where m represents the input data; W_{enc} is the encoder's weight matrix; b_{enc} is the bias vector; h is the encoded representation. The function f_{AE} applies an activation function, such as ReLU or sigmoid, to the linear transformation of the input. The decoder is responsible for reconstructing the original data from the compressed encoding. It receives the encoded data h from the encoder and produces an approximation of the original input data.

The decoding process is mathematically defined as:

$$\hat{m} = g_{AE}(h) + W_{dec}h + b_{dec}, \qquad (2)$$

where $\hat{m}$ is the reconstructed input data; W_{dec} is the decoder's weight matrix; b_{dec} is the corresponding bias vector. The function g_{AE} applies an activation function to the decoder's output. The training objective is to minimize the loss function, which consists of several terms: the reconstruction error, weight regularization, and a sparsity constraint.

The reconstruction error is the mean squared difference between the original input data m_i and its reconstructed counterpart $\hat{m}_i$:

$$\mathcal{L}_{recon} = \frac{1}{N_{train}} \sum_{i=1}^{N_{train}} \sum_{j=1}^{N_{para}} (m_{ij} - \hat{m}_{ij})^2, \qquad (3)$$

where N_{train} is the number of training samples; N_{para} is the number of parameters (or features) per sample.

Additionally, weight regularization Ω_W is employed to prevent overfitting by penalizing excessively large weights:

$$\Omega_W = \frac{1}{2} \sum_{i=1}^{N_{train}} \sum_{j=1}^{N_{para}} w_{ij}^2. \qquad (4)$$

The sparsity constraint Ω_s encourages the model to activate only a small subset of the hidden units, thus promoting efficient learning. It is defined as:

$$\Omega_s = \sum_{k=1}^{N_{node}} \rho \log\left(\frac{\rho}{\hat{\rho}_k}\right) + (1-\rho)\log\left(\frac{1-\rho}{1-\hat{\rho}_k}\right), \qquad (5)$$

where ρ is the desired average activation for the sparsity constraint; $\hat{\rho}_k$ is the actual activation of the $k-th$ hidden unit.

The average activation $\hat{\rho}_k$ is computed as the mean activation across the training samples:

$$\hat{\rho}_k = \frac{1}{N_{train}} \sum_{i=1}^{N_{train}} k_h(m_i), \qquad (6)$$

where $k_h(m_i)$ is the activation function of the $k-th$ hidden unit for the $i-th$ training sample, the total loss function $\mathcal{L}$ to be minimized is the sum of the reconstruction error, weight regularization, and sparsity constraint:

$$\mathcal{L} = \mathcal{L}_{recon} + \lambda\Omega_W + \beta\Omega_s, \qquad (7)$$

where λ and β are regularization parameters that control the importance of the weight regularization and sparsity terms, respectively. By comparing the reconstruction error for new input data, the trained autoencoder widely used for anomaly detection (IDS).By comparing the reconstruction error for fresh input data m to a predetermined threshold, the trained autoencoder may be utilized for anomaly detection (IDS). The input is deemed abnormal if the reconstruction error is greater than this cutoff.

This is how the reconstruction error is calculated:

$$error = \|m - \hat{m}\|. \qquad (8)$$

This ability to reconstruct normal data patterns and detect deviations makes the autoencoder a good tool for identifying anomalous activities in IDS applications.

According to [14] Autoencoder can process two main categories of attack kinds are assault and regular. There are around 38 subclasses for the attacks. The class is transformed into a binary class for normal and attack because of numerous distinct attack kinds and feature sets. Evaluation metrics are utilized to evaluate this data. Next, we will adjust our dense autoencoder for this model. Figure 3 showing the evaluation metrics, ROC curve, and confusion matrix look like this with using NSL-KDD dataset.

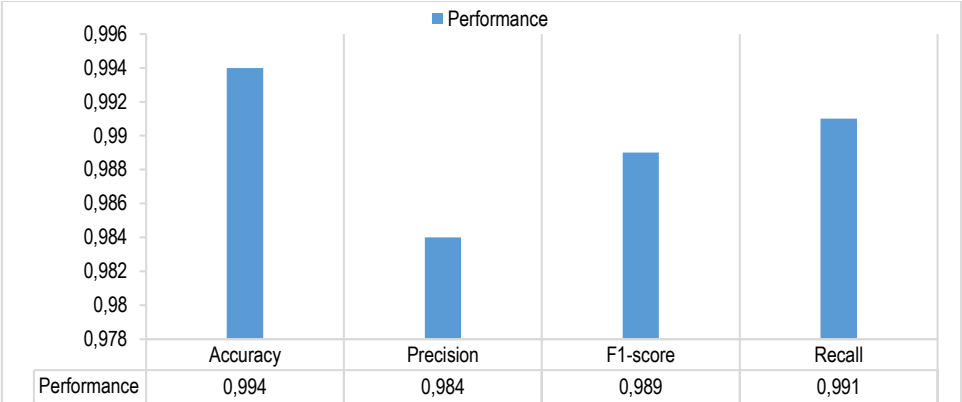


Fig. 3. Autoencoder Evaluation Metrics Using NSL-KDD Dataset [14]

2.1.2. Restricted Boltzmann Machine (RBM)

A Restricted Boltzmann Machine (RBM) is a stochastic neural network widely used in intrusion detection systems (IDS) for its ability to extract features from complex network data and detect anomalies [5]. It consists of a visible layer *V* that represents the input data and a hidden layer *H* that encodes latent features [17] Figure 4 showing Structural model of the RBM.

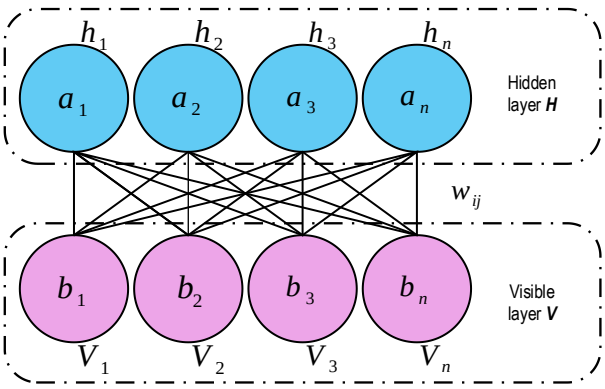


Fig. 4. Structural Model of the Restricted Boltzmann Machine (RBM)

The layers are fully connected to each other, but there are no connections within a single layer [17]. RBMs do not distinguish between forward and backward directions, making the weights symmetric. This property is critical for training RBMs effectively using contrastive divergence. The energy function of the RBM is defined as:

$$E(\varphi, h) = -\sum_{i-1}^{N} a_i \varphi_i - \sum_{j-1}^{M} b_j h_j - \sum_{i,j} \varphi_i h_j w_{ij}. \quad (9)$$

During training, the probability of activating a hidden unit given the visible units is computed as:

$$P(h_i) = \sigma\left(b_i + \sum_{i=1}^{n} \varphi_i w_{ij}\right), \quad (10)$$

where $\sigma(x)$ is the sigmoid activation function:

$$\sigma(x) = \frac{1}{1 + \exp(-x)}. \quad (11)$$

To reconstruct the visible layer, the conditional probability for each visible unit given the hidden units is calculated as:

$$P(\varphi_i) = \sigma\left(a_i + \sum_{j=1}^{m} h_j w_{ij}\right). \quad (12)$$

The RBM is trained by minimizing the difference between the data and its reconstruction [18].

Weight updates are calculated using the contrastive divergence algorithm:

$$\delta w_{ij} = \epsilon\left(\langle \varphi_i h_j \rangle_{data} - \langle \varphi_i h_j \rangle_{model}\right), \quad (13)$$

where ϵ is the learning rate; $\langle \varphi_i h_j \rangle_{data}$ represents the expectation over the training data; $\langle \varphi_i h_j \rangle_{model}$ represents the expectation over the model distribution.

Bias updates for the visible and hidden layers are defined as:

$$\delta a_i = \epsilon(\langle \varphi_i \rangle_{data} - \langle \varphi_i \rangle_{recon}), \quad (14)$$

$$\delta b_j = \epsilon\left(\langle h_j \rangle_{data} - \langle h_j \rangle_{recon}\right). \quad (15)$$

A sparsity constraint is often introduced to enforce meaningful feature extraction. The sparsity penalty is:

$$\Omega_s = \sum_{j=1}^{M} \left[\rho \log\left(\frac{\rho}{\hat{\rho}_j}\right) + (1-\rho) \log\left(\frac{1-\rho}{1-\hat{\rho}_j}\right)\right], \quad (16)$$

where the average activation of a hidden unit is:

$$\hat{\rho}_j = \frac{1}{N}\sum_{i=1}^{N} P(1|\varphi_i). \quad (17)$$

The reconstruction error, typically measured as the mean squared error (MSE), is minimized during training to enhance model performance:

$$MSE = \frac{1}{N}\sum_{i=1}^{N}\sum_{j=1}^{M}(\varphi_{ij} - \varphi_{ij}, recon)^2, \quad (18)$$

these equations and principles allow the RBM to effectively model normal network behavior while identifying deviations that signify potential intrusions. According to [19] Experiment was performed by only adjusting the size of training data on the model set with the batch data of 10 and the learning rate of 0.01 showing the top performance in the above trial. Figure 5 showing Accuracy, Precision, Recall and F-measure with batch size = 10 and learning rate = 0.1 using NSL-KDD dataset.

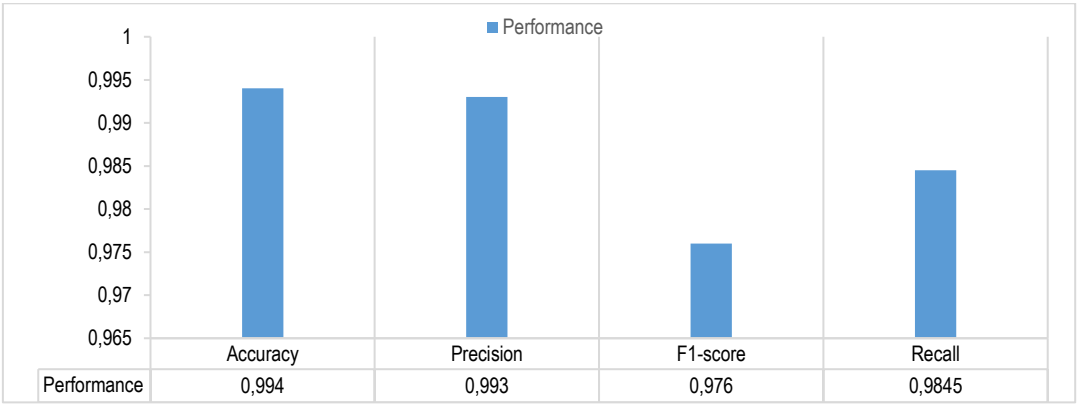


Fig. 5. RBM Evaluation Metrics Using NSL-KDD Dataset [19]

2.1.3. Deep Belief Networks (DBNs)

Deep Belief Networks (DBNs) are highly effective tools for Intrusion Detection Systems (IDS). A DBN is constructed by stacking multiple Restricted Boltzmann Machines (RBMs), where the output of one layer serves as the input to the next. As shown in Figure 6, the DBN architecture consists of an input layer, multiple hidden layers, and a softmax layer at the top for classification.

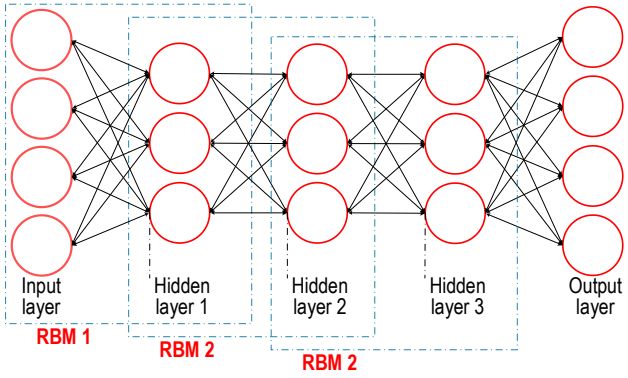


Fig. 6. Structural Model of the DBNs

The DBN is trained in a layer-wise manner using the following principles: First, in unsupervised pretraining, each RBM in the DBN is trained individually [3, 20]. The energy function of an RBM is defined as:

$$E(v,h) = -\sum_{i=1}^{N} a_i v_i - \sum_{j=1}^{M} b_j h_j - \sum_{i=1}^{N}\sum_{j=1}^{M} v_i h_j w_{ij}, \quad (19)$$

where v and h represent the visible and hidden layers, respectively a_i and b_j are their biases, and w_{ij} are the weights connecting the layers. During training, the probability of hidden units and visible units being activated is calculated as:

$$P(h_i) = \sigma\left(b_j + \sum_i v_i w_{ij}\right), \quad (20)$$

$$P(v_i) = \sigma\left(a_j + \sum_j h_j w_{ij}\right), \quad (21)$$

where $\sigma(x)$ is the sigmoid activation function:

$$\sigma(x) = \frac{1}{1+e^{-x}}. \quad (22)$$

After unsupervised pretraining, the entire DBN is fine-tuned using supervised learning, which involves minimizing a loss function, such as cross-entropy for classification tasks, and optimizing the weights and biases across all layers [3, 20]. For final classification in IDS, a softmax layer is added at the top of the DBN.

The probability of class k is given by:

$$P(y,k|x) = \frac{\exp(z_k)}{\sum_{j=1}^{k}\exp(z_j)}, \quad (23)$$

where z_k represents the activation of the $k-th$ neuron in the softmax layer. This hierarchical approach allows DBNs to extract meaningful features from raw

data and enhance detection performance, making them well-suited for IDS applications. By combining unsupervised feature learning and supervised classification, DBNs improve the ability to detect and classify intrusions effectively.

According to [21] DBNs integrate feature extraction and classification modules into a system that can automatically extract features and classify them. This is an effective way to improve the detection performance. Figure 7 showing the classification performance of DBN was evaluated on the NSL-KDD.

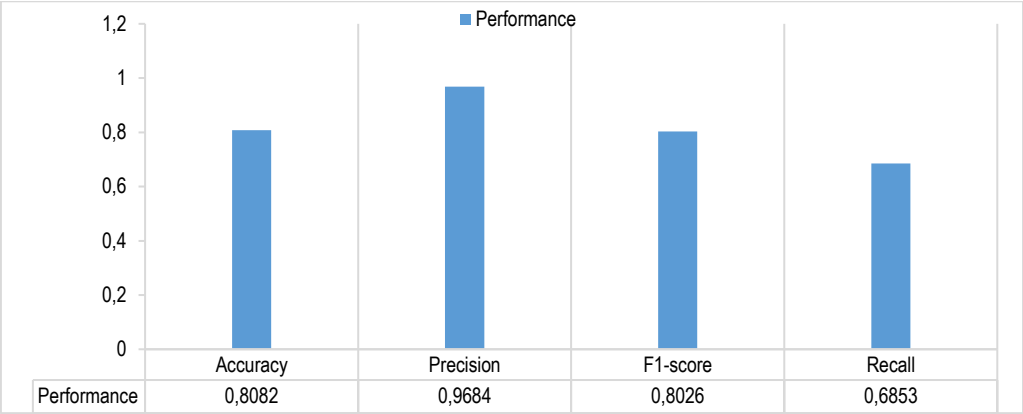


Fig. 7. DBM Evaluation Metrics Using NSL-KDD Dataset [21]

2.1.4. Recurrent Neural Networks (RNN)

RNN Conventional systems frequently depended on streamlined encoding techniques, including one-hot encoding [22]. Nevertheless, one-hot encoding's incapacity to accurately capture semantic similarities between features is a major drawback. Researchers are using LSTM networks to tackle this problem [23]. Long-term selective retention of pertinent information is made easier by LSTM networks, which incorporate memory cells and control mechanisms to manage information flow. Additionally, because RNN-LSTM can capture long-term dependencies, the model can identify subtle deviations that may be signs of intrusions the network is recurrent sequential analysis is made possible, which is crucial for comprehending the temporal dynamics of network behavior [23]. The architecture allows IDS-RNN model to adaptively learn from historical data, improving detection accuracy over time, IDS-RNN model is fully capable of detecting intrusions in dynamic network environments. In RNN architecture hidden layers have a simple structure (e.g. single tanh layer), while the LSTM architecture is more complex, It is constituted of 4 hidden layers (Figure 8) [24] showing LTMS unit and RNN unit.

To add or remove information from the cell state, the gates are used to protect it, using sigmoid function (one means allows the modification, while a value of zero means denies the modification).

We can identify three different gates.

1) Input/Update gate layer (Figure 8): which controls how information enters the memory cell, is the key component of the LSTM. The computation of the input gate involves the current input x and the previous hidden state h_{t-1}:

$$\tilde{c}_t = \tanh(W_c x_t + U_c h_{t-1} + b_c), \qquad (24)$$

where W_c and U_c are weight matrices; b_c represents the bias parameter. The function, tanh denotes the hyperbolic tangent activation function.

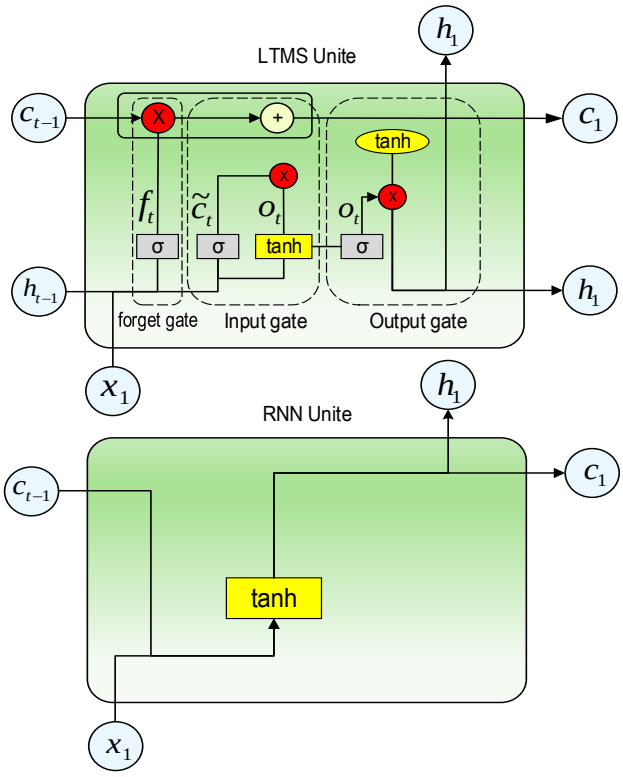


Fig. 8. LTMS Unit and RNN Unit

2) Forget gate layer (Figure 8): The forget gate is a crucial part that works in tandem with the input gate to filter out old data from the memory cell. This gate is controlled by the sigmoid activation function, and its

operation at time t is represented by the following equation:

$$f_t = \sigma\left(W_f x_t + U_f h_{t-1} + b_f\right). \quad (25)$$

3) Output gate Layer (Figure 8): The output gate serves as the last arbiter in the intrusion detection system (IDS) its decides what will be our output by executing a sigmoid function that decides which part of the cell LSTM is going to output, the result is passed through a tanh layer (value between – 1 and 1) to output only the information we decide to pass to the next neuron. The output gate helps the RNN-LSTM-based IDS to deliver actionable information to security analysts or supporting systems by selectively broadcasting pertinent signals, allowing prompt reactions to abnormalities and possible security breaches [25].

Mathematically, the output gate o_t at the time t is represented by the equation:

$$O_t = \sigma\left(W_o x_t + U_o h_{t-1} + \tilde{C}_t\right), \quad (26)$$

according to [24] the performance model of RNN, a series of experiments were conducted using varying hidden layer sizes. The highest accuracy was achieved with a hidden layer size of 100, and based on this, the hyperparameters were set for further model training. The model was implemented on an intrusion detection system (IDS) using the NSL-KDD dataset Figure 9 showing the classification performance of RNN was evaluated on the NSL-KDD dataset.

2.2. Unsupervised Learning

2.2.1. Deep Neural Network (DNN)

A Deep Neural Network (DNN) is a kind of neural network that has many layers which are set up in a feedforward topology [26]. It is made up of the input layer, several hidden layers, and the output layer. DNN operates in a unidirectional manner unlike recurrent neural networks, where data will move from the input nodes, through the hidden nodes to the output nodes, in the edge-weighted DAG without any loops or cycles. Each neuron in a layer is connected directly with the neurons in the subsequent layers. In the training process, the network's weights are adjusted through backpropagation method [27] Figure 10 illustrates the structure of a DNN.

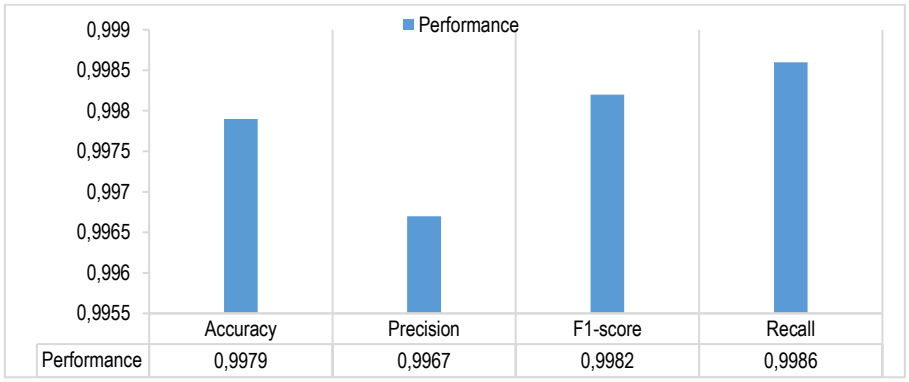


Fig. 9. RNN Evaluation Metrics Using NSL-KDD Dataset [24]

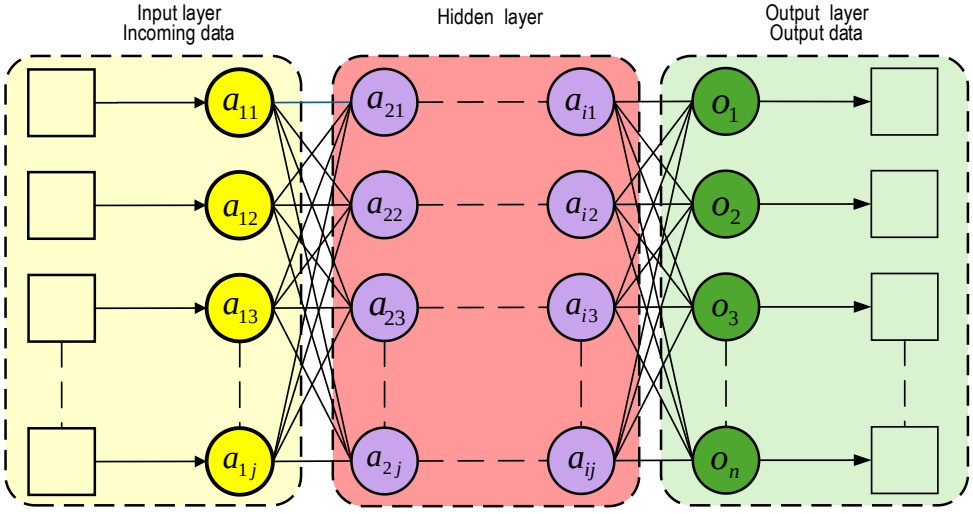


Fig. 10. The Structure of DNN

DNN famous for two main reasons [24, 27]:

1) they deliver a close to 100% accurate approximation of complex multidimensional and nonlinear functions built directly from the input data;

2) they are the foundation of the strong approximation theory which is adapted to a much wider list of natural and artificial occurring phenomena.

The training process of a DNN involves minimizing a cost function that measures the discrepancy between the network's predicted output and the actual output.

The cost function, denoted as $C(\vec{w}, \vec{x}, y)$ is typically defined as the mean squared error between the predicted output $h_w(\vec{x})$ and the true output y:

$$C(\vec{w}, \vec{x}, y) = \frac{1}{2}\|h_w(\vec{x}) - y\|^2, \quad (27)$$

where w represents the weights of the network $\vec{x}$ is the input vector to regularize the model and prevent overfitting, a regularization term is added to the cost function.

The regularized cost function $C(w\vec{x})$ is expressed as follows:

$$C(\vec{w}) = \frac{1}{N}C(\vec{w}; \vec{x}^n, y^n) + \frac{\lambda}{2}\sum_{K}^{k}\sum_{i}^{L_m}\sum_{j}^{L_{m+1}}\left(w_{ij}^k\right)^2, \quad (28)$$

where N represents the number of data points in the training set; λ is the regularization parameter; w_{ij}^k denotes the weights between the neurons in layers m and $m+1$ at the $k-th$ layer. During the training process, the weights of the network are updated iteratively using gradient descent.

The weight update rule is given by:

$$w_{ij}^k = w_{ij}^{k-1} + \xi\frac{\partial}{\partial w_{ij}^{k-1}}C(\vec{w}), \quad (29)$$

where ξ is the learning rate, and the update is based on the gradient of the cost function with respect to the weights, which guides the network towards minimizing the cost.

According to [28], the proposed model uses DNN to classify network traffic as either normal or attack. Due to the complexity of attack types, the model simplifies detection by grouping attacks into a binary classification. Evaluation metrics, including the ROC curve and confusion matrix shown in Figure 11, are used to assess performance on the NSL-KDD dataset. The DNN employs ReLU activation in hidden layers and Softmax activation in the output layer, ensuring efficient and accurate intrusion detection.

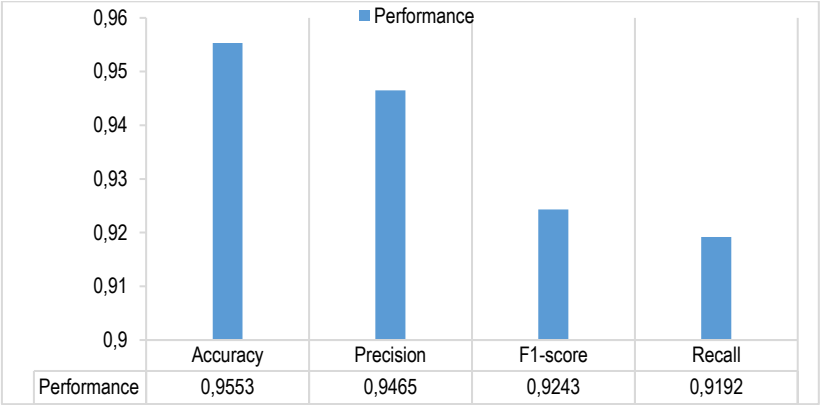


Fig. 11. DNN Evaluation Metrics Using NSL-KDD Dataset [28]

2.2.2 Convolutional Neural Networks (CNNs)

Convolutional Neural Networks (CNNs) are powerful systems that mimic the characteristics of the human visual system (HVS) and have led to significant breakthroughs in the field of computer vision [29, 30]. CNNs have become some of the most advanced algorithms in image recognition, object detection, and classification tasks, drawing inspiration from natural vision mechanisms. A typical CNN architecture, as shown in Figure 12, consists of multiple layers arranged in a sequence. These layers include convolutional layers, pooling layers, and fully connected layers.

The convolutional layers are the first to process the input data, where they apply a set of filters to extract fundamental features such as patterns and spatial relationships. These filters create feature maps that highlight important areas of the image, allowing the network to focus on key patterns [31].

The convolution operation itself is expressed as:

$$F(X, W) = Y, \quad (30)$$

where X is the input data; W represents the convolutional filter weights; Y is the output feature map. In a convolutional layer, the activation of a feature map at position (i, j) is calculated using the following formula:

$$a_{ij} = \sigma\left((W * X)_{ij} + b\right), \quad (31)$$

where $a_{ij}$is the activated value at position (i, j); σ is the activation function (such as ReLU), and b is the bias term.

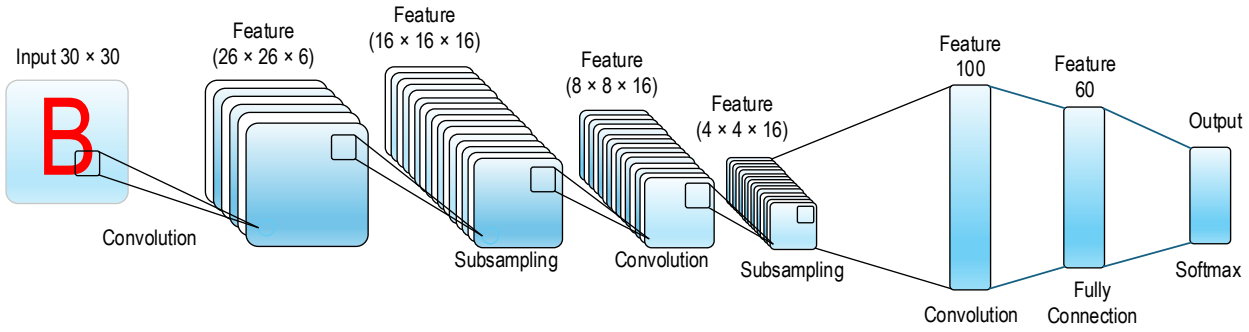


Fig. 12. CNN Architecture

The output of the convolution operation for a feature map C_q^l in layer l is computed by applying the filter $k_{p,q}^l$ to the input feature map S_p^{l-1} from the previous layer, along with a bias term b_q^l:

$$C_q^l = \left(\sum_{p=1}^{n} S_p^{l-1} * k_{p,q}^l + b_q^l\right). \quad (32)$$

To handle spatial shifts in the input data, this convolution operation can be extended as:

$$C_q^l = \left(\sum_{p=1}^{n}\sum_{u=-x}^{x}\sum_{v=-x}^{x} S_p^{l-1}(i-u, j-v) \times k_{p,q}^l(u,v) + b_q^l\right). \quad (33)$$

After applying the convolution operation, pooling layers are used to reduce the spatial dimensions of the feature maps. For example, the output $S_q^l(i,j)$ of a pooling layer can be computed as:

$$S_q^l(i,j) = \frac{1}{4}\sum_{u=0}^{z}\sum_{v=0}^{z} C_q^l(2i-u, 2j-v). \quad (34)$$

Once the convolutional and pooling layers have processed the input, the network typically uses fully connected layers for the final prediction. The output $\hat{y}(i)$ for each class is obtained using the softmax function, which normalizes the raw output scores:

$$\hat{y}(i) = \frac{e^{\widehat{output}}}{\sum_1^{labels} e^{\widehat{output}}}. \quad (35)$$

The objective during training is to minimize the loss function, which measures the difference between the predicted output $\hat{y}(i)$ and the true output $y(i)$.

The loss function is often represented as:

$$L = \frac{1}{2}\sum_{i=1}^{training\ patters}\left(\hat{y}(i) - y(i)\right)^2. \quad (36)$$

The weights of the network are updated using the gradient of the loss with respect to each weight:

$$\Delta W(i,j) = \frac{\partial L}{\partial W(i,j)} = \frac{\partial L}{\partial \hat{y}}.\frac{\partial \hat{y}}{\partial w(i,j)}. \quad (37)$$

Expanding the derivative:

$$\Delta W(i,j) = \left(\hat{y}(i) - y(i)\right).\frac{\partial L}{\partial W(i,j)} \times \times \left(\sigma\left(\sum_{j=1}^{nodes} W(i,j) * f(j) + b(i)\right)\right). \quad (38)$$

Additionally, the derivative of the output $\hat{y}(i)$ with respect to the loss is:

$$\Delta\hat{y}(i) = \left(\hat{y}(i) - y(i)\right).\hat{y}(i)\left(1 - \hat{y}(i)\right). \quad (39)$$

These gradients are used to update the weights through an optimization technique like stochastic gradient descent (SGD).

According to [32] the experimental results on the NSL-KDD dataset showing in Figure 13.

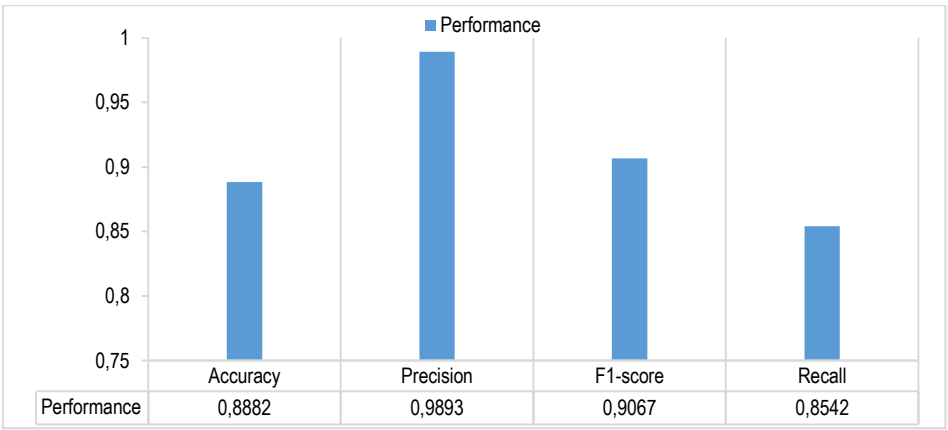


Fig. 13. CNN Evaluation Metrics Using NSL-KDD Dataset [32]

2.3. Sim-Supervised Learning

2.3.1. Generative Adversarial Networks (GANs)

Generative Adversarial Networks (GANs) have gained significant attention in various application domains, with anomaly detection being one of the most prominent [33]. The ability of GANs to learn complex representations and generate data that appears realistic makes them highly effective for anomaly detection tasks. These networks are trained using a data distribution approach in an unsupervised manner, allowing them to detect irregularities without requiring labeled datasets [33], Figure 14 showing GANs architecture.

Mathematically, the operation of GANs can be described using the divergence function:

$$D_f\left(P_{data}\|P_g\right) = \int_x P_g(x) f\left(\frac{P_{data}(x)}{P_g(x)}\right) dx, \qquad (40)$$

where $f(1) = 0$ indicates that P_g and P_{data} are equivalent. In the origin of GAN, the Jensen-Shannon JS divergence was adopted as f:

$$f(t) = t\log(t) - (t+1)\log(t+1). \qquad (41)$$

This function measures the discrepancy between the real data distribution P_{data} and the generator's distribution P_g quantifying how closely the generated data approximates the real data [34].

Another crucial metric in GANs is the Jensen-Shannon Divergence JS defined as:

$$JS\left(P_{data}\|P_g\right) = \frac{1}{2}KL(P_{data}\|P_m) + \frac{1}{2}(P_s\|P_m), \qquad (42)$$

where:

$$P_m = \frac{1}{2}\left(P_{data}\|P_g\right). \qquad (43)$$

The JS divergence evaluates the similarity between P_{data} and P_g with lower values indicating a better match. This property makes GANs particularly well-suited for distinguishing anomalies, as deviations from the expected distribution can be easily detected.

The core of GAN functionality lies in the minimax optimization framework (44), where $D(x)$ is the discriminator function (45), which assigns a higher probability to real samples. The generator seeks to minimize the term $\log\left(1 - D\left(G(z)\right)\right)$ improving its ability to produce realistic data. Further refinement involves the optimization objectives for the discriminator (46) and generator (47).

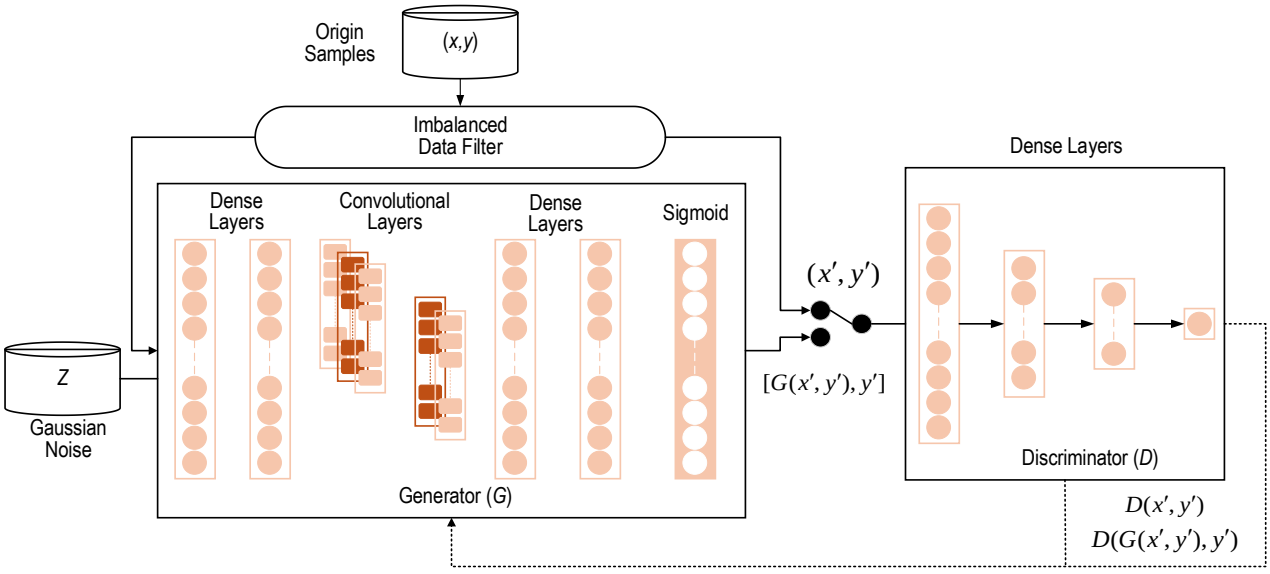


Fig. 14. GANs Architecture

$$\min_G \max_D V(D,G) = \min_G \max_D \begin{pmatrix} \mathbb{E}_{x\sim P_{data(x)}}[\log D(x)] \\ +\mathbb{E}_{z\sim P_{data(z)}} \\ \left[\log\left(1 - D\left(G(z)\right)\right)\right] \end{pmatrix}. \qquad (44)$$

$$D(x) = \frac{P_{data}(x)}{P_{data}(x) + P_g(x)}. \qquad (45)$$

$$\max_{\theta_D} \hat{V}(D) = \max_{\theta_D} \frac{1}{m}\sum_{i=1}^{m} \begin{pmatrix} \log D(\acute{x}_i, \acute{y}_i) + \\ \log\left(1 - D(G(z_i, \acute{y}_i)\acute{y}_i)\right) \end{pmatrix}. \qquad (46)$$

$$\min_{\theta_G} \hat{V}(D) = \max_{\theta_G} \frac{1}{m} \sum_{i=1}^{m} \left(\log\left(1 - D(G(z_i, \acute{y}_i)\acute{y}_i)\right)\right). \quad (47)$$

The probabilistic classification in GANs can be modeled as:

$$P(y|a) = P(y = C_\tau|v) = \frac{e^{v_\tau}}{\sum_{v_{\tau\in v}} e^{v_\tau}}, \quad (48)$$

where the probability of a sample belonging to a particular class is determined by the class scores. These mathematical foundations enable GANs to perform effectively in anomaly detection, making them invaluable for applications like fraud detection, network intrusion detection, and industrial fault diagnosis. According to [33] showing the evaluation of the metrics GAN using NSL-KDD (Figure 15).

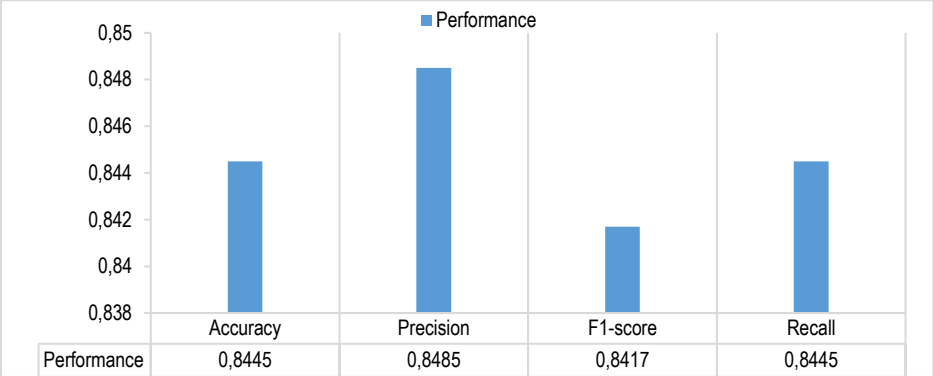


Fig. 15. GAN Evaluation Metrics Using NSL-KDD Dataset [33]

3. RESULTS AND DISCUSSIONS

In order to evaluate the deep learning models discussed, this study utilized the NSL-KDD dataset, which comprises 41 features and 125,973 instances categorized into normal and four attack types: DoS, Probe, R2L, and U2R. Various deep learning models – Autoencoders, Restricted Boltzmann Machines (RBMs), Deep Belief Networks (DBNs), Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Deep Neural Networks (DNNs), and Generative Adversarial Networks (GANs – were implemented and tested to assess their effectiveness in intrusion detection. The results showed varying performance across the models based on evaluation metrics, as seeing in Figures (3, 5, 7, 9, 11, 13, 15).

Among the tested models, RNNs achieved the highest accuracy (99.79 %), precision (99.67 %), and recall (99.86 %), demonstrating their effectiveness in detecting temporal patterns in network traffic. Autoencoders and RBMs also performed well, with accuracy metrics of 99.4 %. However, DBNs exhibited lower accuracy (80.82 %) and recall (68.53 %), suggesting limitations in handling complex datasets. CNNs and GANs showed promising results but lagged behind RNNs in overall performance metrics. DNNs provided a balanced performance, achieving high accuracy (95.53 %) and precision (94.65 %).Figures illustrating these results emphasize the superiority of RNNs and the suitability of Autoencoders and RBMs for intrusion detection tasks. The findings also align with prior studies, underscoring the importance of selecting appropriate models based on the specific requirements of IDS applications and the characteristics of available datasets.

4 CONCLUSIONS

The findings of this study emphasize the transformative impact of deep learning on intrusion detection systems. By leveraging advanced neural network architectures, IDS can achieve superior performance in detecting and responding to cyber threats. Models like autoencoders and RBMs enable efficient anomaly detection through automatic feature learning, while DBNs, RNNs, and CNNs provide enhanced capabilities for processing temporal and spatial data patterns. The integration of these models has demonstrated significant improvements in accuracy, precision, and recall metrics, as evidenced by evaluations on the NSL-KDD dataset. While computational complexity remains a challenge, recent advancements in hardware technologies, such as GPUs and AI accelerators, have made it feasible to implement deep learning-based IDS in resource-constrained environments. Future research should focus on improving model scalability, reducing computational demands, and adapting to the ever-changing landscape of network security threats. These advancements will be crucial for developing IDS that are both effective and practical across diverse applications.

Список источников

1. Navya V.K., Adithi J., Rudrawal D., Tailor H., James N. Intrusion Detection System Using Deep Neural Networks (DNN) // Proceedings of the International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA, Coimbatore, India, 08–09 October 2021). IEEE, 2022. DOI:10.1109/ICAECA52838.2021.9675513

2. Vinayakumar R., Soman K.P. Poornachandran P. Applying convolutional neural network for network intrusion detection // Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI, Udupi, India, 13–16 September 2017). IEEE, 2017. PP. 1222–1228. DOI:10.1109/ICACCI.2017.8126009

3. Wu Y., Lee W.W., Xu Z., Ni M. Large-scale and robust intrusion detection model combining improved deep belief network with feature-weighted SVM // IEEE Access. 2020. Vol. 8. PP. 98600–98611. DOI:10.1109/ACCESS.2020.2994947. EDN:APJZGY

4. Alpaydin E. Introduction to Machine Learning. MIT Press, 2020.

5. Aldwairi T., Perera D., Novotny M.A. An evaluation of the performance of Restricted Boltzmann Machines as a model for anomaly network intrusion detection // Computer Networks. 2018. Vol. 144. PP. 111–119. DOI:10.1016/j.comnet.2018.07.025

6. Choi H., Kim M., Lee G., Kim W. Unsupervised learning approach for network intrusion detection system using autoencoders // The Journal of Supercomputing. 2019. Vol. 75. Iss. 9. PP. 5597–5621. DOI:10.1007/s11227-019-02805-w. EDN:RJBUQU

7. Shahriar M.H., Haque N.I., Rahman M.A., Alonso M. G-ids: Generative adversarial networks assisted intrusion detection system // Proceedings of the 44th Annual Computers, Software, and Applications Conference (COMPSAC, Virtual, Madrid, 13–17 July 2020). IEEE, 2020. PP. 376–385. DOI:10.1109/COMPSAC48688.2020.0-218. EDN:DJVEFI

8. Al-Qatf M., Lasheng Y., Al-Habib M., Al-Sabahi K. Deep Learning Approach Combining Sparse Autoencoder With SVM for Network Intrusion Detection // IEEE Access. 2018. Vol. 6. PP. 52843–52856. DOI:10.1109/ACCESS.2018.2869577

9. Shone N., Ngoc T.N., Phai V.D., Shi Q. A Deep Learning Approach to Network Intrusion Detection // IEEE Transactions on Emerging Topics in Computational Intelligence. 2018. Vol. 2. Iss. 1. PP. 41–50. DOI:10.1109/TETCI.2017.2772792

10. Li Z., Qin Z., Huang K., Yang X., Ye S. Intrusion Detection Using Convolutional Neural Networks for Representation Learning // Proceedings of the 24th International Conference on Neural Information Processing (ICONIP, Guangzhou, China, 14–18 November 2017). Lecture Notes in Computer Science. Cham: Springer, 2017. Vol. 10638. PP. 858–866. DOI:10.1007/978-3-319-70139-4_87

11. Wang S., Wang J., Lu H., Zhao W. A novel combined model for wind speed prediction–Combination of linear model, shallow neural networks, and deep learning approaches // Energy. 2021. Vol. 234. P.121275. DOI:10.1016/j.energy.2021.121275. EDN:FAJRCK

12. Javaid A., Niyaz Q., Sun W., Alam M. A Deep Learning Approach for Network Intrusion Detection System // Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS, New York, USA, 3–5 December 2015). 2016. PP. 21–26. DOI:10.4108/eai.3-12-2015.2262516

13. Manimaran A., Chandramohan D., Shrinivas S.G., Arulkumar N. A comprehensive novel model for network speech anomaly detection system using deep learning approach // International Journal of Speech Technology. 2020. Vol. 23. Iss. 2. PP. 305–313. DOI:10.1007/s10772-020-09693-z. EDN:URAWUT

14. Alrayes F.S., Zakariah M., Amin S.U., Khan Z.I., Helal M. Intrusion Detection in IoT Systems Using Denoising Autoencoder // IEEE Access. 2024. Vol. 12. PP. 122401–122425. DOI:10.1109/ACCESS.2024.3451726. EDN:VCPDLT

15. Vincent P., Larochelle H., Bengio Y., Manzagol P.A. Extracting and composing robust features with denoising autoencoders // Proceedings of the 25th International Conference on Machine Learning (Helsinki, Finland, 5–9 July 2008). Association for Computing Machinery, 2008. PP. 1096–1103. DOI:10.1145/1390156.1390294

16. Vincent P., Larochelle H., Lajoie I., Bengio Y., Manzagol P.A., Bottou L. Stacked Denoising Autoencoders: Learning Useful Representations in a Deep Network with a Local Denoising Criterion // Journal of Machine Learning Research. 2010. Vol. 11. PP. 3371–3408. EDN:OCLKDJ

17. Zhang N., Ding S., Zhang J., Xue Y. An overview on restricted Boltzmann machines // Neurocomputing. 2018. Vol. 275. PP. 1186–1199. DOI:10.1016/j.neucom.2017.09.065

18. Mayuranathan M., Murugan M., Dhanakoti V. Retracted article: best features based intrusion detection system by RBM model for detecting DDoS in cloud environment // Journal of Ambient Intelligence and Humanized Computing. 2021. Vol. 12. Iss. 3. PP. 3609–3619. DOI:10.1007/s12652-019-01611-9. EDN:LAAOLK

19. Seo S., Park S., Kim J. Improvement of Network Intrusion Detection Accuracy by Using Restricted Boltzmann Machine // Proceedings of the 8th International Conference on Computational Intelligence and Communication Networks (CICN, Tehri, India, 23–25 December 2016). IEEE, 2016. PP. 413–417. DOI:10.1109/CICN.2016.87

20. Balakrishnan N., Rajendran A., Pelusi D., Ponnusamy V. Deep Belief Network Enhanced Intrusion Detection System to Prevent Security Breach in the Internet of Things // Internet of Things. 2021. Vol. 14. P. 100112. DOI:10.1016/j.iot.2019.100112. EDN:CZRBGW

21. Yang Y., Zheng K., Wu C., Niu X., Yang Y. Building an effective intrusion detection system using the modified density peak clustering algorithm and deep belief networks // Applied Sciences. 2019. Vol. 9. Iss. 2. P. 238. DOI:10.3390/app9020238. EDN:ABGPER

22. Parhizkari S. Anomaly Detection in Intrusion Detection Systems. 2023. DOI:10.5772/intechopen.112733

23. Mehibs S.M., Hashim S.H. Proposed Network Intrusion Detection System in Cloud Environment Based on Back Propagation Neural Network // Journal of University of Babylon for Pure and Applied Sciences. 2018. Vol. 26. Iss. 1. PP. 29–40. DOI:10.29196/jub. v26i1.351

24. Al-Tameemi M.M.A., Alzaghir A.A.H. Improving Network Security Through Deep Learning RNN Approach // Computational Nanotechnology. 2024. Vol. 11. Iss. 4. PP. 114–121. DOI:10.33693/2313-223X-2024-11-4-114-121. EDN:GPCZUD

25. Smagulova K., James A.P. A survey on LSTM memristive neural network architectures and applications // The European Physical Journal Special Topics. 2019. Vol. 228. Iss. 10. PP. 2313–2324. DOI:10.1140/epjst/e2019-900046-x. EDN:HRKIKB

26. Han K., Yu D., Tashev I. Speech emotion recognition using deep neural network and extreme learning machine // Interspeech 2014. DOI:10.21437/Interspeech.2014-57

27. Roy S.S., Mallik A., Gulati R., Obaidat M.S., Krishna P.V. A deep learning based artificial neural network approach for intrusion detection // Proceedings of the Third International Conference on Mathematics and Computing (ICMC 2017, Haldia, India, 17–21 January 2017). Communications in Computer and Information Science. Singapore: Springer, 2017. Vol. 655. PP. 44–53. DOI:10.1007/978-981-10-4642-1_5

28. Gowdhaman V., Dhanapal R. An intrusion detection system for wireless sensor networks using deep neural network // Soft Computing. 2022. Vol. 26. Iss. 23. PP. 13059–13067. DOI:10.1007/s00500-021-06473-y. EDN:KHFOPY

29. Yang Y., Zheng K., Wu C., Niu X., Yang Y. Building an Effective Intrusion Detection System Using the Modified Density Peak Clustering Algorithm and Deep Belief Networks // Applied Sciences. 2019. Vol. 9. Iss. 2. P. 238. DOI:10.3390/app9020238. EDN:ABGPER

30. Mohammadpour L., Ling T.Ch., Liew Ch.S., Aryanfar A. A Survey of CNN-Based Network Intrusion Detection // Applied Sciences. 2022. Vol. 12. Iss. 16. P. 8162. DOI:10.3390/app12168162. EDN:EFJJTR

31. Razavian A.S., Azizpour H., Sullivan J., Carlsson S. CNN features off-the-Shelf: An Astounding Baseline for Recognition // arXiv. 2014. DOI:10.48550/arXiv.1403.6382

32. Jo W., Kim S., Lee C., Shon T. Packet preprocessing in CNN-based network intrusion detection system // Electronics. 2020. Vol. 9. Iss. 7. P. 1151. DOI:10.3390/electronics9071151. EDN:XVUGFM

33. Sabuhi M., Zhou M., Bezemer C.P., Musilek P. Applications of Generative Adversarial Networks in Anomaly Detection: A Systematic Literature Review // IEEE Access. 2021. Vol. 9. PP. 161003–161029. DOI:10.1109/ACCESS.2021.3131949. EDN:TJDTSD

34. Dunmore A., Jang-Jaccard J., Sabrina F., Kwak J. A Comprehensive Survey of Generative Adversarial Networks (GANs) in Cybersecurity Intrusion Detection // IEEE Access. 2023. Vol. 11. PP. 76071–76094. DOI:10.1109/ACCESS.2023.3296707. EDN:NOKCVG

References

1. Navya V.K., Adithi J., Rudrawal D., Tailor H., James N. Intrusion Detection System Using Deep Neural Networks (DNN). *Proceedings of the International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation, ICAECA, 08–09 October 2021, Coimbatore, India*. IEEE; 2022. DOI:10.1109/ICAECA52838.2021.9675513

2. Vinayakumar R., Soman K.P. Poornachandran P. Applying convolutional neural network for network intrusion detection. *Proceedings of the International Conference on Advances in Computing, Communications and Informatics, ICACCI, 13–16 September 2017, Udupi, India*. IEEE; 2017. p.1222–1228. DOI:10.1109/ICACCI.2017.8126009

3. Wu Y., Lee W.W., Xu Z., Ni M. Large-scale and robust intrusion detection model combining improved deep belief network with feature-weighted SVM. *IEEE Access*. 2020;8:98600–98611. DOI:10.1109/ACCESS.2020.2994947. EDN:APJZGY

4. Alpaydin E. *Introduction to Machine Learning*. MIT Press; 2020.

5. Aldwairi T., Perera D., Novotny M.A. An evaluation of the performance of Restricted Boltzmann Machines as a model for anomaly network intrusion detection. *Computer Networks*. 2018;144:111–119. DOI:10.1016/j.comnet.2018.07.025

6. Choi H., Kim M., Lee G., Kim W. Unsupervised learning approach for network intrusion detection system using autoencoders. *The Journal of Supercomputing*. 2019;75(9):5597–5621. DOI:10.1007/s11227-019-02805-w. EDN:RJBUQU

7. Shahriar M.H., Haque N.I., Rahman M.A., Alonso M. G-ids: Generative adversarial networks assisted intrusion detection system. *Proceedings of the 44th Annual Computers, Software, and Applications Conference, COMPSAC, 13–17 July 2020, Virtual, Madrid*. IEEE; 2020. p.376–385. DOI:10.1109/COMPSAC48688.2020.0-218. EDN:DJVEFI

8. Al-Qatf M., Lasheng Y., Al-Habib M., Al-Sabahi K. Deep Learning Approach Combining Sparse Autoencoder With SVM for Network Intrusion Detection. *IEEE Access*. 2018;6:52843–52856. DOI:10.1109/ACCESS.2018.2869577

9. Shone N., Ngoc T.N., Phai V.D., Shi Q. A Deep Learning Approach to Network Intrusion Detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*. 2018;2(1):41–50. DOI:10.1109/TETCI.2017.2772792

10. Li Z., Qin Z., Huang K., Yang X., Ye S. Intrusion Detection Using Convolutional Neural Networks for Representation Learning. *Proceedings of the 24th International Conference on Neural Information Processing, ICONIP, 14–18 November 2017, Guangzhou, China. Lecture Notes in Computer Science, vol.10638*. Cham: Springer; 2017. p.858–866. DOI:10.1007/978-3-319-70139-4_87

11. Wang S., Wang J., Lu H., Zhao W. A novel combined model for wind speed prediction–Combination of linear model, shallow neural networks, and deep learning approaches. *Energy*. 2021;234:121275. DOI:10.1016/j.energy.2021.121275. EDN:FAJRCK

12. Javaid A., Niyaz Q., Sun W., Alam M. A Deep Learning Approach for Network Intrusion Detection System. *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies, formerly BIONETICS, 3–5 December 2015, New York, USA*. 2016. p.21–26. DOI:10.4108/eai.3-12-2015.2262516

13. Manimaran A., Chandramohan D., Shrinivas S.G., Arulkumar N. A comprehensive novel model for network speech anomaly detection system using deep learning approach. *International Journal of Speech Technology*. 2020;23(2):305–313. DOI:10.1007/s10772-020-09693-z. EDN:URAWUT

14. Alrayes F.S., Zakariah M., Amin S.U., Khan Z.I., Helal M. Intrusion Detection in IoT Systems Using Denoising Autoencoder. *IEEE Access*. 2024;12:122401–122425. DOI:10.1109/ACCESS.2024.3451726. EDN:VCPDLT

15. Vincent P., Larochelle H., Bengio Y., Manzagol P.A. Extracting and composing robust features with denoising autoencoders. *Proceedings of the 25th International Conference on Machine Learning, 5–9 July 2008, Helsinki, Finland*. Association for Computing Machinery; 2008. p.1096–1103. DOI:10.1145/1390156.1390294

16. Vincent P., Larochelle H., Lajoie I., Bengio Y., Manzagol P.A., Bottou L. Stacked Denoising Autoencoders: Learning Useful Representations in a Deep Network with a Local Denoising Criterion. *Journal of Machine Learning Research*. 2010;11:3371–3408. EDN:OCLKDJ

17. Zhang N., Ding S., Zhang J., Xue Y. An overview on restricted Boltzmann machines. *Neurocomputing*. 2018;275:1186–1199. DOI:10.1016/j.neucom.2017.09.065

18. Mayuranathan M., Murugan M., Dhanakoti V. Retracted article: best features based intrusion detection system by RBM model for detecting DDoS in cloud environment. *Journal of Ambient Intelligence and Humanized Computing*. 2021;12(3):3609–3619. DOI:10.1007/s12652-019-01611-9. EDN:LAAOLK

19. Seo S., Park S., Kim J. Improvement of Network Intrusion Detection Accuracy by Using Restricted Boltzmann Machine. *Proceedings of the 8th International Conference on Computational Intelligence and Communication Networks, CICN, 23–25 December 2016, Tehri, India*. IEEE; 2016. p.413–417. DOI:10.1109/CICN.2016.87

20. Balakrishnan N., Rajendran A., Pelusi D., Ponnusamy V. Deep Belief Network Enhanced Intrusion Detection System to Prevent Security Breach in the Internet of Things. *Internet of Things*. 2021;14:100112. DOI:10.1016/j.iot.2019.100112. EDN:CZRBGW

21. Yang Y., Zheng K., Wu C., Niu X., Yang Y. Building an Effective Intrusion Detection System Using the Modified Density Peak Clustering Algorithm and Deep Belief Networks. *Applied Sciences*. 2019. Vol. 9. Iss. 2. P. 238. DOI:10.3390/app9020238. EDN:ABGPER

22. Parhizkari S. *Anomaly Detection in Intrusion Detection Systems*. 2023. DOI:10.5772/intechopen.112733

23. Mehibs S.M., Hashim S.H. Proposed Network Intrusion Detection System in Cloud Environment Based on Back Propagation Neural Network. *Journal of University of Babylon for Pure and Applied Sciences*. 2018;26(1):29–40. DOI:10.29196/jub.v26i1.351

24. Al-Tameemi M.M.A., Alzaghir A.A.H. Improving Network Security Through Deep Learning RNN Approach. *Computational Nanotechnology*. 2024;11(4):114–121. DOI:10.33693/2313-223X-2024-11-4-114-121. EDN:GPCZUD

25. Smagulova K., James A.P. A survey on LSTM memristive neural network architectures and applications. *The European Physical Journal Special Topics*. 2019;228(10):2313–2324. DOI:10.1140/epjst/e2019-900046-x. EDN:HRKIKB

26. Han K., Yu D., Tashev I. Speech emotion recognition using deep neural network and extreme learning machine. *Interspeech 2014*. DOI:10.21437/Interspeech.2014-57

27. Roy S.S., Mallik A., Gulati R., Obaidat M.S., Krishna P.V. A deep learning based artificial neural network approach for intrusion detection. *Proceedings of the Third International Conference on Mathematics and Computing, ICMC 2017, 17–21 January 2017, Haldia, India. Communications in Computer and Information Science, vol.655*. Singapore: Springer; 2017. p.44–53. DOI:10.1007/978-981-10-4642-1_5

28. Gowdhaman V., Dhanapal R. An intrusion detection system for wireless sensor networks using deep neural network. *Soft Computing*. 2022;26(23):13059–13067. DOI:10.1007/s00500-021-06473-y. EDN:KHFOPY

29. Yang Y., Zheng K., Wu C., Niu X., Yang Y. Building an Effective Intrusion Detection System Using the Modified Density Peak Clustering Algorithm and Deep Belief Networks. *Applied Sciences*. 2019:9(2):238. DOI:10.3390/app9020238. EDN:ABGPER

30. Mohammadpour L., Ling T.Ch., Liew Ch.S., Aryanfar A. A Survey of CNN-Based Network Intrusion Detection. *Applied Sciences*. 2022;12(16):8162. DOI:10.3390/app12168162. EDN:EFJJTR

31. Razavian A.S., Azizpour H., Sullivan J., Carlsson S. CNN features off-the-Shelf: An Astounding Baseline for Recognition. *arXiv*. 2014. DOI:10.48550/arXiv.1403.6382

32. Jo W., Kim S., Lee C., Shon T. Packet preprocessing in CNN-based network intrusion detection system. *Electronics*. 2020; 9(7):1151. DOI:10.3390/electronics9071151. EDN:XVUGFM

33. Sabuhi M., Zhou M., Bezemer C.P., Musilek P. Applications of Generative Adversarial Networks in Anomaly Detection: A Systematic Literature Review. *IEEE Access*. 2021;9:161003–161029. DOI:10.1109/ACCESS.2021.3131949. EDN:TJDTSD

34. Dunmore A., Jang-Jaccard J., Sabrina F., Kwak J. A Comprehensive Survey of Generative Adversarial Networks (GANs) in Cybersecurity Intrusion Detection. *IEEE Access*. 2023;11:76071–76094. DOI:10.1109/ACCESS.2023.3296707. EDN:NOKCVG

Статья поступила в редакцию 24.01.2025; одобрена после рецензирования 10.05.2025; принята к публикации 02.06.2025.
The article was submitted 24.01.2025; approved after reviewing 10.05.2025; accepted for publication 02.06.2025.

Информация об авторах:

АЛЬ-ТАМИМИ Мохалад Мохсин Абдульхасан — аспирант кафедры информационной безопасности Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина)
https://orcid.org/0009-0005-5316-1689

АЛЗАГИР Аббас Али Хасан — кандидат технических наук, доцент кафедры «Сети и системы фиксированной связи» Московского технического университета связи и информатики
https://orcid.org/0000-0003-2937-9934

АЛЬ-СВЕЙТИ Малик А.М. — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
https://orcid.org/0000-0002-6267-4727

Авторы сообщают об отсутствии конфликтов интересов.

The authors declare no conflicts of interests.

Научная статья
УДК 004.85
https://doi.org/10.31854/1813-324X-2025-11-3-87-96
EDN:EDKHNU

Применение адаптивной нейро-нечеткой системы вывода для обнаружения DDoS-атак на основе набора данных CIC-DDoS-2019

Николай Николаевич Васин[1], vasin-nn@psuti.ru
Карен Сергеевич Какабьян[2] ✉, and4r1lh0@yandex.ru

[1]Поволжский государственный университет телекоммуникаций и информатики,
Самара, 443010, Российская Федерация
[2]ООО «Яндекс Облако»,
Москва, 119021, Российская Федерация

Аннотация

Актуальность. *Распределенные атаки типа «отказ в обслуживании» (DDoS) остаются значительной угрозой для доступности онлайн-сервисов. Традиционные системы обнаружения вторжений, основанные на сигнатурах или анализе аномалий, сталкиваются с ограничениями при обнаружении новых и сложных атак, в то время как подходы на основе машинного обучения, демонстрируя высокий потенциал, часто лишены интерпретируемости. Гибридные системы, такие как адаптивная нейро-нечеткая система вывода (ANFIS), объединяют преимущества нейронных сетей и нечеткой логики, предлагая как точность, так и возможность интерпретации. Однако их эффективность применительно к современным наборам данных с разнообразными векторами атак, таким как CIC-DDoS-2019, требует изучения.*

Цель. *Исследование направлено на оценку эффективности и применимости системы ANFIS для задачи обнаружения DDoS-атак с использованием актуального и сложного набора данных CIC-DDoS-2019. В работе* ***использовалась*** *модель ANFIS. Исследование проводилось на репрезентативной подвыборке из набора данных CIC-DDoS-2019. Методология включала тщательную предварительную обработку данных, отбор наиболее релевантных признаков и экспертных знаний, нормализацию признаков. Модель ANFIS с гауссовыми функциями принадлежности обучалась с использованием гибридного алгоритма оптимизации (градиентный спуск и метод наименьших квадратов) на 80 % данных. Эффективность оценивалась на оставшихся 20 % тестовых данных с использованием стандартных метрик классификации: Accuracy, Precision, Recall, F1-Score, а также анализа матрицы ошибок.*

Результаты. *Эксперименты показали высокую производительность модели ANFIS. Были достигнуты следующие показатели: доля правильно классифицированных объектов (Accuracy) – 97,82 %, точность (Precision) – 99,52 %, полнота (Recall) – 85,95 % и F1-мера – 92,24 %. Результаты указывают на очень низкий уровень ложных срабатываний, при некотором количестве пропущенных атак.*

Научная новизна. *Работа демонстрирует применение и оценку эффективности ANFIS на современном и сложном наборе данных CIC-DDoS-2019, содержащем актуальные типы атак. Исследование подтверждает* ***теоретическую применимость*** *гибридных нейро-нечетких моделей для решения актуальных задач кибербезопасности.* ***Практическая значимость*** *состоит в демонстрации того, что ANFIS может служить основой для разработки эффективных систем обнаружения DDoS-атак, обеспечивая высокий уровень точности и приемлемую полноту обнаружения. Возможность анализа функций принадлежности и правил реализует интерпретируемость, что важно для понимания работы системы и анализа угроз. Результаты предоставляют эталонные показатели для ANFIS на данном наборе данных.*

Ключевые слова: *DDoS-атаки, обнаружение вторжений, нейро-нечеткие системы, ANFIS, машинное обучение, анализ сетевого трафика*

Ссылка для цитирования: Васин Н.Н., Какабьян К.С. Применение адаптивной нейро-нечеткой системы вывода для обнаружения DDoS-атак на основе набора данных CIC-DDoS-2019 // Труды учебных заведений связи. 2025. Т. 11. № 3. С. 87–96. (in Russ.) DOI:10.31854/1813-324X-2025-11-3-87-96. EDN:EDKHNU

Original research
https://doi.org/10.31854/1813-324X-2025-11-3-87-96
EDN:EDKHNU

Application of Adaptive Neuro-Fuzzy Inference System for DDoS Attack Detection Based on CIC-DDoS-2019 Dataset

Nikolay N. Vasin[1], vasin-nn@psuti.ru
Karen S. Kakabian[2] ✉, and4r1lh0@yandex.ru

[1]Povolzhskiy State University of Telecommunications and Informatics,
Samara, 443010, Russian Federation
[2]Yandex Cloud, LLC,
Moscow, 119021, Russian Federation

Annotation

The relevance. *Distributed Denial of Service (DDoS) attacks remain a significant threat to the availability of online services. Traditional intrusion detection systems based on signatures or anomaly analysis face limitations in detecting new and complex attacks, while machine learning-based approaches, while showing high potential, often lack interpretability. Hybrid systems, such as the Adaptive Neuro-Fuzzy Inference System (ANFIS), combine the advantages of neural networks and fuzzy logic, offering both accuracy and interpretability. However, their effectiveness with respect to modern datasets with diverse attack vectors, such as CIC-DDoS-2019, needs to be investigated.*

Objective. *The study aims to evaluate the performance and applicability of ANFIS for the task of DDoS attack detection using the current and challenging CIC-DDoS-2019 dataset. The ANFIS model was* ***used*** *in this work. The study was conducted on a representative subsample of the CIC-DDoS-2019 dataset. The methodology included careful data preprocessing, selection of the most relevant features and expert knowledge, and feature normalisation. The ANFIS model with Gaussian membership functions was trained using a hybrid optimisation algorithm (gradient descent and least squares method) on 80 % of the data. Performance was evaluated on the remaining 20 % of the test data using standard classification metrics: Accuracy, Precision, Recall, F1-Score, and error matrix analysis.*

Results. *The experiments showed high performance of the ANFIS model. The following metrics were achieved: proportion of correctly classified objects (Accuracy) – 97.82 %, accuracy (Precision) – 99.52 %, completeness (Recall) – 85.95 % and F1-measure – 92.24 %. The results indicate a very low false positive rate, with some number of missed attacks.*

Novelty. *The work demonstrates the application and performance evaluation of ANFIS on a modern and complex CIC-DDoS-2019 dataset containing relevant attack types.*
The study confirms the theoretical applicability of hybrid neuro-fuzzy models to solve current cybersecurity problems.

The practical significance *consists in demonstrating that ANFIS can serve as a basis for the development of effective DDoS attack detection systems, providing a high level of accuracy and acceptable detection completeness. The ability to analyze membership functions and rules implements interpretability, which is important for understanding system performance and threat analysis. The results provide benchmarks for ANFIS on this dataset.*

Keywords: *DDoS attacks, intrusion detection, neuro-fuzzy systems, ANFIS, machine learning, network traffic analysis*

For citation: Vasin N.N., Kakabian K.S. Application of Adaptive Neuro-Fuzzy Inference System for DDoS Attack Detection Based on CIC-DDoS-2019 Dataset. *Proceedings of Telecommunication Universities.* 2025;11(3):87–96. DOI:10.31854/1813-324X-2025-11-3-87-96. EDN:EDKHNU

Введение

Повсеместное распространение интернет-сервисов сделало их доступность критически важным фактором для современной экономики и общества. Распределенные атаки типа «отказ в обслуживании» (DDoS, *аббр. от англ.* Distributed Denial of Service) направлены на нарушение этой доступности путем перегрузки целевых систем или сетевых

каналов огромным потоком вредоносного трафика, генерируемого с множества скомпрометированных устройств [1]. Последствия успешных DDoS-атак варьируются от временной недоступности сервисов до значительных финансовых и репутационных потерь.

Масштабы DDoS-атак постоянно растут. Злоумышленники используют все более сложные методы, включая атаки на уровне приложений, атаки с амплификацией и отражением, а также атаки, имитирующие легитимный трафик, что значительно усложняет их обнаружение традиционными методами [2]. Классические подходы, такие как системы обнаружения вторжений на основе сигнатур, эффективны против известных атак, но уязвимы перед новыми или модифицированными вариантами. Системы обнаружения вторжений, основанные на обнаружении аномалий, способны выявлять ранее неизвестные атаки, но зачастую подвержены высокому уровню ложных срабатываний [3].

В последние годы методы машинного обучения (ML, *аббр. от англ.* Machine Learning) продемонстрировали большой потенциал в области обнаружения DDoS-атак [4, 5]. Эти подходы позволяют автоматически извлекать сложные закономерности из сетевого трафика и строить модели для классификации потоков на легитимные и вредоносные. Однако многие модели ML функционируют как «черные ящики», что затрудняет интерпретацию их решений и настройку.

В этом контексте перспективным направлением является использование гибридных интеллектуальных систем, объединяющих сильные стороны различных подходов. Нейро-нечеткие системы, в частности адаптивные нейро-нечеткие системы вывода (ANFIS, *аббр. от англ.* Adaptive Neuro-Fuzzy Inference System) [6], представляют собой такой гибридный подход. ANFIS интегрирует способность нейронных сетей к обучению на данных со способностью систем нечеткой логики оперировать неточными, неопределенными данными и представлять знания в виде интерпретируемых правил. Это позволяет создавать системы обнаружения DDoS, которые не только точны, но и потенциально более прозрачны и устойчивы к зашумленным данным.

Целью данной работы является оценка эффективности применения ANFIS для обнаружения DDoS-атак на основе набора данных CIC-DDoS-2019 [7]. Набор данных CIC-DDoS-2019 содержит большой объем трафика (более 430 000 сетевых пакетов), включая как нормальную активность, так и широкий спектр новейших DDoS-атак (DNS, LDAP, MSSQL, NTP, SNMP, SSDP, SYN, TFTP, UDP, UDP-Lag, WebDDoS), что делает его релевантным для оценки современных систем обнаружения.

С развитием ML появилось множество работ, применяющих различные классификаторы для обнаружения DDoS. Среди них Support Vector Machines (SVM), Decision Trees (DT), Random Forest (RF), Naive Bayes (NB) и K-Nearest Neighbors (KNN) [8]. Эти методы часто показывают хорошую производительность, но требуют тщательного отбора признаков и настройки гиперпараметров. Работы [9, 10] предоставляют сравнительный анализ различных ML-алгоритмов на всякого рода наборах данных, включая унаследованные (KDD Cup 99, NSL-KDD) и современные (CICIDS2017, CIC-DDoS-2019).

В последнее время активно применяются методы глубокого обучения (DL, *аббр. от англ.* Deep Learning), такие как сверточные нейронные сети (CNN, *аббр. от англ.* Convolutional Neural Network) и рекуррентные нейронные сети (RNN, *аббр. от англ.* Recurrent Neural Network) – LSTM, GRU. DL-модели способны автоматически извлекать высокоуровневые признаки из сырых данных трафика, что потенциально улучшает точность обнаружения сложных атак. Однако они требуют больших объемов данных для обучения, значительных вычислительных ресурсов и часто страдают от недостатка интерпретируемости.

Применение нейро-нечетких систем для обнаружения вторжений, включая DDoS, также исследовалось, хотя и в меньшей степени по сравнению с чистыми ML/DL-подходами. В работе [11] предлагается использование ANFIS для обнаружения аномалий в сетевом трафике. Авторы [12] применяют ANFIS в сочетании с генетическими алгоритмами для оптимизации параметров системы обнаружения DDoS-атак. В [13] ANFIS используют для классификации атак на наборе данных KDD Cup 99, демонстрируя хорошие результаты. Однако применение ANFIS к новейшим и более сложным наборам данных, таким как CIC-DDoS-2019, содержащим современные векторы атак, остается менее изученной областью.

Методология

ANFIS представляет собой многослойную адаптивную сеть, функционально эквивалентную системе нечеткого вывода типа Сугено. Ее структура позволяет использовать алгоритмы обучения нейронных сетей для настройки параметров системы нечеткого вывода на основе обучающих данных [14]. Типичная архитектура ANFIS для системы с двумя входами и одним выходом показана на рисунке 1 и состоит из пяти слоев.

Слой 1 – слой фаззификации. Каждый узел в этом слое является адаптивным и вычисляет степень принадлежности входного значения к нечеткому множеству. При этом он соответствует одной нечеткой функции принадлежности (ФП).

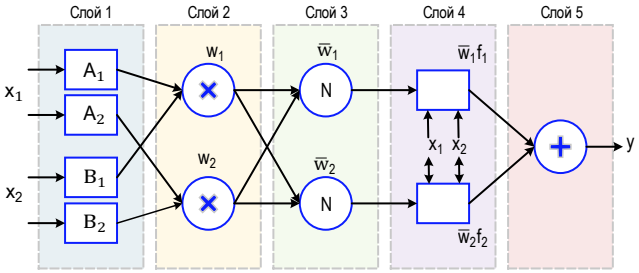


Рис. 1. Архитектура ANFIS для системы с двумя входами и одним выходом

Fig. 1. ANFIS Architecture for a System with Two Inputs and One Output

В данной реализации для каждого из входов используется две гауссовых ФП. Гауссова ФП определяется двумя параметрами – центром c и шириной σ:

$$\mu_{ij}(x_i) = e^{-\frac{1}{2}\left(\frac{x_i - c_{ij}}{\sigma_{ij}}\right)^2}, \quad (1)$$

где $\mu_{ij}(x_i)$ – степень принадлежности входного значения x_i к j-му нечеткому множеству для i-го входа; c_{ij} – центр (среднее значение) j-й гауссовой ФП для i-го входа; σ_{ij} – ширина (стандартное отклонение) j-й гауссовой ФП для i-го входа; x_i – нормализованное входное значение.

Начальные параметры c и σ инициализируются равномерно в диапазоне [0, 1] (после нормализации данных) с добавлением небольшого случайного шума. Сигма ограничивается снизу малым положительным значением $(1 \cdot 10^{-6})$ для стабильности.

Слой 2 – слой правил. Каждый узел соответствует одному нечеткому правилу. В данной реализации, с 10 входами и 2 ФП на вход, система оперирует 1024 правилами. Каждое правило неявно определяется уникальной комбинацией ФП (по одной от каждого входа).

Выход узла r (сила срабатывания правила w_r) вычисляется как произведение степеней принадлежности из Слоя 1, соответствующих данному правилу r:

$$w_r = \mu_{1,k_1}(x_1) \cdot \mu_{2,k_2}(x_2) \cdot \ldots \cdot \mu_{10,k_{10}}(x_{10}), \quad (2)$$

где k_i – индекс ФП для i-го входа в правиле r; $\mu_{i,k_i}(x_i)$ – степень принадлежности x_i к выбранной ФП для i-го входа.

Слой 3 – слой нормализации. Узлы этого слоя вычисляют нормализованную силу срабатывания каждого правила как отношение силы срабатывания правила r к сумме сил срабатывания всех правил:

$$\overline{w}_r = \frac{w_r}{\sum_{k=1}^{N} w_k}, \quad (3)$$

где $\overline{w}_r$ – нормализованная сила срабатывания правила r; w_r – исходная сила срабатывания правила r; N – общее количество правил в системе.

Слой 4 – слой дефаззификации. Каждый узел является адаптивным. Выход узла вычисляется как произведение нормализованной силы срабатывания правила на выход этого правила (линейную комбинацию входов для системы Сугено первого порядка).

Для модели Сугено нулевого порядка выход каждого правила является константой C_r (обучаемый параметр заключения). Выход узла r в этом слое равен произведению нормализованной силы срабатывания на константу этого правила.

Вектор параметров заключения $C = [C_1, C_2 \ldots C_N]$ инициализируется случайными малыми значениями.

Слой 5 – выходной слой. Единственный узел в этом слое вычисляет итоговый выход системы y как сумму выходов всех узлов предыдущего слоя:

$$y = \sum_{r=1}^{N} \overline{w}_r \cdot C_r, \quad (4)$$

где y – итоговый выход системы; $\overline{w}_r$ – нормализованная сила срабатывания правила r; C_r – параметр заключения правила r.

Обучение ANFIS обычно происходит с использованием гибридного алгоритма: параметры предпосылки (в слое 1) настраиваются методом градиентного спуска, а параметры заключения (в слое 4) вычисляются методом наименьших квадратов на прямом проходе. Это позволяет ANFIS эффективно настраивать как ФП, так и параметры выходных функций правил для аппроксимации заданной зависимости между входами и выходами.

Набор данных CIC-DDoS-2019

Для обучения и оценки модели ANFIS был выбран набор данных CIC-DDoS-2019, разработанный канадским университетом Нью–Брансуика. Представленный набор данных является одним из наиболее актуальных и комплексных общедоступных датасетов, специально сфокусированных на современных DDoS-атаках, что делает его референтным для оценки систем их обнаружения. В отличие от наборов, полученных ранее, таких как, CIC-IDS2017, который шире и ориентирован на различные типы вторжений в информационные системы, а не только DDoS [15], CIC-DDoS-2019 включает 16 типов современных DDoS-атак, включая атаки на уровне приложений и атаки с использованием механизмов амплификации. Фокус данного исследования направлен именно на обнаружение DDoS-атак, что делает специализированный набор CIC-DDoS-2019 наиболее подходящим для поставленной задачи. Он был создан путем захвата и анализа реального сетевого трафика в контролируемой среде.

Основные характеристики CIC-DDoS-2019:

– содержит как фоновый легитимный трафик, сгенерированный на основе профилей [16], так и трафик реальных DDoS-атак;

– включает 16 различных типов DDoS-атак, использующих протоколы TCP (SYN), UDP (DNS, LDAP, MSSQL, NetBIOS, NTP, SNMP, SSDP, TFTP, UDP, UDP-Lag) и HTTP (WebDDoS); атаки охватывают как методы отражения / амплификации, так и атаки на уровне приложений и на транспортном уровне;

– содержит значительный объем данных, представленных в виде двунаправленных потоков;

– для каждого потока извлечено более 75 статистических признаков с использованием инструмента CICFlowMeter [17]; данные признаки включают информацию о длительности потока, количестве пакетов, размерах пакетов, временны́х интервалах между пакетами (IAT), флагах TCP и т. д.

Использование CIC-DDoS-2019 позволяет оценить способность ANFIS обнаруживать широкий спектр современных DDoS-угроз в условиях, приближенных к реальным.

Хотя в данном исследовании используется репрезентативная выборка, она была сформирована таким образом, чтобы сохранить разнообразие представленных в исходном наборе типов атак и обеспечить возможность проведения экспериментов на оборудовании с ограниченными ресурсами, не теряя при этом общности выводов.

Предварительная обработка данных

Качество данных имеет решающее значение для построения эффективной модели ML. Данные CIC-DDoS-2019, представленные в формате CSV-файлов, требуют тщательной предварительной обработки.

Ввиду значительного размера полного набора данных (~50 Гб), для исследования была использована репрезентативная выборка, включающая легитимный трафик и несколько характерных типов DDoS-атак. Такой подход позволил провести эксперименты на оборудовании с ограниченными ресурсами, сохранив при этом разнообразие данных.

Признаки, не несущие полезной информации для классификации, были удалены. IP-адреса и порты могут быть полезны для анализа конкретной атаки, но для построения общей модели обнаружения их часто исключают, чтобы избежать переобучения на конкретные адреса. Также была проведена проверка на наличие пропущенных значений. Распространенной стратегией является замена значений NaN на медианное или нулевое значение, либо удаление строк с пропусками, если их немного. В данном исследовании строки с NaN также были удалены.

Признаки, являющиеся результатом деления («Flow Bytes/s», «Flow Packets/s»), могут содержать бесконечные значения, если делитель (длительность потока) равен нулю. Такие значения непригодны для большинства алгоритмов ML. Они были заменены на очень большие числа (представляющие максимальное значение для данного типа данных) или удалены / заменены медианой по столбцу. Были проверены и удалены полностью дублирующиеся строки.

Целевой признак «Label» содержит текстовые метки («Benign» и различные типы атак). Для задачи бинарной классификации все метки атак были объединены в один класс «DDoS». Затем метки «Benign» и «DDoS» были преобразованы в числовой формат (0 и 1).

Использование всех признаков набора данных неизбежно приведет к увеличению вычислительной сложности, переобучению и проблеме «проклятия размерности». Соответственно был применен метод отбора признаков на основе их важности, определенной с помощью алгоритма Random Forest, а также на основе корреляции и экспертных знаний о признаках, наиболее релевантных для DDoS-атак. Было выбрано подмножество наиболее информативных признаков («Down/Up Ratio», «URG Flag Count», «Avg Fwd Segment Size», «Fwd Packet Length Mean», «Packet Length Min», «Fwd Packet Length Min», «Packet Length Mean», «Bwd Packet Length Min», «Avg Packet Size», «Protocol»).

Значения признаков в наборе данных имеют различные диапазоны. Для корректной работы ANFIS необходимо привести все признаки к единому масштабу. Была применена нормализация с использованием функции MinMaxScaler [18], которая масштабирует значения в диапазоне [0, 1].

Обработанный набор данных был разделен на обучающую и тестовую выборки в пропорции 80 % / 20 %, соответственно. Разделение производилось стратифицированно для сохранения исходного соотношения классов в обеих выборках.

Реализация модели ANFIS

Для реализации ANFIS использовалась библиотека sklearn, предоставляющая функциональность для создания и обучения подобных систем. Количество входов модели ANFIS соответствует количеству признаков, выбранных на этапе отбора. Для каждого входа было определено два нечетких множества с использованием гауссовых ФП. Параметры функций (центр, ширина) инициализировались на основе распределения данных и затем настраивались в процессе обучения.

Система автоматически генерирует правила, покрывающие все комбинации нечетких множеств входных переменных. Модель имеет один выход,

представляющий степень уверенности в том, что входной поток является DDoS-атакой (значение близкое к 1) или легитимным трафиком (значение близкое к 0).

Модель обучалась на выборке с использованием гибридного алгоритма оптимизации (градиентный спуск + метод наименьших квадратов) в течение заданного числа эпох. Целевой функцией являлась минимизация среднеквадратичной ошибки (MSE, *аббр. от англ.* Mean Squared Error) между выходами модели и истинными метками (0 или 1).

Метрики оценки

Для оценки производительности обученной модели ANFIS на тестовой выборке использовались стандартные метрики бинарной классификации [19]. Матрица ошибок отображает количество истинно положительных (TP), истинно отрицательных (TN), ложно положительных (FP) и ложно отрицательных (FN) срабатываний.

Значения TP, TN, FP и FN, полученные из матрицы ошибок по результатам тестирования модели на отложенной выборке, напрямую используются для расчета метрик:

– Accuracy (доля правильно классифицированных объектов от общего числа объектов):

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}; \quad (5)$$

– Precision (точность – доля истинно положительных срабатываний среди всех примеров, классифицированных моделью как положительные; показывает, насколько можно доверять сигналу «атака»):

$$Precision = \frac{TP}{TP + FP}; \quad (6)$$

– Recall (полнота – доля истинно положительных срабатываний среди всех реально положительных примеров; показывает, какую долю реальных атак модель смогла обнаружить):

$$Recall = \frac{TP}{TP + FN}; \quad (7)$$

– F1-Score (F1-мера – среднее гармоническое точности и полноты; является метрикой для несбалансированных наборов данных, где важны и Precision, и Recall):

$$F_{score} = \frac{2 \cdot TP}{2 \cdot TP + FN + FP}. \quad (8)$$

Наряду с указанными метриками, для оценки точности непрерывных выходных значений ANFIS (представляющих степень уверенности в принадлежности к классу) до их преобразования в бинарные метки используется MSE, которая минимизируется в процессе обучения модели:

$$MSE = \frac{1}{M}\sum_{i=1}^{M}\left(y_{И}^{(i)} - y_{П}^{(i)}\right)^2, \quad (9)$$

где M – количество объектов в тестовой выборке; $y_{И}^{(i)}$ – истинное значение для i-го объекта; $y_{П}^{(i)}$ – предсказанное значение для i-го объекта.

Вышеуказанные показатели позволяют количественно оценить аспекты производительности классификатора. При этом высокие значения метрик Accuracy, Precision, Recall и F1-Score свидетельствуют о хорошей производительности системы обнаружения, в то время как низкое значение MSE указывает на высокую точность предсказаний модели.

Особое внимание в задачах обнаружения DDoS уделяется высокой полноте (минимизация FN, т. е. пропущенных атак) и приемлемой точности (минимизация FP, т. е. ложных тревог).

Проведение экспериментов

Эксперименты проводились с использованием библиотек языка программирования Python 3, а именно NumPy для вычислений, Pandas для обработки данных, Scikit-learn для предобработки, разделения данных и расчета метрик, Matplotlib для построения графиков. Использовалась подвыборка из CIC-DDoS-2019, включающая файл с легитимным трафиком и несколькими типами атак. Общий размер обработанной подвыборки составил 16 071 пакетов.

Параметры обучения:
– количество эпох: 20;
– размер батча: 64;
– скорость обучения: 0,1;
– количество гауссовых ФП на вход: 2;
– количество правил: $2^{10} = 1024$.

Обучающая выборка – 12 856 записей; тестовая выборка – 3 215 записей.

Выход ANFIS представляет собой непрерывное значение. Для бинарной классификации был установлен порог 0,5 (значения $\geq 0{,}5$ классифицировались как DDoS, а – $< 0{,}5$ как нормальная сетевая активность). После обучения модели ANFIS в течение 20 эпох на 80 % данных и тестирования на оставшихся 20 %, были получены следующие функции принадлежности (рисунок 2).

Среднее время обучения одной эпохи составило порядка 5–8 минут.

График ошибки обучения, изображенный на рисунке 3, показал общее снижение при увеличении количества эпох. Определено оптимальное количество эпох равное 4. Матрица ошибок изображена на рисунке 4. Метрики производительности модели представлены в таблице 1.

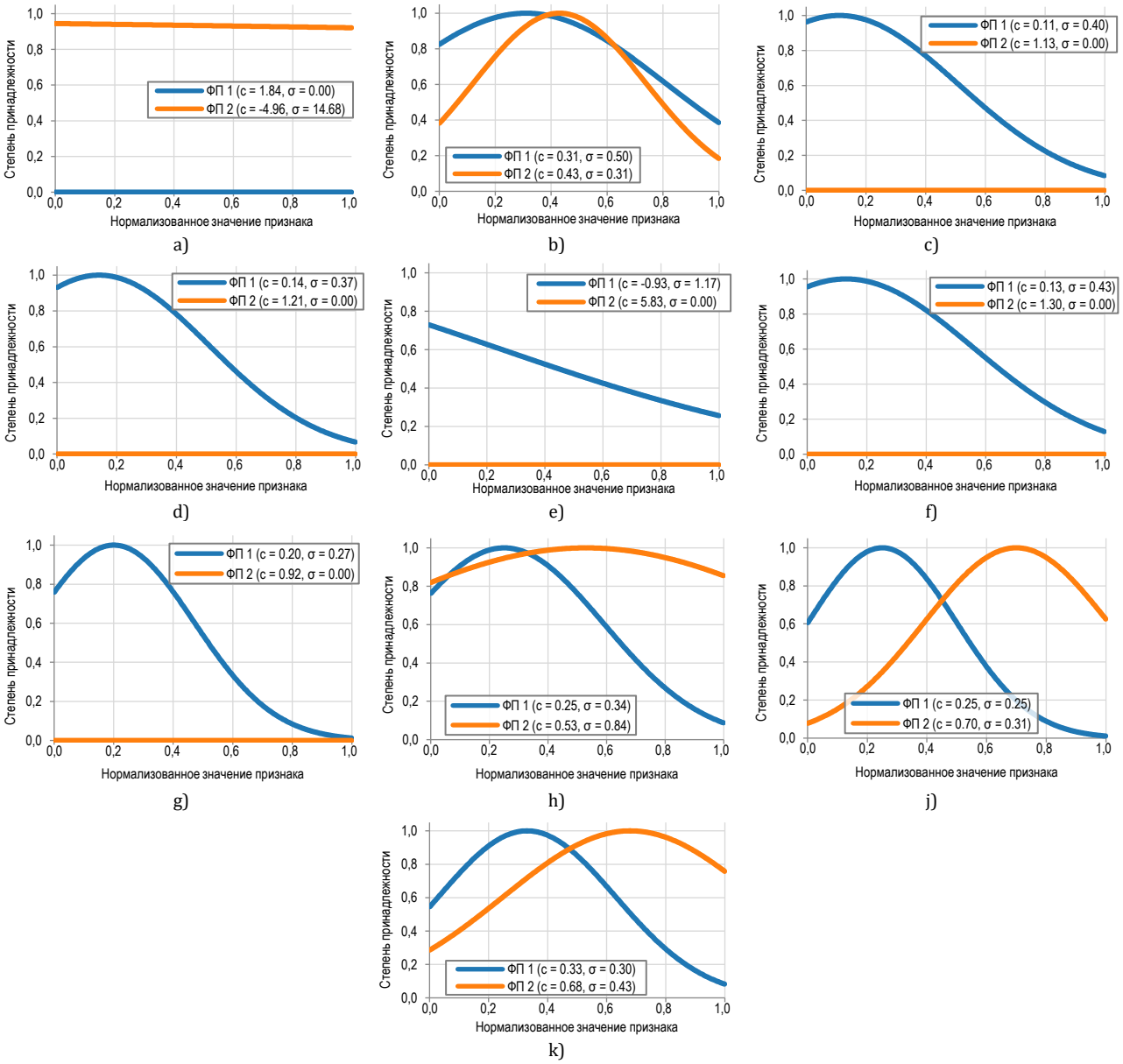


Рис. 2. Функции принадлежности для «Avg Fwd Segment Size» (a), «Avg Packet Size» (b), «Bwd Packet Length Min» (c), «Down/Up Ratio» (e), «Fwd Packet Length Mean» (f), «Fwd Packet Length Min» (g), Packet Length Mean» (h), «Protocol» (j) и «URG Flag Count» (k)

Fig. 2. Accessory Function for «Avg Fwd Segment Size» (a), «Avg Packet Size» (b), «Bwd Packet Length Min» (c), «Down/Up Ratio» (e), «Fwd Packet Length Mean» (f), «Fwd Packet Length Min» (g), Packet Length Mean» (h), «Protocol» (j) and «URG Flag Count» (k)

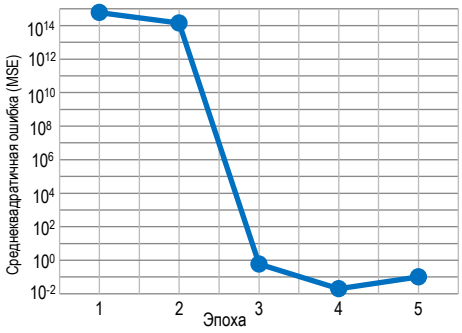


Рис. 3. График ошибки обучения ANFIS (MSE) по эпохам

Fig. 3. Graph of ANFIS Learning Error (MSE) by Epochs

Рис. 4. Матрица ошибок модели ANFIS

Fig. 4. Confusion Matrix for ANFIS

ТАБЛИЦА 1. Метрики производительности ANFIS

TABLE. 1. ANFIS Performance Metrics

Метрика	Значение (%)
Accuracy	97,82
Precision (DDoS)	99,52
Recall (DDoS)	85,95
F1-Score (DDoS)	92,24
MSE	2,46

Результаты свидетельствуют о высокой доле правильно классифицированных объектов. Представленная модель правильно классифицирует подавляющее большинство потоков трафика. Высокий показатель точности (Precision = 99,52 %) является особенно важным результатом, поскольку он указывает на крайне низкий уровень ложных срабатываний (FP = 2 в абсолютных числах из матрицы ошибок на рисунке 4). Это означает, что система редко ошибочно помечает легитимный трафик как атаку, что критично для минимизации перебоев в работе защищаемых сервисов. Полнота (Recall = 85,95 %) несколько ниже, что указывает на пропуск моделью 68 пакетов, относящихся к реальным атакам (FN = 68 на рисунке 4). Достигнутый уровень полноты в сочетании с высокой точностью является значимым для сложных и разнообразных атак, представленных в CIC-DDoS-2019. Высокий показатель F1-меры подтверждает хороший баланс точности и полноты.

Достигнутые метрики сопоставимы с результатами, получаемыми с использованием стандартных библиотек или других методов ML на указанном наборе данных [20], однако предложенный подход на основе ANFIS дополнительно предлагает преимущества в виде интерпретируемости функций принадлежности и правил нечеткого вывода.

Преимущества ANFIS в контексте обнаружения DDoS-атак

Во-первых, возможно дообучение модели на новых данных, что важно для адаптации к изменяющимся тактикам атак.

Во-вторых, в отличие от методов DL, из обученной ANFIS можно извлечь нечеткие правила. Анализ функций принадлежности и их связей может дать представление о том, какие комбинации значений признаков наиболее характерны для атак, что полезно для анализа и понимания угроз и обеспечивает интерпретируемость данного подхода.

В-третьих, нечеткая логика по своей природе хорошо справляется с зашумленными входными данными, что характерно для реального сетевого трафика.

В-четвертых, эксперименты показали, что ANFIS может достигать высоких показателей доли правильно классифицированных объектов, точности и полноты, минимизируя количество пропущенных атак.

Ограничения ANFIS

1) ANFIS, особенно с большим количеством входов и функций принадлежности, может быть вычислительно затратным. Количество правил увеличивается экспоненциально с увеличением числа входов и числа ФП. Это ограничивает количество признаков, которые могут быть эффективно использованы напрямую.

2) Производительность ANFIS зависит от выбора архитектуры (количества и типа ФП, количества входов). Оптимальный выбор параметров требует экспериментов и знаний в предметной области.

3) Применение ANFIS к потокам данных в реальном времени требует оптимизированных реализаций, а также интеграции с аппаратными ускорителями [21].

По сравнению с традиционными ML-алгоритмами (SVM, RF), ANFIS предлагает более удобный способ работы с неопределенностью и потенциально лучшую интерпретируемость правил. По сравнению с DL-моделями, ANFIS может требовать меньше данных для обучения и обеспечивает лучшую прозрачность.

Заключение

В статье было рассмотрено применение адаптивной нейро-нечеткой системы вывода (ANFIS) для задачи обнаружения DDoS-атак на основе набора данных CIC-DDoS-2019. Проведенные эксперименты, включающие этапы предварительной обработки данных, отбора признаков, обучения и тестирования модели ANFIS, продемонстрировали высокую эффективность предложенного подхода. Модель показала отличные результаты по метрикам доли правильно классифицированных объектов, точности, полноты и F1-меры, успешно идентифицируя DDoS-атаки с минимальным количеством ложных срабатываний, что особенно важно для практического применения, и приемлемым уровнем пропущенных атак, учитывая сложность и разнообразие атак, представленных в наборе данных.

Результаты подтверждают, что гибридный подход ANFIS, сочетающая адаптивность нейронных сетей и интерпретируемость нечеткой логики, делает ее мощным инструментом для разработки интеллектуальных систем обнаружения вторжений. Способность ANFIS моделировать границы между нормальным и аномальным поведением является ценным качеством при анализе сетевого трафика.

Список источников

1. Арикова К.Г. Анализ статистических данных по реализации кибератак и их последствий // Всероссийская студенческая научно-практическая конференция «Цифровая экономика и безопасность: вызовы и перспективы» (Москва, Российская Федерация, 21–22 марта 2024 г.). М.: РТУ МИРЭА, 2024. С. 10–14. EDN:DHNDAL

2. Баранов И.А., Кучеренко М.А., Карасев П.И. DDOS атаки и методы защиты от них // I Национальная научно-практическая конференция (Москва, Российская Федерация, 24–26 мая 2023 г.) «Кибербезопасность: технические и правовые аспекты защиты информации». М.: РТУ МИРЭА, 2023. С. 133–136. EDN:BQZKRL

3. Козлова Н.Ш., Довгаль В.А. Анализ применения искусственного интеллекта и машинного обучения в кибербезопасности // Вестник Адыгейского государственного университета. Серия: Естественно-математические и технические науки. 2023. № 3(326). С. 65–72. DOI:10.53598/2410-3225-2023-3-326-65-72. EDN:CYUKLH

4. Лизнева Ю.С., Ростова Е.В. К вопросу о применении машинного обучения для классификации сетевых аномалий // Всероссийская научно-техническая конференция с международным участием «Обработка информации и математическое моделирование» (Новосибирск, Российская Федерация, 19–20 апреля 2023 г.). Новосибирск: СибГУТИ, 2023. С. 58–61. EDN:DILYWD

5. Попов А.С., Константинова А.А. Применение искусственного интеллекта в системах информационной безопасности // Всероссийская студенческая научно-практическая конференция «Математические модели техники, технологий и экономики» (Санкт-Петербург, Российская Федерация, 15 мая 2024 г.). СПб.: СПбГЛТУ, 2024. С. 363–367. EDN:FNVXCM

6. Ростовцев В.С. Искусственные нейронные сети: учебник для вузов. СПб.: Лань, 2025. 216 с.

7. DDoS evaluation dataset (CIC-DDoS2019) // University of New Brunswick. URL: https://www.unb.ca/cic/datasets/ddos-2019.html (Accessed 29.03.2025)

8. Rahman M.A. Detection of distributed denial of service attacks based on machine learning algorithms // International Journal of Smart Home. 2020. Vol. 14. Iss. 2. PP. 15–24. DOI:10.21742/ijsh.2020.14.2.02. EDN:MMRDIG

9. Le D.C., Dao M.H., Nguyen K.L.T. Comparison of Machine Learning Algorithms for DDOS Attack Detection in SDN // Information and Control Systems. 2020. № 3(106). С. 59–70. DOI:10.31799/1684-8853-2020-3-59-70. EDN:GLVTEL

10. Shakya S., Abbas R. Comparative Evaluation of Machine Learning Models for DDoS Detection in IoT Networks. 2024. DOI:10.48550/arXiv.2411.05890

11. Mohamed Y.A., Salih D.A., Khanan A. An Approach to Improving Intrusion Detection System Performance Against Low Frequent Attacks // Journal of Advances in Information Technology. 2023. Vol. 14. Iss. 3. PP. 472–478. DOI:10.12720/jait.14.3.472-478

12. Toosi A.N., Kahani M. A new approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers // Computer Communications. 2007. Vol. 30. Iss. 10. PP. 2201–2212. DOI:10.1016/j.comcom.2007.05.002

13. Nwasra N., Daoud M., Qaisar Z.H. ANFIS-AMAL: Android Malware Threat Assessment Using Ensemble of ANFIS and GWO // Cybernetics and Information Technologies. 2024. Vol. 24. Iss. 3. PP. 39–58. DOI:10.2478/cait-2024-0024. EDN:EIOXIL

14. Молотникова А.А. Системный анализ. Краткий курс: учебное пособие для вузов. СПб.: Лань, 2021. 212 с.

15. Ahmed A.S., Kurnaz S., Khaleel A.M. Evaluation DDoS Attack Detection Through the Application of Machine Learning Techniques on the CICIDS2017 Dataset in the Field of Information Security // Mathematical Modelling of Engineering Problems. 2023. Vol. 10. Iss. 4. PP. 1125–1134. DOI:10.18280/mmep.100404

16. Копашенко М.А., Поздняк И.С. Нейросети при защите от DDOS атак // XXX Российская научно-техническая конференция «Актуальные проблемы информатики, радиотехники и связи» (Самара, Российская Федерация, 28 февраля – 3 марта 2023 г.). Самара: ПГУТИ, 2023. С. 85–87. EDN: ZWYLIB

17. Ковалев Е.А. Применение искусственных нейронных сетей в системах обеспечения информационной безопасности // Безопасность. Управление. Искусственный интеллект. 2022. Т. 4. № 4(4). С. 26–35. EDN:THNLOH

18. Груздев А.В. Предварительная подготовка данных в Python. Т. 2. План, примеры и метрики качества. М.: ДМК Пресс, 2023. 814 с.

19. Алексейчук А.С. Введение в нейронные сети: модели, методы и программные средства. М.: МАИ, 2023. 105 с.

20. Васин Н.Н., Какабьян К.С. Сравнительный анализ методов машинного обучения для решения задачи бинарной классификации сетевого трафика // Инфокоммуникационные технологии. 2025. Т. 22. № 2. С. 20–25. DOI:10.18469/ikt.2024.22.2.03. EDN:VZCOSB

21. Назаркин О.А., Сараев П.В. Повышение эффективности параллельного обучения ансамблей аппроксиматоров на основе ненормализованного варианта моделей ANFIS // 4-я Всероссийская научно-техническая конференция «Суперкомпьютерные технологии» (СКТ-2016, Дивноморское, Российская Федерация, 19–24 сентября 2016 г.). Ростов-на-Дону: Южный федеральный университет, 2016. С. 184–188. EDN:YQTHCB

References

1. Arikova K.G. Analysis of statistical data on the implementation of cyberattacks and their consequences. *Proceedings of the All-Russian Student Scientific and Practical Conference on Digital Economy and Security, 21–22 March 2024, Moscow, Russian Federation*. Moscow: RTU MIREA Publ.; 2024. p.10–14. (in Russ.) EDN:DHNDAL

2. Baranov I.A., Kucherenko M.A., Karasev P.I. DDoS attacks and methods of protection against them. *Proceedings of the Ist National Scientific and Practical Conference on Cybersecurity: Technical and Legal Aspects of Information Protection, 24–26 May 2023, Moscow, Russian Federation*. Moscow: RTU MIREA Publ.; 2023. p.133–136. (in Russ.) EDN:BQZKRL

3. Kozlova N.Sh., Dovgal V.A. Analysis of the Use of Artificial Intelligence and Machine Learning In Cybersecurity. *Bulletin of the Adyghe State University. Series: Natural, Mathematical and Technical Sciences*. 2023;3(326):65–72. (in Russ.) DOI:10.53598/2410-3225-2023-3-326-65-72. EDN:CYUKLH

4. Lizneva Yu.S., Rostova E.V. On the application of machine learning for network anomaly classification. *Proceedings of the All-Russian Scientific and Technical Conference with International Participation on Information Processing and Mathematical Modeling, 19–20 April 2023, Novosibirsk, Russian Federation*. Novosibirsk: SibSUTI Publ.; 2023. p.58–61. (in Russ.) EDN:DILYWD

5. Popov A.S., Konstantinova A.A. Application of artificial intelligence in information security systems. *Proceedings of the All-Russian Student Scientific and Practical Conference on Mathematical Models of Technology, Techniques, and Economics, 15 May 2024, St. Petersburg, Russian Federation*. St. Petersburg: SPbGLTU Publ.; 2024. p.363–367. (in Russ.) EDN:FNVXCM

6. Rostovtsev V.S. *Artificial Neural Networks*. St. Petersburg: Lan Publ.; 2025. 216 p. (in Russ.)

7. *University of New Brunswick*. DDoS evaluation dataset (CIC-DDoS2019). URL: https://www.unb.ca/cic/datasets/ddos-2019.html [Accessed 29.03.2025]

8. Rahman M.A. Detection of distributed denial of service attacks based on machine learning algorithms. *International Journal of Smart Home*. 2020;14(2):15–24. DOI:10.21742/ijsh.2020.14.2.02. EDN:MMRDIG

9. Le D.C., Dao M.H., Nguyen K.L.T. Comparison of Machine Learning Algorithms for DDOS Attack Detection in SDN. *Information and Control Systems*. 2020;3(106):59–70. DOI:10.31799/1684-8853-2020-3-59-70. EDN:GLVTEL

10. Shakya S., Abbas R. *Comparative Evaluation of Machine Learning Models for DDoS Detection in IoT Networks*. 2024. DOI:10.48550/arXiv.2411.05890

11. Mohamed Y.A., Salih D.A., Khanan A. An Approach to Improving Intrusion Detection System Performance Against Low Frequent Attacks. *Journal of Advances in Information Technology*. 2023;14(3):472–478. DOI:10.12720/jait.14.3.472-478

12. Toosi A.N., Kahani M. A new approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers. *Computer Communications*. 2007;30(10):2201–2212. DOI:10.1016/j.comcom.2007.05.002

13. Nwasra N., Daoud M., Qaisar Z.H. ANFIS-AMAL: Android Malware Threat Assessment Using Ensemble of ANFIS and GWO. *Cybernetics and Information Technologies*. 2024;24(3):39–58. DOI:10.2478/cait-2024-0024. EDN:EIOXIL

14. Molotnikova A.A. *System Analysis. Short Course*. St. Petersburg: Lan Publ.; 2021. 212 p. (in Russ.)

15. Ahmed A.S., Kurnaz S., Khaleel A.M. Evaluation DDoS Attack Detection Through the Application of Machine Learning Techniques on the CICIDS2017 Dataset in the Field of Information Security. *Mathematical Modelling of Engineering Problems*. 2023;10(4):1125–1134. DOI:10.18280/mmep.100404

16. Kopashenko M.A., Pozdnyak I.S. Neural networks in DDoS attack protection. *Proceedings of the XXX Russian Scientific and Technical Conference on Current Problems of Informatics, Radio Engineering and Communications, 28 February – 3 March 2023, Samara, Russian Federation*. Samara: PSUTI Publ.; 2023. p.85–87. (in Russ.) EDN: ZWYLIB

17. Kovalev E.A. Application of Artificial Neural Networks in Information Security Systems. *Bezopasnost'. Upravlenie. Iskusstvennyj intellekt*. 2022;4(4):26–35. (in Russ.) EDN:THNLOH

18. Gruzdev A.V. *Data Preprocessing in Python. Vol. 2. Plan, Examples, and Quality Metrics*. Moscow: DMK Press Publ.; 2023. 814 p. (in Russ.)

19. Alekseychuk A.S. *Introduction to Neural Networks: Models, Methods, and Software Tools*. Moscow: MAI Publ.; 2023. 105 p. (in Russ.)

20. Vasin N.N., Kakabian K.S. Comparative Analysis of Machine Learning Methods for Network Traffic Binary Classification. *Infocommunication Technologies*. 2025;22(2):20–25. (in Russ.) DOI:10.18469/ikt.2024.22.2.03. EDN:VZCOSB

21. Nazarkin O.A., Saraev P.V. Improving the Efficiency of Parallel Training of Approximator Ensembles Based on the Unnormalized Version of ANFIS Models. *Proceedings of the 4th All-Russian Scientific and Technical Conference on Supercomputer Technologies, SCT-2016, 19–24 September 2016, Divnomorskoye, Russian Federation*. Rostov-on-Don: Southern Federal University Publ.; 2016. p.184–188. (in Russ.) EDN:YQTHCB

Статья поступила в редакцию 13.05.2025; одобрена после рецензирования 27.05.2025; принята к публикации 23.06.2025.
The article was submitted 13.05.2025; approved after reviewing 27.05.2025; accepted for publication 23.06.2025.

Информация об авторах:

ВАСИН Николай Николаевич — доктор технических наук, профессор, профессор кафедры сетей и систем связи Поволжского государственного университета телекоммуникаций и информатики
https://orcid.org/0000-0001-9749-4884

КАКАБЬЯН Карен Сергеевич — инженер технической поддержки ООО «Яндекс Облако»
https://orcid.org/0009-0000-0043-1757

Авторы сообщают об отсутствии конфликтов интересов.
The authors declare no conflicts of interests.

Научная статья
УДК 621.391
https://doi.org/10.31854/1813-324X-2025-11-3-97-107
EDN:GUNCQI

Корпоративный алгоритм множественного доступа в киберпространстве

Наталья Аркадьевна Верзун ✉, verzun.n@unecon.ru
Михаил Олегович Колбанёв, mokolbanev@mail.ru
Борис Яковлевич Советов, bysovetov@etu.ru

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург, 197022, Российская Федерация

Аннотация

Актуальность. *Неотъемлемым компонентом киберпространства являются системы доступа, обеспечивающие распределение инфокоммуникационных ресурсов киберпространства между пользователями. Развитие и внедрение цифровых технологий требуют внесения корректив в архитектуру и принципы функционирования систем доступа. При этом необходимо учитывать, что требования, предъявляемые к ним, могут быть разнообразными, противоречивыми и определяются спецификой предметной области.*

Цель проведенного исследования: *предложить корпоративный алгоритм множественного доступа, основная идея которого – отказ от принципа состязательности источников нагрузки. «Корпоративность» алгоритма проявляется в использовании принципа «справедливого распределения» общего ресурса – канала передачи таким образом, чтобы все данные от всех источников нагрузки собирались и передавались организационно без задержек / без потерь. Главное требование к функционированию корпоративной системы множественного доступа – удовлетворение общему критерию оптимальности. Таким критерием может быть: средневзвешенная доля блоков данных принятых безошибочно и вовремя, или средневзвешенное среднее время задержки передачи блоков данных, или средневзвешенная доля потерянных блоков данных. В статье изложена концепция корпоративного алгоритма множественного доступа, за основу взят комбинированный* ***метод*** *разделения общего канала передачи: между группами источников нагрузки используется временно́е разделение, а внутри каждой группы – случайный синхронный доступ. Для реализации принципа корпоративного доступа используется процедура динамического регулирования доступом.*

Результаты. *Разработана математическая модель сети корпоративного множественного доступа и выражения для расчета вероятностно-временны́х характеристик передачи блоков данных. Сформулирована задача оптимизации: выбор наилучшего режима работы сети доступа, который предусматривает такое распределение временны́х окон между источниками нагрузки, что достигается экстремум общего критерия оптимальности. Для решения этой задачи предложен трехэтапный алгоритм: 1 этап – расчет всех возможных значений выбранного критерия оптимизации, за который принята средневзвешенная доля принятых безошибочно и вовремя блоков данных; 2 этап – построение графической модели задачи оптимизации; 3 этап – нахождение кратчайшего пути для построенного графа, совокупность ребер составляющих такой путь и будет решением задачи. Представлена апробация данного алгоритма.*

Теоретическая значимость *заключается в формализации описания архитектуры киберпространства, развитии методов, технологий и математических моделей множественного доступа в киберпространстве, а также в полученных расчетных выражениях, алгоритмах оптимизации процессов функционирования систем, реализующих корпоративный подход к множественному доступу.*

Ключевые слова: *киберпространство, система доступа, корпоративный алгоритм множественного доступа, общий критерий оптимальности*

Ссылка для цитирования: Верзун Н.А., Колбанёв М.О., Советов Б.Я. Корпоративный алгоритм множественного доступа в киберпространстве // Труды учебных заведений связи. 2025. Т. 11. № 3. С. 97–107. (in Russ.) DOI:10.31854/1813-324X-2025-11-3-97-107. EDN:GUNCQI

Original research
https://doi.org/10.31854/1813-324X-2025-11-3-97-107
EDN:GUNCQI

Corporate Algorithm of Multiple Access in Cyberspace

Natalia A. Verzun ✉, verzun.n@unecon.ru
Mikhail O. Kolbanev, mokolbanev@mail.ru
Boris Ya. Sovetov, bysovetov@etu.ru

Saint Petersburg Electrotechnical University "LETI",
St. Petersburg, 197022, Russian Federation

Annotation

Relevance*. An integral component of cyberspace are access systems that ensure the distribution of cyberspace information and communication resources among users. The development and implementation of digital technologies requires making adjustments to the architecture and principles of functioning of access systems. At the same time, it should be borne in mind that the requirements imposed on them can be diverse, contradictory and determined by the specifics of the subject area.* ***The purpose of the research*** *is to propose a competitive algorithm for multiple access, the main idea of which is the rejection of the principle of adversarial load sources. The "corporativeness" of the algorithm is manifested in the use of the principle of "fair distribution" of a common resource, the transmission channel, so that all data from all sources of the load is collected and transmitted corporately without delay/loss. The main requirement for the functioning of a corporate multiple access system is to meet the general criterion of optimality. Such criteria can be: the weighted average proportion of data blocks received correctly and on time, or the weighted average delay time in transmitting data blocks, or the weighted average proportion of lost data blocks.*

Methods. *The article outlines the concept of a corporate multiple access algorithm based on a combined method for dividing a common transmission channel: temporary separation is used between groups of load sources, and random synchronous access is used within each group. To implement the corporate access principle, a dynamic access control procedure is used.*

Results. *A mathematical model of a corporate multiple access network and expressions for calculating the probabilistic-temporal characteristics of data block transmission have been developed. The optimization problem is formulated: choosing the optimal mode of operation of the access network, which provides for such a distribution of time windows between load sources that the extremum of the general optimality criterion is achieved. A three–stage algorithm for solving the optimization problem is proposed: stage 1 is the calculation of all possible values of the selected optimization criterion, for which the weighted average proportion of data blocks received correctly and on time is taken, stage 2 is the construction of a graphical model of the optimization problem, and stage 3 is the finding of the shortest path for the constructed graph, the set of edges that make up such a path will be solving the problem. The approbation of this algorithm is presented.*

The theoretical significance *is the expansion in the formalization of the description of the architecture of cyberspace, the development of methods, technologies and mathematical models of multiple access in cyberspace, as well as in the calculated expressions obtained, algorithms for optimizing the functioning of systems that implement a corporate approach to multiple access.*

Keywords: *cyberspace, access system, corporate multiple access algorithm, general optimality criterion*

For citation: Verzun N.A., Kolbanev M.O., Sovetov B.Ya. Corporate Algorithm of Multiple Access in Cyberspace. *Proceedings of Telecommunication Universities.* 2025;11(3):97–107. DOI:10.31854/1813-324X-2025-11-3-97-107. EDN:GUNCQI

Введение

Киберпространство (кибернетическое пространство) относится к искусственным материальным пространствам, которое представляет собой комплекс взаимосвязанных и взаимодействующих друг с другом цифровых систем, используемых в процессах деятельности для сохранения, распространения и переработки информации, представленной в

форме цифровых данных. В [1, 2] дается ряд определений киберпространства:

– ISO/IEC 27032:2012 (заменен ISO/IEC 27032:2023): «Киберпространство – сложная среда, которая возникает в результате взаимодействия людей, программного обеспечения и услуг в интернете и поддерживается распределенными по всему миру физическими устройствами информационных и коммуникационных технологий и подключенными сетями»;

– США: Глобальная информационная среда, состоящая из взаимозависимых сетей, информационной инфраструктуры и данных, включая интернет, телекоммуникационные сети, компьютерные системы, а также встроенные процессоры и контроллеры;

– Япония: Пространство, основанное на сети интернет, которая расширена за счет развития цифровых технологий и множества независимых участников; в этой среде создается интеллектуальная собственность в форме технологических инноваций и новых бизнес-моделей, которые способствуют устойчивому развитию экономики;

– Китай: Киберпространство состоит из интернета, коммуникационных сетей, компьютерных систем, систем автоматического управления, цифровых устройств и приложений, услуг и данных.

Общее понимание термина «Киберпространство» содержит два элемента:

1) рукотворный глобальный объект, объединяющий в общую технологическую среду всевозможные цифровые системы и данные множества участников;

2) использование этой общей технологической среды ведет к созданию недоступных ранее моделей деятельности в широком круге предметных областей и росту экономики.

Киберпространство, как сложная система, включает в себя несколько подсистем (рисунок 1).

Рис. 1. Подсистемы киберпространства

Fig. 1. Subsystems of Cyberspace

Пользователями выступают люди и программы. Больше половины жителей Земли являются пользователями интернета, в РФ – это более 75 % населения [3].

Инфраструктура представляет собой три типа систем со следующими объемными характеристиками:

1) центры хранения данных – предназначены для хранения от сотен терабайт до нескольких эксабайт данных;

2) сети передачи данных со скоростями, достигающими гигабит в секунду на участках доступа и терабит в секунду на магистральных участках;

3) системы обработки данных (скорость обработки до нескольких эксафлопс).

Системы доступа в киберпространстве обеспечивают распределение ресурсов между пользователями, их функционирование основано на принципах и идеях, предложенных специалистами в те времена, когда появлялись первые сети связи: почтовые, телеграфные, телефонные. Используемые в этой подсистеме механизмы доступа позволяют задавать разграничительные политики, регламентировать процедуры распределения общего ресурса в целях эффективного и безопасного его использования [4].

Специфика систем доступа в киберпространстве

Многие принципы функционирования систем доступа, разработанные раньше, сохранились и полезны для современных систем доступа к киберпространству. К ним можно отнести следующее:

– применение процедур идентификации, аутентификация, авторизации пользователей;

– согласование технических характеристик доступа с затребованной услугой;

– идея применения технологий множественного доступа к общим ресурсам – для большой группы пользователей выделяется ограниченный объем ресурсов, который по определенным правилам и алгоритмам распределяется между ними и др.

Общим, разделяемым для реализации передачи данных от множества источников, ресурсом системы доступа выступает физическая среда распространения сигналов [5]. Задача системы доступа – распределение между пользователями этой физической среды таким образом, чтобы обеспечить качество предоставляемых услуг при рациональном потреблении ресурсов. Среда передачи может быть естественной (эфирные сети) или искусственно созданной (сети кабельные: электрические, оптические). Для передачи данных при этом используют электромагнитные колебания, свойства которых, а также природа канала передачи, позволяют применять разнообразные способы разделения физической среды между абонентами [6, 7]: пространственное деление – технология MIMO; временно́е деление – TDMA4; частотное деление – FDMA; кодовое разделение – CDMA; волновое разделение – WDMA и пр. Также используются комбинации всех вышеприведенных способов деления канала.

Доступ к среде передачи абонентов (источников нагрузки) носит состязательный характер и может быть реализован с применением:

– состязательного принципа, когда абоненты случайным образом пытаются захватить канал для передачи своих данных (это большая группа случайных методов доступа, к которой относят синхронный случайный доступ, ALOHA, семейство методов с контролем несущей CSMA и пр.);

– определенных правил, обеспечивающих некоторую очередность доступа абонентов к общим ресурсам и выделение каждому абоненту своей «части» канала для передачи данных. К подобным методам можно отнести методы: временно́го разделения, маркерный доступ, методы опроса и пр.

Системы доступа являются важным элементом киберпространства и требования, предъявляемые к ним, могут быть разнообразными, противоречивыми и определяются спецификой предметной области [8–12]. Это, в частности, может быть:

– огромное разнообразие видов терминалов;

– поддержка мобильности терминалов;

– большие объемы передаваемых данных;

– широкий диапазон скоростей передачи;

– малые временны́е задержки и поддержка режима реального времени;

– требования к масштабированию, надежности, скорости восстановления после сбоев;

– высокая плотность сети (появление сверхплотных сетей) и пр.

Развитие цифровых технологий требует внесения корректив в архитектуру и принципы функционирования сетей доступа. Необходимо отметить следующие аспекты, влияющие на эволюцию систем доступа:

– рост объемов передаваемых данных;

– увеличение числа подключенных терминальных устройств, прежде всего, за счет роста числа подключенных умных вещей;

– увеличение числа мобильных терминалов и, соответственно, рост значимости беспроводных технологий передачи;

– множество вариантов доступа терминальных устройств к глобальным инфокоммуникационным ресурсам через эфирные сети, использующие разнообразные технологии и образующие в совокупности гетерогенную беспроводную сеть;

– конвергенция различных, созданных на протяжении нескольких десятилетий, сетей электросвязи и образование единой гетерогенной инфокоммуникационной сети.

В киберпространстве требования к доступу меняются. В частности, можно выделить предложенную авторами концепцию шеринговых сетей доступа [13, 14]. Предусматривается не постоянное подключение абонентов к определенной сети, а аренду канала у одного из множества доступных в определенной точке пространства провайдера – соответственно тип канала / технология передачи может различаться. Т. е. вариативность системы доступа, которая предполагает, что на этапе доступа к ресурсам киберпространства можно выбирать разные сети доступа, процедуры, протоколы, операторов и пр.

Кроме того, данные сообщений, передаваемые через сети доступа киберпространству как в одном,

так и в другом направлении, «превратились» в контент, который несет те или иные смыслы пользователям и / или от них и, соответственно, может нарушить или оказать какое-либо негативное влияние на когнитивную безопасность киберпространства. Также можно отметить интеллектуализацию систем доступа.

Изменения в архитектуре систем доступа

Все эти требования так или иначе находят отражение в развитии архитектуры системы доступа в киберпространство. Теперь недостаточно, как раньше, только осуществить техническое подключение пользователя к ресурсам сети. Кроме этого, необходимо: выбрать оператора; обеспечить требуемую скорость интерфейса доступа, которая может изменяться в широком диапазоне значений; реализовывать функции информационного фильтра, который должен «работать» в двух направлениях: ограждать и защищать от опасностей проникновения как к пользователю, так и в киберпространство нежелательного и запрещенного контента. Учет новых (вышеперечисленных) требований киберпространства к системам доступа заставляет менять их архитектуру.

Во-первых, если описывать архитектуру сети доступа языком OSI, то это означает добавление еще одного подуровня к канальному (2-му) уровню модели OSI подобно тому, как это делалось, например, в MPLS (рисунок 2).

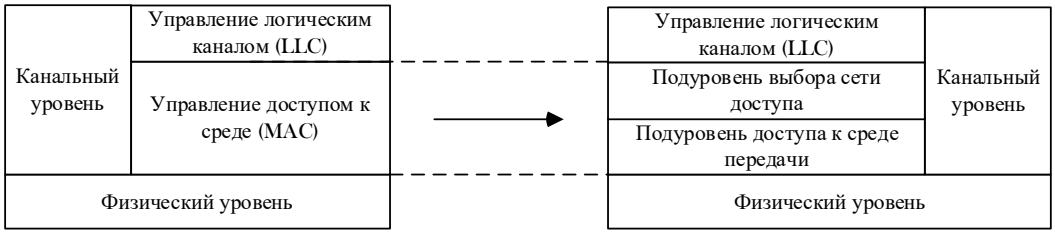


Рис. 2. Архитектура протоколов доступа устройств к глобальным инфокоммуникационным ресурсам [13]

Fig. 2. Architecture of Device Access Protocols to Global Infocommunication Resources

В архитектуре (см. рисунок 2) уровень управления доступом к среде передачи (MAC) разделен на два подуровня: выбора сети доступа и доступ к среде передачи.

В соответствии с данной архитектурой, сценарий предоставления услуги доступа к ресурсам реализуется в два шага.

Шаг 1. Выбор сети для доступа.

Шаг 2. Передача пользовательских данных.

Во-вторых, еще одним возможным новшеством при организации передачи данных является отказ от принципа состязательности источников нагрузки. Необходимость отказа возникает в случаях, когда, например:

– речь идет о передаче данных в интернете вещей, если предметная область требует непременного своевременного получения данных обязательно от всех устройств (например, в медицине для постановки диагноза или принятия решения о состоянии пациента, необходимо без опоздания получить данные от всех датчиков);

– организуется рой беспилотных автономных устройств, и без информации о координатах каждого устройства невозможно принимать решение о дальнейшей траектории движения роя в целом.

Отказ от принципа состязательности может быть реализован путем создания системой множественного доступа дополнительных канальных ресурсов, которые способны обеспечить уменьшение задержек при передаче критически важных данных (состояние пациента, координаты беспилотного устройства, регистрация атаки системой информационной безопасности и т. п).

Алгоритм, отвечающий данным требованиям, предлагается назвать *корпоративным алгоритмом множественного доступа*. Термин «корпоративный» используется в данном случае в том же смысле, что и в теории игр (корпоративные игры). Так, в [15] следующим образом описывается специфика понятия «корпоративный»: «Основное внимание кооперативной теории концентрируется на описании и изучении вариантов возможных стабильных и справедливых «дележей» (распределения) общественного продукта». В основе этого утверждения лежит принцип «справедливого распределения общественного продукта», т. е. распределение канала передачи таким образом, чтобы все данные от всех источников нагрузки собирались и передавались корпоративно без задержек / без потерь.

Главное требование к функционированию корпоративной системы множественного доступа – удовлетворение *общему критерию оптимальности*. Таким критерием может быть, например: средневзвешенная доля принятых безошибочно и вовремя блоков данных; средневзвешенное среднее время задержки передачи блоков данных; средневзвешенная доля потерянных блоков данных.

Концепция корпоративного алгоритма множественного доступа

Изложим суть алгоритма в терминах интернета вещей и за основу возьмем синхронно-временно́й метод доступа к каналу передачи [16, 17]. Объектом исследования является беспроводная сенсорная сеть интернета вещей с M типами источников нагрузки (M типов сенсоров), число источников каждого типа m_i, i = 1, …, M. Физическая структура сети показана на рисунке 3.

Таким образом, имеем M групп источников нагрузки, для каждой из которых (т. е. для каждого типа сенсора) могут быть определены свои параметры передаваемых блоков (длина k, бит) и требования к качеству передачи. Например: среднее допустимое время старения данных $\overline{T_{дi}}$, с; допустимая вероятность потерь блоков данных $p_{дi}$, $i = \overline{1, M}$ и пр.

На вход источников нагрузки поступают бернуллиевские потоки пакетов данных с интенсивностью λ_i, $i = \overline{1, M}$, на интервалах T_0:

$$T_0 = 1/V_c,$$

где V_c – скорость передачи сигналов в физической среде, бит/с.

Для физической среды определены скорость передачи бит в среде V_c, б/с, и качество среды передачи (определяется вероятностью искажения 1 бита информации – p).

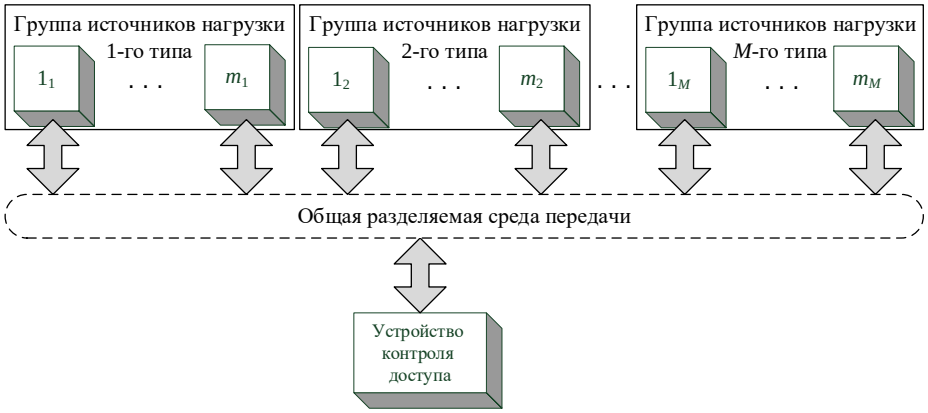


Рис. 3. Физическая структура сети корпоративного множественного доступа

Fig. 3. The Physical Structure of the Corporate Multiple Access Network

Предположим комбинированный метод разделения общего канала передачи: между группами источников нагрузки (между разными типами сенсоров) используется временно́е разделение, а внутри каждой группы – случайный синхронный доступ [17]. Для управления доступом источников нагрузки предусмотрено устройство контроля доступа (УКД), работающее в режиме временно́го разделения канала. УКД принимает запросы на передачу данных от источников нагрузки и отправляет ответ-разрешение на передачу с указанием числа временны́х окон, основываясь при принятии решения о выделении определенного числа окон для передачи данных в следующем цикле на текущем состоянии системы – на расчете используемого *общего критерия оптимальности*. Будем предполагать, что обмен служебными сообщениями между УКД и источниками нагрузки реализуется по отдельному каналу и в математической модели не учитывается.

Для реализации принципа корпоративного доступа используется процедура динамического регулирования. Предусматривается неравномерное распределение имеющихся в наличии временны́х окон. N – количество временны́х окон, доступных для передачи данных в цикле ($N > M$). Идея динамического регулирования доступом состоит в том, что для тех групп источников нагрузки, где требования к скорости / качеству передачи выше, в цикле предоставляется большее число временны́х окон для передачи. Для каждой группы источников нагрузки предоставляется минимум одно временно́е окно для передачи, а максимальное число окон, соответственно, равно ($N – M$). Распределение временны́х окон происходит *согласно общему критерию оптимальности*.

Длительность временны́х окон для передачи блоков данных будем считать постоянной и определим по выражению:

$$T_{ок} = kV_c^{-1}. \quad (1)$$

Математическая модель сети корпоративного множественного доступа

Математическая модель сети корпоративного множественного доступа представляется в виде совокупности моделей групп источников нагрузки ее составляющих [17]. Всего M групп для M типов источников нагрузки. Каждая группа источников

описана системой массового обслуживания *M/G/1* в дискретном времени на интервалах T_0 [18].

Блоки данных, поступающие от источников, считаются обслуженными, если:

– в них не обнаружено ошибки в результате применения помехоустойчивого кодирования (вероятность необнаружения ошибки $Q_к$):

$$Q_к = (1-p)^k; \quad (2)$$

– разрешен доступ источника к сети с вероятностью $q_{дi}$ (в соответствии с протоколом ССД):

$$q_{дi} = \frac{1}{m_i}, i = \overline{1,M}; \quad (3)$$

– отсутствовали мешающие воздействия других источников нагрузки того же типа, т. е. не было конфликтов при передаче (вероятность отсутствия мешающих воздействий других источников того же типа $Q_{мi}$):

$$Q_{мi} = (1-q_{дi}\Theta_i)^{m_i-1}, i = \overline{1,M}, \quad (4)$$

где Θ_i – вероятность занятости источника нагрузки *i*-го типа.

В противном случае доставка блока данных источником повторяется.

Используется временно́е разделение канала между группами источников нагрузки, но общее число выделяемых для передачи блоков данных временны́х окон (N) больше числа подсетей (M) и в цикле передачи источникам нагрузки определенного типа может выделяться j = 1, 2, … (N – M) временны́х окон.

В этом случае интервал однократной передачи блоков в интервалах T_0 в каждой группе будет определяться следующим образом:

$$C_i = \frac{Nk}{n_i}, \sum_i^M n_i = N, i = \overline{1,M}, \quad (5)$$

где k – длительность временно́го окна для передачи блока данных в интервалах T_0; n_i – число окон, выделенных для передачи блоков данных от источника *i*-го типа, $i = \overline{1,M}$.

z-преобразования рядов распределения (z-ппр) интервалов однократной передачи в интервалах T_0 для всех групп источников будут иметь вид:

$$g_{si}(z) = z^{-C_i}, \ i = \overline{1,M}, \quad (6)$$

Тогда z-ппр интервала обслуживания при передаче блоков данных от источников *i*-го типа в интервалах T_0 (для режима «бесконечное число переспросов») будет иметь вид:

$$g_i(z) = \frac{Q_{ci}}{z^{C_i} - P_{ci}}, \ Q_{ci} = q_{дi}Q_к Q_{мi}, \quad P_{ci} = 1 - Q_{ci}, i = \overline{1,M}, \quad (7)$$

где $Q_к$, $q_{дi}$ и $Q_{мi}$ определяется из (2, 3 и 4).

z-ппр интервала обслуживания при передаче блоков данных от источников *i*-го типа в интервалах T_0 (для режима «прямая передача без переспросов») будет иметь вид:

$$g_i(z) = g_{si}(z) = z^{-C_i}, \ i = \overline{1,M}, \quad (8)$$

где z-ппр времени задержки при передаче блоков данных от источников *i*-го типа:

$$f_i(z) = \frac{(1-\Theta_i)(1-z)g_i(z)}{1 - zp_i - q_i z g_i(z)}, q_i = \lambda_i T_0, \quad p_i = 1 - q_i, i = \overline{1,M}, \quad (9)$$

где $g_i(z)$ – z-ппр интервала обслуживания при передаче информации от источников нагрузки *i*-го типа определяется из (7) или (8) в зависимости от используемого режима передачи блоков данных.

Взаимовлияние групп различных типов источников нагрузки учитывается в системе уравнений интерференции:

$$\Theta_i = q_i\overline{n_{si}}, \overline{n_{si}} = g_i'(1) = (d/dz^{-1})g_i(z)|_{z=1}, \quad \Theta_i < 1, i = \overline{1,M}. \quad (10)$$

Подставив в (10) выражения (2, 3, 4 и 7) и упростив, найдем следующую систему уравнений для режима «бесконечное число переспросов»:

$$\Theta_i = \frac{q_i C_i}{Q_{ci}}, \ \Theta_i < 1, i = \overline{1,M}. \quad (11)$$

Подставив в (10) выражения (2, 3, 4 и 8) и упростив, найдем следующую систему уравнений для режима «прямая передача без переспросов»:

$$\Theta_i = q_i C_i, \Theta_i < 1, i = \overline{1,M}. \quad (12)$$

Вероятностно-временны́е характеристики

Среднее время задержки при передаче блоков данных *i*-й группы источников можно найти, используя формулу Хинчина – Полячека [19]:

$$\overline{t_i} = \overline{n_i}T_0, \overline{n_i} = g_i'(1) + \frac{q_i g''_i(1)}{2(1-\Theta_i)}, \quad g_i''(1) = (d/dz^{-2})g_i(z)|_{z=1}, \ \Theta_i < 1, i = \overline{1,M}. \quad (13)$$

Для режима «бесконечное число переспросов» в (13) надо подставить выражения (2, 3, 4, 7 и 11), а для режима «прямая передача без переспросов» в (13) надо подставить выражения (2, 3, 4, 8 и 12).

Выражения для расчета вероятности своевременной доставки блоков данных блоков данных *i*-й группы источников предлагаются для случая стохастического ограничения на время обслуживания блоков, при котором допустимые времена передачи блоков данных задаются геометрическими распределениями с параметрами $s_{дi}$, $i = \overline{1,M}$:

$$\Pi_i = f_q(z)\big|z = s_{дi}^{-1},\ s_{дi} = 1 - T_0/\overline{T_{дi}},\ i = \overline{1,M}, \quad (14)$$

где $\overline{T_{дi}},\ i = \overline{1,M}$ – средние допустимые времена старения блоков данных передаваемых источниками i-го типа; $f_q(z)$ z-прр времени задержки при передаче блоков данных определяется из (9).

Сформулируем задачу оптимизации

Предположим, что для M групп источников нагрузки внутри цикла опроса выделяется N временны́х окон, причем $N > M$. Поставим задачу оптимального распределения N временны́х окон между источниками нагрузки таким образом, чтобы средневзвешенная доля потери передаваемых блоков данных была минимальной.

Целевая функция принимает следующий вид:

$$\sum_{i=1}^{M} \frac{\lambda_i}{\lambda} Q_i(n_i) \to \min, \quad \sum_{i=1}^{M} \lambda_i = \lambda, \quad \sum_{i}^{M} n_i = N, \quad (15)$$

где $Q_i(n_i)$ – вероятность потери пакетов, поступающих от i-й группы источников нагрузки в случае выделения для этой группы n_i временны́х окон, определяется из выражения:

$$Q_i(n_i) = 1 - \Pi_i(n_i),\ i = \overline{1,M}. \quad (16)$$

где $\Pi_i(n_i)$ – вероятность своевременной безошибочной доставки пакетов, поступающих от i-й группы источников нагрузки в случае выделения для этой группы n_i временны́х окон, определяется из (14); дополнительно могут быть введены ограничения на количество временны́х окон выделяемых каждой группе источников нагрузки.

Задача оптимизации (15) относится к области динамического программирования и может быть решена [20, 21] при помощи рекуррентного уравнения Беллмана (в три этапа).

Решение задачи оптимизации.

Этап 1. Расчет всех возможных значений вероятностей потерь пакетов.

Этап 2. Построение графической модели задачи оптимизации.

Этап 3. Нахождение кратчайшего пути для построенного графа, совокупность ребер составляющих такой путь и будет решением задачи.

Численный пример решения задачи оптимизации

Исходные данные для расчетов:

$M = 3$ – число групп источников нагрузки;

$N = 5$ – число временны́х окон;

$m_i = 5, i = \overline{1,3}$ – число источников нагрузки в каждой группе;

предположим, что для каждой группы источников может быть выделено от 1 до 3-х временны́х окон, т. е. $n_i = \overline{1,3}, i = \overline{1,3}$;

$\lambda_i = 10$ блок/с $, i = \overline{1,3}$ – интенсивность входных потоков блоков данных для всех типов источников;

$k = 1024$ бит – длина передаваемых блоков данных;

$V_c = 10^6$ бит/с – скорость передачи;

$p = 10^{-7}$ – вероятность искажения 1 бит при передаче в физической среде;

$\overline{T_{д1}} = 0{,}5$ с – среднее допустимое время старения данных для источников нагрузки 1-й группы;

$\overline{T_{д2}} = 1$ с – среднее допустимое время старения данных для источников нагрузки 2-ой группы;

$\overline{T_{д3}} = 3$ с – среднее допустимое время старения данных для источников нагрузки 3-й группы.

Этап 1. Расчет всех возможных значений вероятностей потерь блоков данных производился по формулам, представленным выше. Результаты расчетов показаны в таблице 1.

ТАБЛИЦА 1. Результаты расчетов вероятностей потерь блоков данных

TABLE 1. Results of Calculations of Data Block Loss Probabilities

	$n_i=1, i = \overline{1,3}$	$n_i=2, i = \overline{1,3}$	$n_i=3, i = \overline{1,3}$
$Q_1(n_i)$	$Q_1(1) = 0{,}0913$	$Q_1(2) = 0{,}0322$	$Q_1(3) = 0{,}0197$
$Q_2(n_i)$	$Q_2(1) = 0{,}0477$	$Q_2(2) = 0{,}0163$	$Q_2(3) = 0{,}0099$
$Q_3(n_i)$	$Q_3(1) = 0{,}0164$	$Q_3(2) = 0{,}0055$	$Q_3(3) = 0{,}0033$

Этап 2. Представим все возможные варианты распределения временны́х окон в системе корпоративного множественного доступа в виде графа (рисунок 4). На графе $\hat{n}_i$ обозначено суммарное количество временны́х окон, выделяемых первой, второй … и i-й (в данном случае 3-й) группе источников нагрузки. Каждому ребру графа соответствует значение $Q_i(n_i)$ из таблицы 1.

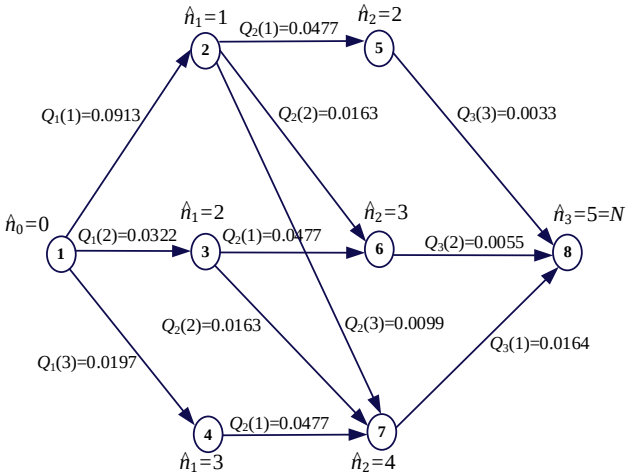


Рис. 4. Графическая модель задачи оптимизации

Fig. 4. Graphical Model of the Optimization Problem

Этап 3. Найдем кратчайший путь для построенного графа. Графическая модель (см. рисунок 4) показывает все возможные варианты распределения пяти временны́х окон между тремя группами источников нагрузки. Например, путь графа, который проходит через вершины 1–2–5–8, соответствует тому случаю, когда для 1-й группы источников нагрузки выделено одно временно́е окно для передачи, для 2-й – одно, а для 3-ей группы – три временны́х окна. Получаемая при этом средневзвешенная доля потери передаваемых блоков данных (15) определяется следующим образом:

$$\frac{10}{30}(0.0913 + 0.0477 + 0.0033) = 0{,}0474.$$

Таким образом, задача оптимизации сведена к поиску пути графа, имеющего минимальную длину из всех возможных. После того, как кратчайший путь будет найден, по ребрам, составляющим этот путь, можно определить искомое распределение временны́х окон между группами источников нагрузки.

В данном случае решением задачи оптимизации будет путь графа, проходящий через вершины 1–4–7–8. Получаемая при этом средневзвешенная доля потери передаваемых блоков данных будет наименьшей:

$$\frac{10}{30}(0.0197 + 0.0477 + 0.0164) = 0{,}0279.$$

Путь 1–4–7–8 соответствует случаю, когда для 1-й группы источников нагрузки выделено три временны́х окна для передачи, а для 2-ой и 3-й групп – по одному временно́му окну. Именно такое распределение временны́х окон между группами источников нагрузки даст наиболее эффективное разделение среды передачи с точки зрения выбранного для оптимизации критерия – средневзвешенной доли потери передаваемых блоков данных.

Заключение

В статье изложена концепция корпоративного алгоритма множественного доступа, которая состоит в отказе от принципа состязательности источников нагрузки в процессе разделения общей среды передачи. «Корпоративность» предполагает «справедливое распределение» канала передачи таким образом, чтобы данные, поступающие от всех источников нагрузки, собирались и передавались совместно без задержек (или без потерь). Для оценки качества функционирования системы корпоративного множественного доступа предлагается использовать общий критерий оптимальности. Это может быть: средневзвешенная доля принятых безошибочно и вовремя блоков данных, или средневзвешенное среднее время задержки передачи блоков данных, или средневзвешенная доля потерянных блоков данных. За основу корпоративного алгоритма множественного доступа взят комбинированный метод разделения общего канала передачи: между группами источников нагрузки используется временно́е разделение, а внутри каждой группы – случайный синхронный доступ.

В работе предложена математическая модель сети корпоративного множественного доступа, приведен метод расчета вероятностно-временны́х характеристик передачи блоков данных, а также сформулирована задача оптимизации. Выбор наилучшего режима работы сети доступа обеспечивает такое распределение временны́х окон между источниками нагрузки, при котором достигается экстремум общего критерия оптимальности.

Предложен трехэтапный алгоритм решения задачи оптимизации: расчет всех возможных значений выбранного критерия оптимизации, за который принята вероятность потерь блоков данных; построение графической модели задачи оптимизации; нахождение кратчайшего пути для построенного графа, совокупность ребер составляющих такой путь и будет решением задачи.

Представлены численные расчеты, которые иллюстрируют возможности применения рассмотренных в статье моделей, методов и алгоритмов.

Список источников

1. Аналитический отчет. Стратегии кибербезопасности. URL: https://www.infowatch.ru/sites/default/files/publication_file/analiticheskiy-otchet-strategii-kiberbezopasnosti.pdf (дата обращения 18.06.2025)

2. ISO/IEC 27032:2023. Cybersecurity – Guidelines for Internet security. 2023. URL: https://www.iso.org/standard/76070.html (Accessed 18.06.2025)

3. Digital 2024: Global Overview Report // Kepios. 2024. URL: https://datareportal.com/reports/digital-2024-global-overview-report (Accessed 18.06.2025)

4. Верзун Н.А., Колбанёв М.О. Глава 5. Модели опасности доступа в киберпространстве // Модели цифровой опасности в кибернетическом и когнитивном пространствах. СПб.: Санкт-Петербургский государственный экономический университет. 2023. С. 93–123. EDN:AAHVOZ

5. Vaezi M., Ding Z., Poor H.V. Multiple Access Techniques for 5G Wireless Networks and Beyond. Cham: Springer, 2019. DOI:10.1007/978-3-319-92090-0

6. Бакулин М.Г., Бен Режеб Т.Б.К., Крейнделин В.Б., Миронов Ю.Б., Панкратов Д.Ю, Смирнов А.Э. Многостанционный доступ в системах связи пятого и последующих поколений // Электросвязь. 2022. № 5. С. 16–21. DOI:10.34832/ELSV.2022.30.5.002. EDN:KCCLIL

7. Basharat M., Ejaz W., Naeem M., Khattak A.M., Anpalagan A. A survey and taxonomy on nonorthogonal multiple-access schemes for 5G networks // Transactions on Emerging Telecommunications Technologies. 2018. Vol. 29. Iss. 1. P. e3202. DOI:10.1002/ett.3202

8. Росляков А.В. Сети фиксированной связи пятого поколения. М.: ООО «ИКЦ «Колос-с», 2024. 232 с. EDN:DXGSFN

9. Богатырев В.А., Богатырев С.В., Богатырев А.В. Оценка готовности компьютерной системы к своевременному обслуживанию запросов при его совмещении с информационным восстановлением памяти после отказов // Научно-технический вестник информационных технологий, механики и оптики. 2023. Т. 23. № 3. С. 608–617. DOI:10.17586/2226-1494-2023-23-3-608-617. EDN:JWPOKM

10. Кучерявый А.Е., Парамонов А.И., Маколкина М.А., Мутханна А.С.А., Выборнова А.И., Дунайцев Р.А. и др. Трехмерные многослойные гетерогенные сверхплотные сети // Информационные технологии и телекоммуникации. 2022. Т. 10. № 3. С. 1–12. DOI:10.31854/2307-1303-2021-10-3-1-12. EDN:LHLYEM

11. Захаров М.В., Киричек Р.В. Методы построения сверхплотной сети e-health с использованием граничных вычислений // 75-я Научно-техническая конференция Санкт-Петербургского НТО РЭС им. А.С. Попова, посвященная Дню радио: сб. докладов. СПб.: СПбГЭТУ «ЛЭТИ», 2020. С. 145–147. EDN:XVIGBJ

12. Росляков А.В., Герасимов А.В. Детерминированные сети связи и их стандартизация. // Стандарты и качество. 2024. № 7. С. 42–47. DOI:10.35400/0038-9692-2024-7-70-24. EDN:UTBDXB

13. Verzun N., Kolbanev M., Shamin A. The Architecture of the Access Protocols of the Global Infocommunication Resources // Computers. 2020. Vol. 9. Iss. 2. P.49. DOI:10.3390/computers9020049. EDN:KJCHRF

14. Verzun N., Kolbanev M., Vorobeva D. Access Control Model to Global Infocommunication Resources // Proceedings of The Majorov International Conference on Software Engineering and Computer Systems (Saint Petersburg, Russian Federation, 12–13 December 2019). Vol. 11. Saint Petersburg: Federal State Autonomous Educational Institution of Higher Education "National Research University ITMO" Publ., 2020. PP. 218–221. EDN:RDFFNM

15. Маракулин В.М. Элементы теории кооперативных игр. URL: http://old.math.nsc.ru/~mathecon/Marakulin/CooGAMES.pdf (дата обращения 18.06.2025)

16. Гезалов Э.Б. Модель неоднородной локальной сети связи с протоколом синхронного временного доступа с учетом надежности ее элементов // T-Comm: Телекоммуникации и Транспорт. 2021. Т. 15. № 3. С. 25–29. DOI:10.36724/2072-8735-2021-15-2-25-29. EDN:WDTOSM

17. Верзун Н.А., Воробьёв А.И., Пойманова Е.Д. Моделирование процесса передачи информации с разграничением прав доступа пользователей // Известия высших учебных заведений. Приборостроение. 2014. Т. 57. № 9. С. 33–37. EDN:SMPASB

18. Вишневский В.М. Теоретические основы проектирования компьютерных сетей. М.: Техносфера. 2003. 512 с.

19. Вентцель Е.С. Исследование операций. Задачи, принципы, методология. М.: Наука, 1988. 208 с.

20. Беллман Р., Дрейфус С. Прикладные задачи динамического программирования. Пер. с англ. М.: Наука, 1965.

21. Рачков М.Ю. Оптимальное управление в технических системах. М.: Юрайт, 2023. 120 с.

References

1. *Analytical report. Cybersecurity strategies*. (in Russ.) URL: https://www.infowatch.ru/sites/default/files/publication_file/analiticheskiy-otchet-strategii-kiberbezopasnosti.pdf. [Accessed 18.06.2025]

2. ISO/IEC 27032:2023. *Cybersecurity – Guidelines for Internet security*. 2023. URL: https://www.iso.org/standard/76070.html [Accessed 18.06.2025]

3. Digital 2024: Global Overview Report // Kepios. 2024. URL: https://datareportal.com/reports/digital-2024-global-overview-report (Accessed 18.06.2025)

4. Verzun N.A., Kolbanev M.O. Chapter 5. Models of access hazards in cyberspace. *In: Models of digital danger in cybernetic and cognitive spaces.* St. Petersburg: St. Petersburg State University of Economics Publ.; 2023. p.93–123. (in Russ.) EDN:AAHVOZ

5. Vaezi M., Ding Z., Poor H.V. *Multiple Access Techniques for 5G Wireless Networks and Beyond*. Cham: Springer; 2019. DOI:10.1007/978-3-319-92090-0

6. Bakulin M.G., Ben Rejeb T.B.K., Kreindelin V.B., Mironov Yu.B., Pankratov D.Yu., Smirnov A.E. Multiple Access Schemes for 5G And Next Generations Communication Systems. *Electrosvyaz.* 2022;5:16–21. (in Russ.) DOI:10.34832/ELSV.2022.30.5.002. EDN:KCCLIL

7. Basharat M., Ejaz W., Naeem M., Khattak A.M., Anpalagan A. A survey and taxonomy on nonorthogonal multiple-access schemes for 5G networks. *Transactions on Emerging Telecommunications Technologies*. 2018;29(1):e3202. DOI:10.1002/ett.3202

8. Roslyakov A.V. *Fifth–Generation Fixed-Line Networks*. Moscow: Kolos-S Publ.; 2024. 232 p. (in Russ.) EDN:DXGSFN

9. Bogatyrev V.A., Bogatyrev S.V., Bogatyrev A.V. Assessment of the readiness of a computer system for timely servicing of requests when combined with information recovery of memory after failures. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics.* 2023;23(3):608–617 (in Russ.) DOI: 10.17586/2226-1494-2023-23-3-608-617. EDN:JWPOKM

10. Koucheryavy A., Paramonov A., Makolkina A., Muthanna A. S. A., Vybornova A., Dunaytsev R., et al. 3 Dimension Multilayer Heterogenous Ultra Dense Networks. *Telecom IT*. 2022;10(3):1–12. (in Russ.) DOI:10.31854/2307-1303-2022-10-3-1-12. EDN:LHLYEM

11. Zakharov M.V., Kirichek R.V. Methods of building a super-dense e-health network using edge computing. *Proceedings of the 75th Scientific and Technical Conference of the St.* Petersburg NTO RES named after A.S. Popov, dedicated to Radio Day. Saint-Petersburg: SPbSETU "LETI" Publ.; 2020. p.145–147. (in Russ.) EDN:XVIGBJ

12. Roslyakov A.V., Gerasimov A.V. Deterministic Networks and Their Standardization. *Standards and Quality.* 2024;7:42-47. (in Russ.) DOI:10.35400/0038-9692-2024-7-70-24. EDN:UTBDXB
13. Verzun N., Kolbanev M., Shamin A. The Architecture of the Access Protocols of the Global Infocommunication Resources. *Computers*. 2020;9(2):49. DOI:10.3390/computers9020049. EDN:KJCHRF
14. Verzun N., Kolbanev M., Vorobeva D. Access Control Model to Global Infocommunication Resources. *Proceedings of the Majorov International Conference on Software Engineering and Computer Systems, 12–13 December 2019, Saint Petersburg, Russian Federation, vol.11.* Saint Petersburg: Federal State Autonomous Educational Institution of Higher Education "National Research University ITMO" Publ.; 2020. p.218–221. EDN:RDFFNM
15. Marakulin V.M. *Elements of the theory of cooperative games*. (in Russ.) URL: http://old.math.nsc.ru/~mathecon/Marakulin/CooGAMES.pdf [Accessed 18.06.2025]
16. Gezalov E.B. Model of heterogeneous local communication network with synchronous time access protocol, considering the reliability of its elements. *T-Comm.* 2021;15(3):25–29. (in Russ.) DOI:10.36724/2072-8735-2021-15-2-25-29. EDN:WDTOSM
17. Verzun N.A., Vorobyov A.I., Poimanova E.D. Modeling information transfer process in network with access rights differentiation. *Journal of Instrument Engineering*. 2014;57(9):33–37. (in Russ.) EDN:SMPASB
18. Vishnevsky V.M. *Theoretical foundations of computer network design*. Moscow: Technosphere Publ.; 2003. p. 512. (in Russ.)
19. Wentzel E.S. *Investigation of surgery. Tasks, principles, methodology*. Moscow: Nauka Publ.; 1988. 208 p. (in Russ.)
20. Bellman R., Dreyfus S. *Applied Dynamic Programming*. Princeton: University Press; 1962. DOI:10.1515/9781400874651
21. Rachkov M.Y. *Optimal control in technical systems*. Moscow: Yurait Publ.; 2023. 120 p. (in Russ.)

Статья поступила в редакцию 28.04.2025; одобрена после рецензирования 28.05.2025; принята к публикации 04.06.2025.
The article was submitted 28.04.2025; approved after reviewing 28.05.2025; accepted for publication 04.06.2025.

Информация об авторах:

ВЕРЗУН Наталья Аркадьевна — кандидат технических наук, доцент, доцент кафедры информационных систем Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина)
https://orcid.org/0000-0002-0126-2358

КОЛБАНЁВ Михаил Олегович — доктор технических наук, профессор, профессор кафедры информационных систем Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина)
https://orcid.org/0000-0003-4825-6972

СОВЕТОВ Борис Яковлевич — доктор технических наук, профессор, профессор кафедры информационных систем Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина)
https://orcid.org/0000-0003-3116-8810

Авторы сообщают об отсутствии конфликтов интересов.
The authors declare no conflicts of interests.

Научная статья
УДК 004.023
https://doi.org/10.31854/1813-324X-2025-11-3-108-118
EDN:XTDMRI

Реализация стратегии коллективного восприятия в самоорганизующейся роевой системе с использованием байесовского решающего правила

Игорь Алексеевич Зикратов[1], zikratov.ia@sut.ru
Татьяна Викторовна Зикратова[2] ✉, ztv64@mail.ru
Егор Анатольевич Новиков[1], novikov.ea@sut.ru

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация
[2]Военно-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. *Совершенствование стратегий коллективного восприятия в роевых системах является ключевой задачей для повышения эффективности работы автономных роботизированных групп в сложных и динамичных условиях. Существующие подходы, такие как DMMD, DMVD и DC, обладают ограниченными возможностями при классификации объектов с неочевидными признаками, что требует разработки новых методов.*

Цель исследования: *повышение вероятности восприятия определенных характеристик объекта, исследуемого мультиагентной робототехнической системой.* ***Используемые методы.*** *Предлагаемый критерий использует байесовское решающее правило для пересчета апостериорных вероятностей альтернатив на основе данных, собираемых роботами. Корректность предлагаемых решений подтверждалась имитационным моделированием типовой задачи коллективного восприятия заданного полигона.*

Результаты. *Проведено сравнение с известными стратегиями коллективного восприятия: DMMD, DMVD и DC. Показано, что эти стратегии имеют ограниченные возможности в задачах классификации сложных объектов. Программно реализован сценарий коллективного восприятия в роевой робототехнической системе, состоящей из 20 роботов, обследующих сцену, состоящую из разноцветных плиток. Результаты проведенного эксперимента показали, что использование предлагаемого авторами подхода позволило приобрести рою роботов недостижимые прежде функциональные возможности в стратегии коллективного восприятия для сложных сценариев.* ***Новизна.*** *Предложено выявления свойств исследуемого объекта с использованием статистического критерия. Стратегия основана на квантификации процесса достижения консенсуса членами роя на последовательные такты (шаги), с последующей внутри- и межпериодной обработкой информации, продуцируемой роботами роя. Результаты работы расширяют* ***теоретические основы*** *роевого интеллекта, предлагая новый метод обработки распределенной информации.* ***Практическая значимость*** *заключается в повышении эффективности роевых систем для задач мониторинга, поиска и классификации в медицине, экологии и других областях.*

Ключевые слова: *групповая робототехника, коллектив роботов, роевый интеллект, мультиагентные робототехнические системы, коллективное восприятие, байесовское решающее правило*

Ссылка для цитирования: Зикратов И.А., Зикратова Т.В., Новиков Е.А. Реализация стратегии коллективного восприятия в самоорганизующейся роевой системе с использованием байесовского решающего правила // Труды учебных заведений связи. 2025. Т. 11. № 3. С. 108–118. (in Russ.) DOI:10.31854/1813-324X-2025-11-3-108-118. EDN:XTDMRI

Original research
https://doi.org/10.31854/1813-324X-2025-11-3-108-118
EDN:XTDMRI

Implementation of Collective Perception Strategy in a Self-Organizing Swarm System Using Bayesian Decision Rule

Igor A. Zikratov[1], zikratov.ia@sut.ru
Tatyana V. Zikratova[2], ztv64@mail.ru
Egor A. Novikov[1] ✉, novikov.ea@sut.ru

[1]The Bonch-Bruevich Saint Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation
[2]Naval 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

Relevance. *Improving collective perception strategies in swarm systems is a key challenge for enhancing the efficiency of autonomous robotic groups in complex and dynamic environments. Existing approaches, such as DMMD, DMVD, and DC, have limited capabilities in classifying objects with non-obvious features, necessitating the development of new methods.*
Objective. *Increasing the accuracy of perceiving specific characteristics of an object investigated by a multi-agent robotic system.*
Methods. *The proposed criterion employs a Bayesian decision rule to update the posterior probabilities of alternatives based on data collected by the robots. The validity of the proposed solutions was confirmed through simulation of a typical collective perception task on a defined tested.*
Results. *A comparison was made with established collective perception strategies: DMMD, DMVD, and DC. It was shown that these strategies have limited applicability in classifying complex objects. A software implementation of the collective perception scenario was tested in a swarm robotic system consisting of 20 robots inspecting a scene composed of multicolored tiles. The experimental results demonstrated that the authors' approach endowed the robot swarm with previously unattainable functional capabilities in collective perception for complex scenarios.*
Novelty. *A method for detecting object properties using a statistical criterion was proposed. The strategy quantifies the consensus-building process among swarm members over sequential time steps, followed by intra- and inter-period processing of information generated by the swarm's robots. The results expand the* ***theoretical foundations*** *of swarm intelligence by introducing a new method for processing distributed information.* ***Practical significance*** *lies in improving the efficiency of swarm systems for monitoring, search, and classification tasks in medicine, ecology, and other fields.*

Keywords: *swarm robotics, robot collective, swarm intelligence, multi-agent robotic systems, collective perception, Bayesian decision rule*

For citation: Zikratov I.A., Zikratova T.V., Novikov E.A. Implementation of Collective Perception Strategy in a Self-Organizing Swarm System Using Bayesian Decision Rule. *Proceedings of Telecommunication Universities.* 2025;11(3): 108–118. DOI:10.31854/1813-324X-2025-11-3-108-118. EDN:XTDMRI

Введение

Привлекательность роевой робототехники состоит в том, что в результате локального информационного взаимодействия между отдельными агентами и внешней средой роевой интеллект позволяет решать задачи, стоящие перед сложными техническими системами, относительно простыми средствами [1–3]. Такой подход подразумевает, что вместо высокотехнологичных и дорогостоящих

технических средств достаточно проектировать и использовать примитивные устройства, которые благодаря самоорганизации образовывают высокомасштабируемую и устойчивую к шуму (противодействию) и отказам отдельных компонентов систему [4–6]. Вместе с тем управление большими группами (роями) автономных роботов остается недостаточно изученной проблемой, которая требует новых решений. Ключевыми аспектами стратегии роевого интеллекта являются децентрализация, координация и согласованность, адаптивность, распределенные алгоритмы.

1) Децентрализация – каждый агент действует как самостоятельная единица, принимая решения на основе данных, которые он получает от своих сенсоров и / или от других роботов в пределах своей зоны взаимодействия.

2) Координация и согласованность – роботы должны координировать свои действия, чтобы достичь общей цели, например, выполнить задачу поиска, сбора данных или построения карты. Для этого используются алгоритмы, которые позволяют роботам «договариваться» между собой, например, на основе правил поведения [5, 7].

3) Адаптивность – самоорганизация позволяет рою адаптироваться к изменяющимся условиям, таким как появление новых препятствий и деструктивных воздействий, изменение цели или выход из строя отдельных роботов. Роботы могут перераспределять задачи между собой, чтобы сохранить эффективность работы.

4) Распределенные алгоритмы – используются распределенные алгоритмы, такие как консенсус, флокинг (поведение стаи) или алгоритмы на основе теории игр, чтобы обеспечить согласованное принятие решений.

Следствием реализации указанных аспектов являются появление таких свойств роевых систем, как устойчивость к сбоям, масштабируемость и гибкость. Эти факторы позволяют роям роботов эффективно работать в сложных и динамичных условиях, обеспечивая автономность и устойчивость системы [8, 9].

Совершенствование стратегий управления роями в последние годы идет применительно ко многим типам задач. К ним относятся, например, следующие виды:

– задачи маршрутизации (поиск оптимального пути для группы агентов (например, роботов или дронов) в условиях препятствий или динамически изменяющейся среды, а также координация движения роя в пространстве [10]);

– задачи распределения ресурсов (оптимизация распределения задач между агентами роя, в том числе в условиях энергетических или временны́х ограничений [11, 12]):

– задачи кластеризации, классификации и коллективного восприятия [13–16];

– задачи поиска и слежения (поиск цели в пространстве (например, в рамках поисково-спасательных работ), слежение за движущейся целью в динамической среде [17]);

– задачи координации и синхронизации действий агентов роя (например, синхронное движение или выполнение задач) в условиях ограниченной коммуникации или помех [18, 19].

В этой статье мы предлагаем новую стратегию принятия решений, относящуюся к проблеме коллективного восприятия [20–22], и используем ее для развития ранее предложенных стратегий: прямой модуляции решений, основанных на большинстве (DMMD, *аббр. от англ.* Direct Modulation of Majority-based Decisions) [23], прямой модуляции решений, основанных на голосах избирателей (DMVD, *аббр. от англ.* Direct Modulation of Voter-based Decisions) [24] и прямого сравнения (DC, *аббр. от англ.* Direct Comparison) [13].

В сценарии коллективного восприятия рой роботов используется для исследования среды (объекта) и оценки частоты определенных признаков, которые разбросаны по нему (например, наличие драгоценных металлов, загрязняющих веществ или раковых клеток) с целью определить, какая функция является наиболее частой. Совершенствование алгоритмов роевого управления исследователями направлено на повышение качества принимаемых роем решений (стратегии DMMD и DMVD) или на сокращение временны́х затрат выполнения задачи (стратегия DC).

В свою очередь, повышение качества принимаемых решений может осуществляться либо за счет совершенствования алгоритмов обработки информации, получаемой роботом при исследовании среды «на борту» каждого робота, либо путем совершенствования межагентной обработки информации, предоставляемой агентами в распределенных алгоритмах. Первый путь направлен на то, чтобы робот принимал более обоснованные решения в отношении наблюдаемой среды. Второй путь предполагает повышение эффективности коллективного принятия решения, после обработки «мнений» об объекте исследования всех роботов.

Сокращение временны́х затрат достигается чаще всего с использованием эвристик в распределенных алгоритмах. Так, стратегии DMMD и DMVD предполагают обследование среды всеми агентами, и после окончания такого обследования на втором этапе используется процедура обмена информации между агентами. В результате этой процедуры решения принимаются на основе «мнения» большинства (стратегия DMMD), либо на основе «мнения» случайно отобранных «выборщиков» (стратегия DMVD).

В стратегии DC обмен информацией происходит периодически в процессе обследования среды агентами, по мере накопления этой информации. Тогда к моменту завышения обследования среды коллективное «мнение» о ее свойствах уже оказывается сформированным. Следует отметить, что на практике целью применения роя роботов в сценарии коллективного восприятия может являться отнюдь не только выявление наличия тех или иных признаков, присущих исследуемому объекту. Конечной целью чаще всего является принятие решения – в какой степени эти признаки характеризуют свойства объекта. Например, свидетельствует ли присутствие тех или иных признаков о наличии рака у пациента, или это доброкачественное образование. Такая цель не ставилась в работах [13, 20–24], поэтому в своем исследовании мы провели сравнительный анализ по возможностям классификации сложных сцен известными методами.

Целью данной работы является разработка стратегии, позволяющей, в отличие от известных, не только исследовать свойства предъявленного объекта, но и осуществить его классификацию по результатам коллективного восприятия. Для достижения этой цели авторами реализована стратегия, которая основана на использовании статистических решающих правил «на борту» агента в процессе получения сведений о параметрах среды и непрерывном информировании об этих параметрах всего коллектива.

Проблемный сценарий коллективного восприятия и принятия решения

Применимость той или иной стратегии роевого управления характеризуется не только точностными или временны́ми показателями, но и степенью, в которой она может быть обобщена для различных типовых задач. Высокая степень обобщения предполагает определенный уровень абстрагирования предметной области. С этой целью различными исследователями предложены некоторые виды полигонов – моделей среды – на которых удобно оценивать успешность той или иной стратегии. В частности, задачи коллективного восприятия оказалось удобно исследовать при помощи модели внешней среды, представленной в виде сцены, составленной из множества плиток, раскрашенными несколькими цветами. В работе [13] использовалась двухцветная черно-белая сцена. В работах [25, 26] – сцена, состоящая из 100 плиток, окрашенных в пять цветов (рисунок 1). 40 % плиток окрашены в желтый цвет. На сцене инициируются роботы со случайными начальными координатами и произвольными маршрутами движения. Передвигаясь по сцене, роботы посредством бортовых сенсоров определяют цвет, в который окрашена текущая клетка.

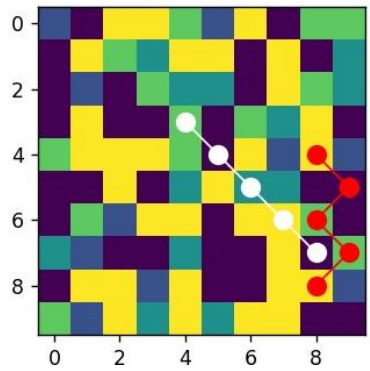


Рис. 1. Маршруты двух роботов по сцене 10×10 [26]

Fig. 1. Routes for 2 Robots in 10×10 Scene [26]

Цель роя состоит в том, чтобы на основе исследования сцены и дальнейшего «обсуждения» определить, клетки какого именно цвета преобладают на сцене, и на основании этого выбрать альтернативу $A_i = A_{opt}$ $(i = 1, 2, \dots, N)$ из конечного числа N доступных альтернатив $(i = 1, 2, \dots, N)$. Здесь под альтернативой понимается тот или иной тип исследуемой сцены, отличающийся от других соотношением цветов, которыми окрашены плитки сцены. Очевидно, что сложность задачи исследования можно варьировать, изменяя соотношение между процентами плиток преобладающего цвета и других цветов.

После запуска итерационного цикла j-й робот $r_j \in R$, где R – множество роботов группы, последовательно обходит плитки сцены, определяя их цвет. При достижении количества итераций j-го робота $k_{r_j}^{\text{ит}}$ заданного числа K, r_j вырабатывает решение в отношении альтернативы A_{ij}^k. Алгоритм действий робота представлен на рисунке 2. Вероятность события $P(A_{ij} = A_{opt})$ зависит от количества клеток разного цвета, встретившихся роботу на пути. Очевидно, что в случае, когда робот исследует все клетки сцены, задача будет решена со 100-процентным результатом в отношении точности. Однако время выполнения задачи в ряде случаев может оказаться неприемлемым.

Авторами было предложено коллективное решение задачи путем извещения о цвете текущей плитки каждым роботом, находящимся в активной стадии итерационного процесса, всех остальных роботов роя (см. рисунок 2 в [26]). На каждой итерации j-й робот получает статус активного агента, перемещается на k-ю соседнюю свободную плитку, оценивает ее свойства (цвет) посредством своих сенсоров, и исходя из оценки свойств, выбирает соответствующую альтернативу A_{ij}^k. Свою оценку свойству (в данном случае – цвету) текущей плитки он сообщает по сети связи членам коллектива $r \in R$, находящимся в пассивной фазе итерационного цикла. В зависимости от расстояния до робота

r_j члены коллектива могут либо принять информацию от него, либо не «услышать» ее в случае неустойчивой радиосвязи. Те роботы, которые приняли информацию, записывают данные о свойстве плитки, на которой находится r_j, в хэш-таблицу, если соответствующая ячейка пустая. Если информация о свойствах какой-то плитки противоречит информации, полученной роботом от своих сенсоров, то приоритет отдается «своим» данным. Статус активного агента поочередно получают все роботы группы.

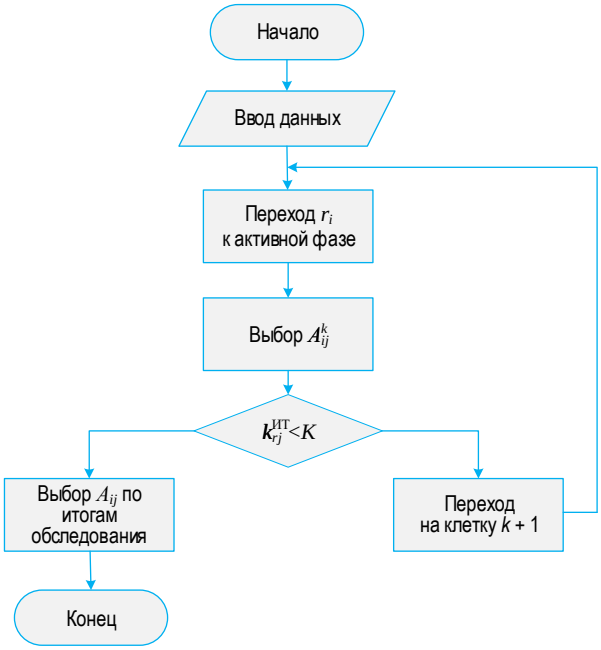


Рис. 2. Итерационный алгоритм обследования сцены одним роботом

Fig. 2. Iterative Algorithm for Scene Exploration by a Single Robot

Такой обмен информацией позволяет сформировать более полное представление каждого робота об окружающей среде, которое выходит за рамки исследованной области, непосредственно самим роботом, что существенно сокращает время обследования сцены.

После каждой итерации роботы на основе анализа всех хэш-таблиц оценивают каждую альтернативу в отношении исследуемой сцены. В стратегиях DMMD, DMVD и DC для этого используется подсчет частоты встречаемости того или иного цвета плитки. Эта операция хорошо отражает искомое сочетание цветов и вычислительно доступна для простейших процессоров, которыми оснащены роботы. Очевидно, чем чаще встречается цвет сцены, тем с большей уверенностью и с меньшим временем принимается коллективное решение о выбранной альтернативе A_i. Однако для случаев, когда доминирование како-либо цвета уменьшается, такой подход требует более тщательного исследования сцены [25].

Авторы предлагают вместо арифметического подсчета частоты встречаемости цветов использовать критерий принятия решения, основанный на байесовском решающем правиле. Проиллюстрируем его работу на примере.

Пусть имеются три возможные альтернативы:

1) альтернатива A_1 – сцена, в которой имеется около 60 % плиток желтого цвета, остальные 40 % плиток распределены поровну между 4 оставшимися цветами;

– альтернатива A_2 – сцена, в которой имеется около 40 % плиток синего цвета, остальные 60 % плиток распределены поровну между 4 оставшимися цветами;

– альтернатива A_3 – сцена, в которой все 5 цветов распределены примерно поровну между всеми плитками.

Рою необходимо исследовать предъявленную сцену, определить соотношение цветов, и принять решение, какой из трех альтернатив она соответствует.

Пусть перед началом исследования известны априорные вероятности альтернатив $P(A_i)$, причем $P(A_1)+P(A_2)+P(A_3)=1$. Априорные вероятности альтернатив и условные вероятности $p(a_m/A_i)$ событий a_m, ($m \in M$, где M – множество цветов сцены) – обнаружение плиток определенного цвета (таблица 1). Значение вероятностей $p(a_m/A_i)$ получены из описания альтернатив.

ТАБЛИЦА 1. Вероятности обнаружения плиток для альтернатив

TABLE 1. Discovery Probabilities for Alternatives

Вид вероятности	A_1	A_2	A_3
$P(A_i)$	$P(A_1)$	$P(A_2)$	$P(A_3)$
$p(a_{\text{желтый}}/A_i)$	0,6	0,15	0,2
$p(a_{\text{синий}}/A_i)$	0,1	0,4	0,2
$p(a_{\text{зеленый}}/A_i)$	0,1	0,15	0,2
$p(a_{\text{фиолетовый}}/A_i)$	0,1	0,15	0,2
$p(a_{\text{голубой}}/A_i)$	0,1	0,15	0,2

В процессе обследования сцены j-м роботом вероятности альтернатив будут повышаться, если факты, обнаруженные этим роботом, поддерживают их, и понижаться в противном случае. Так, например, если на k-й итерации движения j-го робота $P(A_{1j}^k)=P(A_{2j}^k)=0{,}3$, $P(A_{3j}^k)=0{,}4$, и робот, переместившись на очередную плитку, определил ее цвет, происходит пересчет апостериорных вероятностей альтернатив. Если цвет очередной плитки синий, тогда, согласно известной формуле Байеса, вероятности будут равны:

$$p(A_{1j}^k/a_{\text{синий}})=\frac{p\left(\frac{a_{\text{синий}}}{A_1}\right)P(A_1)}{\sum_{i=1}^{3}p\left(\frac{a_{\text{синий}}}{A_i}\right)P(A_i)}=0{,}13, \qquad (1)$$

$$p(A_{2j}^k/a_{\text{синий}}) = \frac{p\left(\frac{a_{\text{синий}}}{A_2}\right)P(A_2)}{\sum_{i=1}^{3} p\left(\frac{a_{\text{синий}}}{A_i}\right)P(A_i)} = 0{,}52, \quad (2)$$

$$p(A_{3j}^k/a_{\text{синий}}) = \frac{p\left(\frac{a_{\text{синий}}}{A_3}\right)P(A_3)}{\sum_{i=1}^{3} p\left(\frac{a_{\text{синий}}}{A_i}\right)P(A_i)} = 0{,}35. \quad (3)$$

Из результатов расчетов видно, что после того, как событие $a_{\text{синий}}$ произошло (на k-й итерации стало известно, что очередная плитка окрашена в синий цвет), доверие j-го робота к альтернативам A_1 и A_3 понизилось, а к A_2 возросло. На следующей итерации пересчет повторяется. При этом априорные вероятности альтернатив на $k + 1$ итерационном шаге принимают значение апостериорных вероятностей альтернатив, вычисленных на k-м шаге.

Очевидно, что согласно алгоритму, представленному в [26] (см. рисунок 2), событие a_m может происходить не только при перемещении j-го робота на очередную плитку в активной стадии, но и нахождении этого робота в пассивной стадии. Соответствующую информацию робот будет получать от активных роботов. В любом случае процедура пересчета апостериорных вероятностей позволяет каждому роботу уточнять текущие альтернативы при поступлении новой информации о свойствах плиток сцены.

Следует учесть, что из-за разных условий радиосвязи информация о свойствах исследуемой сцены, получаемая роботами от активного агента, может отличаться. Вследствие этого решения, принимаемые роботами в отношении выбираемой ими альтернативы, также могут отличаться.

Результаты эксперимента

Для экспериментальной проверки работоспособности предложенной стратегии авторами использовалась имитационная модель, разработанная в работе [26]. Она представляет собой программную реализацию рассмотренного проблемного сценария в среде Phyton с использованием объектно-ориентированного подхода. Целью эксперимента было оценить работоспособность и возможности предложенного статистического критерия для классификации предложенной сцены и сравнить его с возможностями стратегии DC. Рою из 20 роботов предлагались для исследования сцены, состоящие из 100 плиток, которые окрашены в соответствии с одной из трех альтернатив, представленных выше. Оцениваемой величиной являлась оценка гипотез: $H1$ – сцена соответствует альтернативе A_1; $H2$ – сцена соответствует альтернативе A_2; $H3$ – сцена соответствует альтернативе A_3. Соответствующие вероятности рассчитывались после каждой итерации как отношение количества роботов, выбравших $A_{ij}^k = A_{opt}$ к количеству всех роботов роя.

В начале эксперимента генерировалась сцена, соответствующая одной из трех альтернатив со случайным расположением цветов, и роботы случайным образом размещались внутри арены. Траектория движения каждого робота представляется ломаной линией – в своей активной фазе робот чередует движение в произвольно выбранном направлении либо вращение на месте. Направление вращения и движение также выбирается случайным образом. Робот способен принимать извещения только от тех роботов, которые находятся на расстоянии, не превышающем заданную дальность радиосвязи. Площадь зоны покрытия радиосвязи робота задавалась равной либо 20 % площади сцены, либо 80 %. Все роботы при обследовании сцены действовали по единому алгоритму, представленному на рисунке 3.

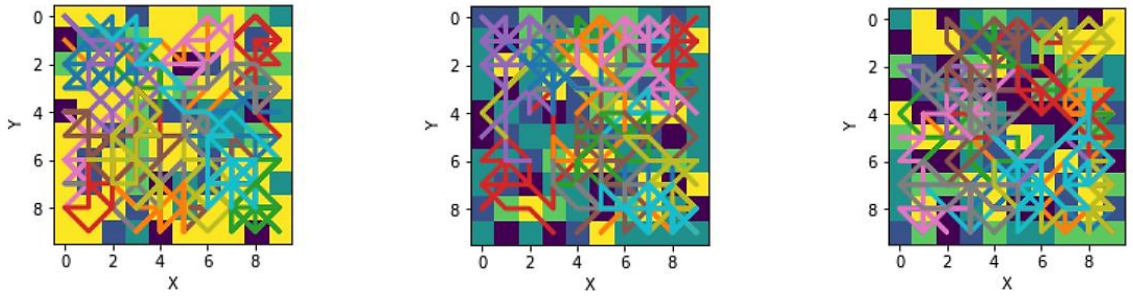
Значение A_{ij}^k вычислялось как с использованием предлагаемого статистического критерия по формулам (1–3), так и подсчетом частоты встречаемости того или иного цвета плитки, в соответствии со стратегиями DMMD, DMVD и DC.

На рисунке 3 представлены экземпляры сцен, содержащей около 60 % плиток желтого цвета, (альтернатива A_1), около 40 % плиток голубого цвета, (альтернатива A_2) и равномерным распределением цветов (альтернатива A_3).

На рисунках 4a и 4b представлены результаты экспериментов, когда расчет вероятности $P(A_{opt})$ осуществлялся при зоне покрытия радиосвязи 20 (слева) и 80 % от площади сцены (справа). На рисунке приведены значения, усредненные по 300 сериям экспериментов. Из рисунка видно, что при наличии доминирующего цвета, использование роем обеих стратегий позволяет за счетное число шагов итерационного процесса с вероятностью, близкой к 1, определить альтернативу A_{opt}. При этом чем больше дальность радиосвязи, тем больше агентов участвуют в информационном обмене, и, как следствие, алгоритм сходится за меньшее число шагов.

На рисунках 4c и 4d представлены результаты экспериментов для тех же условий, но предъявляемая рою сцена соответствовала альтернативе A_2. Несмотря на то, что количество плиток доминирующего цвета уменьшилось, обе стратегии коллективного восприятия также позволили рою получить верное решение. Однако при малой дальности связи сходимость алгоритма ухудшилась.

На рисунках 4e и 4f представлены результаты экспериментов при тех же условиях для альтернативы A_3.



a) b) c)

Рис. 3. Случайные маршруты движения 20 роботов по сцене 10×10 за 25 итерации: a) сцена альтернативы A_1; b) сцена альтернативы A_2; c) сцена альтернативы A_3

Fig. 3. Random Movement Trajectories of 20 Robots across a 10×10 Scene over 25 Iterations: a) Alternative A_1 Scene; b) Alternative A_2 Scene; c) Alternative A_3 Scene

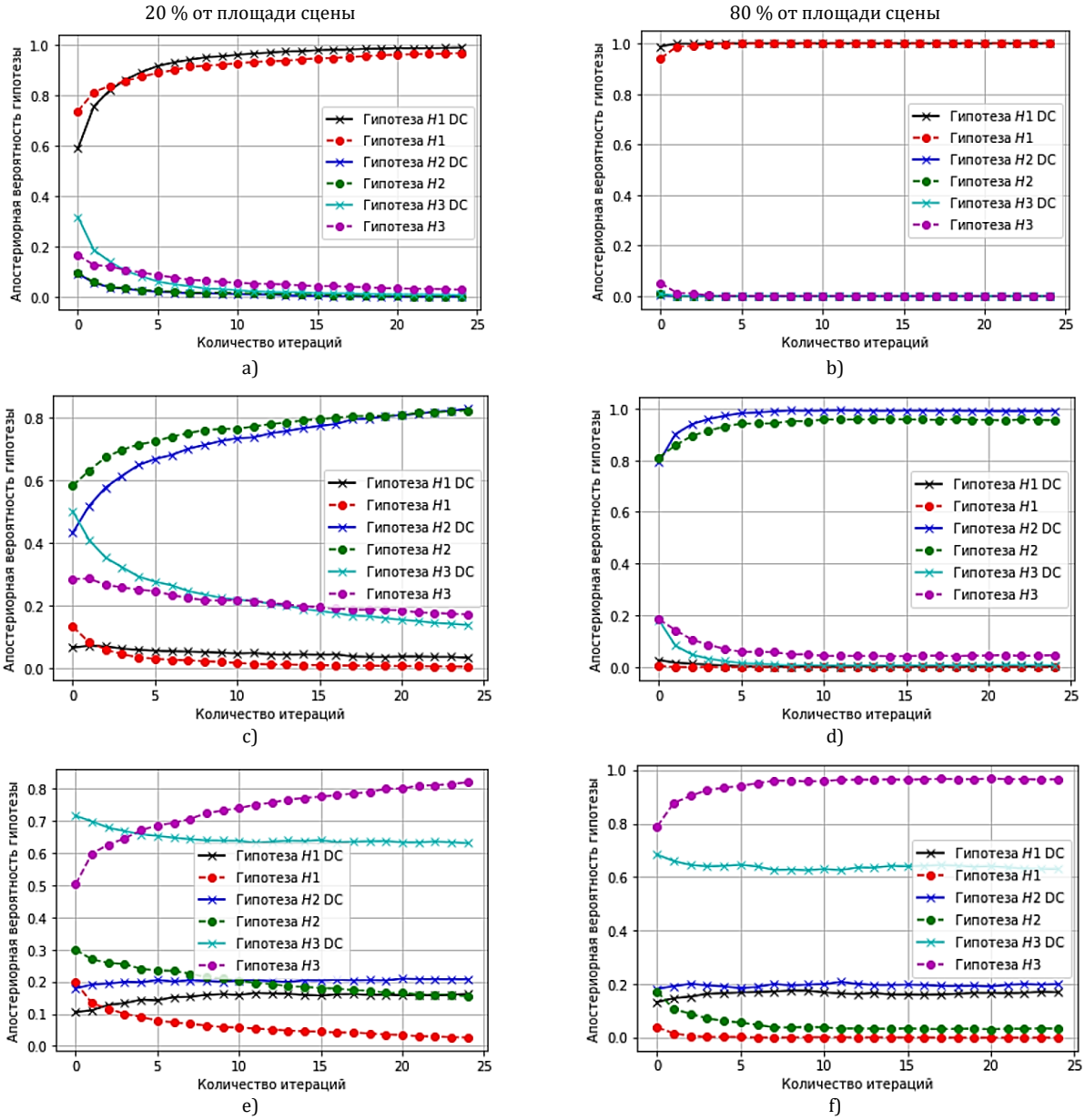
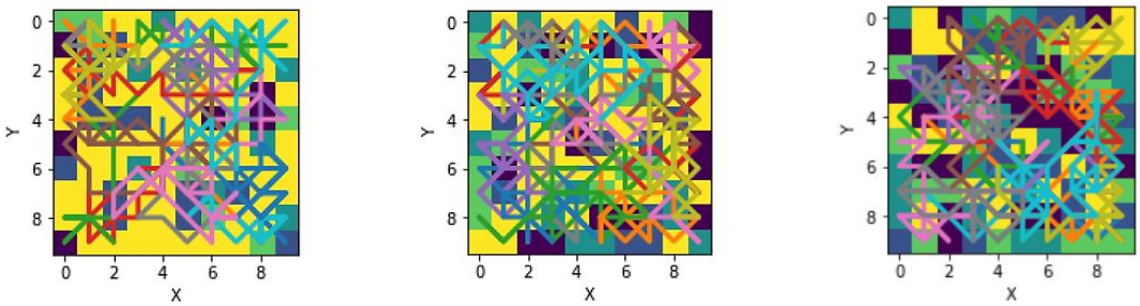


Рис. 4. Оценка результатов коллективного восприятия сцены альтернативы A_1 (a, b), A_2 (c, d), A_3 (e, f) при изменении дальности радиосвязи в рое с использованием стратегии DC и с использованием байесовского решающего правила

Fig. 4. Evaluation of Collective Perception Results for Alternative A_1 (a, b), A_2 (c, d), A_3 (e, f) Scene with Varying Communication Ranges in the Swarm, Comparing DC Strategy and Bayesian Decision Rule

Из графиков (см. рисунок 4) видно, что в отсутствии доминирующего цвета обе стратегии позволили рою верно классифицировать предъявленную сцену. Однако результаты коллективного восприятия более высокие в случае, когда агентами использовалось формулы (1–3). Это проявляется в меньшем количестве итераций, необходимых для схождения алгоритма, а также в более высокой апостериорной вероятности $P(A_{opt})$.

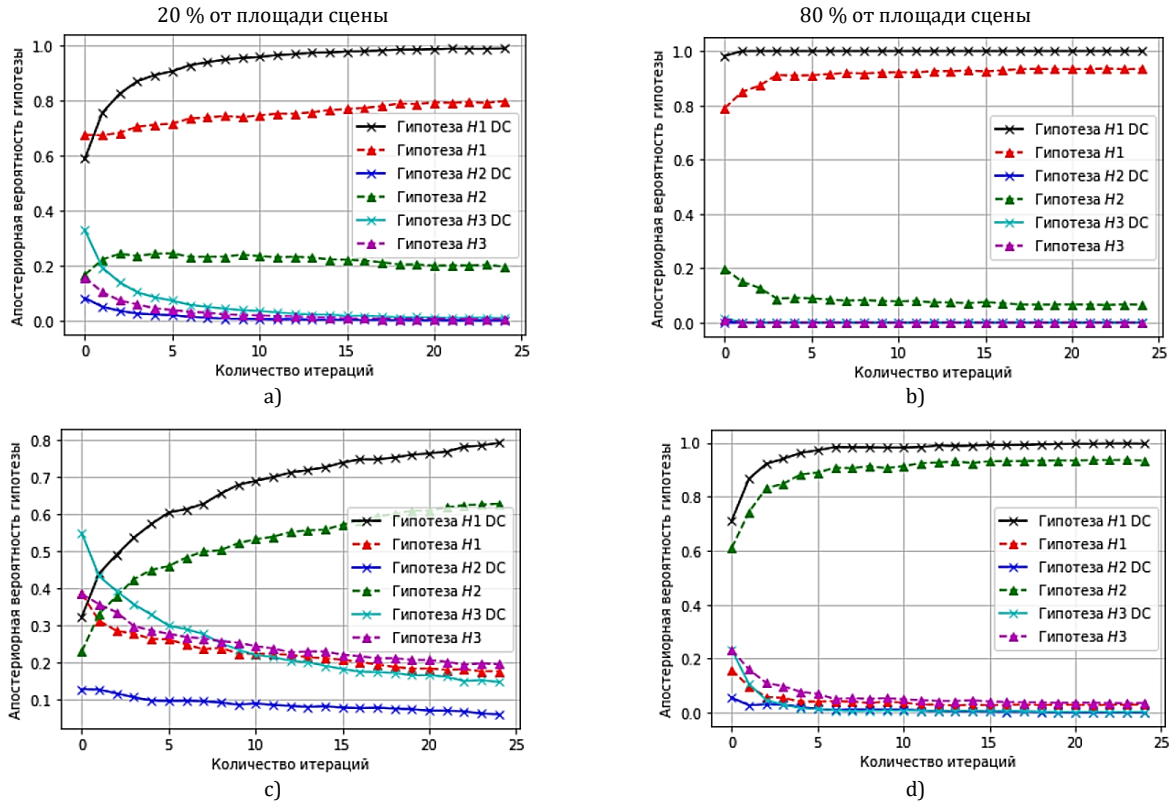
Усложним задачу. При прочих равных условиях изменим содержание альтернатив предъявляемых сцен. Альтернатива A_3 останется прежней, а альтернативы A_1 и A_2 отличаются между собой только концентрацией доминирующего цвета. Доминирующий цвет (желтый) для A_1 и A_2, в отличие от предыдущего случая, один и тот же (рисунок 5). Сложность в этом случае заключается в том, что стратегия коллективного восприятия должна помочь рою не просто выявить доминирующий цвет сцены, но и обеспечить различие его концентрации. В таблице 2 представлены значения условных и априорных вероятностей для такого сценария.



a) b) c)

Рис. 5. Сцены с 60 % концентрацией желтого цвета (альтернатива 1), 40 % концентрацией желтого цвета (альтернатива 2) и равномерным распределением цветов (альтернатива 3): a) A_1; b) A_2; c) A_3

Fig. 5. Scenes with 60 % Yellow Color Concentration (Alternative 1), 40 % Yellow Color Concentration (Alternative 2), and Uniform Color Distribution (Alternative 3): a) A_1; b) A_2; c) A_3



a) b)

c) d)

Рис. 6. Оценка результатов коллективного восприятия сцены для альтернатив A_1 и A_2 при различных концентрациях доминирующего цвета: 20 % (a, c) и 80 % (b, d)

Fig. 6. Evaluation of Collective Perception Results for Alternatives A_1 and A_2 with Different Dominant Color Concentrations: 20 % (a, c) and 80 % (b, d)

ТАБЛИЦА 2. Вероятности обнаружения плиток для модифицированных альтернатив

TABLE 2. Discovery Probabilities for Modified Alternatives

Вид вероятности	A_1	A_2	A_3
$P(A_i)$	0,33	0,33	0,33
$p(a_{\text{желтый}}/A_i)$	0,6	0,4	0,2
$p(a_{\text{синий}}/A_i)$	0,1	0,15	0,2
$p(a_{\text{зеленый}}/A_i)$	0,1	0,15	0,2
$p(a_{\text{фиолетовый}}/A_i)$	0,1	0,15	0,2
$p(a_{\text{голубой}}/A_i)$	0,1	0,15	0,2

На рисунке 6 представлены результаты экспериментов для альтернатив A_1 и A_2.

Как следует из результатов экспериментов, если агенты роя используют подсчет частоты встречаемости доминирующего признака, то стратегия коллективного восприятия не в состоянии различить сцены двух альтернатив A_1 и A_2. Однако использование агентами байесовского решающего правила позволило успешно решить эту задачу, что свидетельствует о появлении новых возможностей роевого интеллекта в решении проблем коллективного восприятия.

Оценка вычислительной сложности алгоритмов проводилась экспериментально, путем измерения времени, необходимого для достижения заданного уровня апостериорной вероятности гипотез, с последующим усреднением по 300 сериям. Оценка показала, что время в большей степени зависит от начального расположения агентов на сцене, их географии их маршрутов и расположения плиток, и пренебрежимо мало, на уровне статистической погрешности, зависит от незначительного усложнения вычислительной процедуры «на борту» агента.

Список источников

1. Dorigo M., et al. Swarm robotics // Scholarpedia. 2014;9(1):1463. DOI:10.4249/scholarpedia.1463
2. Campo A., Garnier S., Dedriche O., Zekkri M., Dorigo M. Self-Organized Discrimination of Resources // PLoS ONE. 2011. Vol. 6. Iss. 5. P. e19888. DOI:10.1371/journal.pone.0019888
3. Sailor M.J., Link J.R. “Smart dust”: nanostructured devices in a grain of sand // Chemical Communications. 2005. Iss. 11. P. 1375. DOI:10.1039/b417554a. EDN:MHMXGT
4. Montes de Oca M.A., Ferrante E., Scheidler A., Pinciroli C., Birattari M., Dorigo M. Majority-rule opinion dynamics with differential latency: a mechanism for self-organized collective decision-making // Swarm Intelligence. 2011. Vol. 5. Iss. 3-4. PP. 305–327. DOI:10.1007/s11721-011-0062-z. EDN:GHZZLS
5. 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
6. Карпов В.Э. Социальные сообщества роботов: от реактивных к когнитивным агентам // Мягкие измерения и вычисления. 2019. № 2(15). С. 61–78. EDN:SEFEFV
7. Зикратов И.А., Викснин И.И., Зикратова Т.В. Мультиагентное планирование проезда перекрестка дорог беспилотными транспортными средствами // Научно-технический вестник информационных технологий, механики и оптики. 2016. Т. 16. № 5. С. 839–849. DOI:10.17586/2226-1494-2016-16-5-839-849. EDN:WRPHSP
8. Юрьева Р.А., Комаров И.И., Викснин И.И. Иммунологические принципы принятия решения в мультиагентных робототехнических системах // Глобальный научный потенциал. 2015. Т. 5. № 50. С. 87–91. EDN:UKOVSB
9. Strobel V., Ferrer E.C., Dorigo M. Managing Byzantine Robots via Blockchain Technology in a Swarm Robotics Collective Decision Making Scenario // Proceedings of the 17th International Conference on Autonomous Agents and Multiagent Systems (AAMAS '14, Stockholm Sweden, 10–15 July 2018). IFAAMAS, 2018. PP. 541–549.
10. Иванов Д.Я. Методы роевого интеллекта для управления группами малоразмерных беспилотных летательных аппаратов // Известия ЮФУ. Технические науки. 2011. № 3(116). С. 221–229. EDN:NPKHEP
11. Каляев И.А., Гайдук А.Р., Капустян С.Г. Модели и алгоритмы коллективного управления в группах роботов. М.: ФИЗМАТЛИТ, 2009. 280 с. EDN:MUWSIT
12. Саенко И.Б., Соколов А.П., Лаута О.С., Губский П.М. Методика целераспределения при групповом полете мини-БПЛА к целям // Информация и космос. 2024. № 2. С. 113–120. EDN:CGIZBA
13. Valentini G., Brambilla D., Hamann H., Dorigo M. Collective Perception of Environmental Features in a Robot Swarm // Proceedings of the 10th International Conference on Swarm Intelligence (Brussels, Belgium, 7–9 September 2016). Lecture Notes in Computer Science. Cham: Springer, 2016. Vol. 9882. PP. 65–76. DOI:10.1007/978-3-319-44427-7_6
14. Fagiolini A., Pellinacci M., Valenti G., Dini G., Bicchi A. Consensus-based distributed intrusion detection for multi-robot systems // Proceedings of the International Conference on Robotics and Automation (ICRA 2008, Pasadena, USA, 19–23 May 2008). PP. 120–127. DOI:10.1109/ROBOT.2008.4543196
15. Valentini G., Hamann H. Time-variant feedback processes in collective decision-making systems: influence and effect of dynamic neighborhood sizes // Swarm Intelligence. 2015. Vol. 9. PP. 153–176. DOI:10.1007/s11721-015-0108-8
16. Reina A., Valentini G., Hamann H., Dorigo M. A Design Pattern for Decentralised Decision Making // PLoS ONE. 2015. Vol. 10. DOI:10.1371/journal.pone.0140950
17. Зикратов И.А., Зикратова Т.В. Использование поведенческих моделей для исследования социумов роботов // Информация и космос. 2022. № 4. С. 170–174. EDN:DQASLC
18. 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

19. Valentini G. Indirect Modulation of Majority-Based Decisions // Studies in Computational Intelligence. 2017. Vol. 706. PP. 55–66. DOI:10.1007/978-3-319-53609-5_4

20. Valentini G., Hamann H., Dorigo M. Efficient Decision-Making in a Self-Organizing Robot Swarm: On the Speed Versus Accuracy Trade-Off // Proceedings of the 14th International Conference on Autonomous Agents and Multiagent Systems (AAMAS '15, Istanbul, Turkey, 4–8 May 2015). IFAAMAS, 2015. PP. 1305–1314.

21. Valentini G., Hamann H., Dorigo M. Self-organized collective decision making: the weighted voter model // Proceedings of the 13th International Conference on Autonomous Agents and Multiagent Systems (AAMAS '14, Paris, France, 5–9 May 2014). IFAAMAS, 2014. PP. 45–52.

22. Valentini G. Achieving Consensus in Robot Swarms // Studies in Computational Intelligence. 2017. Vol. 706. DOI:10.1007/978-3-319-53609-5

23. Valentini G., Ferrante E., Hamann H., Dorigo M. Collective decision with 100~Kilobots: speed versus accuracy in binary discrimination problems // Autonomous Agents and Multi-Agent Systems. 2015. Vol. 30. Iss. 3. PP. 553–580. DOI:10.1007/s10458-015-9323-3

24. Valentini G., Hamann H., Dorigo M. Self-Organized Collective Decision-Making in a 100-Robot Swarm // Twenty-Ninth AAAI Conference on Artificial Intelligence. 2015. Vol. 29. Iss. 1. DOI:10.1609/aaai.v29i1.9720

25. 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

26. 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

References

1. Dorigo M., et al. Swarm robotics. *Scholarpedia*. 2014;9(1):1463. DOI:10.4249/scholarpedia.1463

2. Campo A., Garnier S., Dedriche O., Zekkri M., Dorigo M. Self-Organized Discrimination of Resources. *PLoS ONE*. 2011;6(5): e19888. DOI:10.1371/journal.pone.0019888

3. Sailor M.J., Link J.R. “Smart dust”: nanostructured devices in a grain of sand. *Chemical Communications*. 2005;11;1375. DOI:10.1039/b417554a. EDN:MHMXGT

4. Montes de Oca M.A., Ferrante E., Scheidler A., Pinciroli C., Birattari M., Dorigo M. Majority-rule opinion dynamics with differential latency: a mechanism for self-organized collective decision-making. *Swarm Intelligence*. 2011;5(3-4):305–327. DOI:10.1007/s11721-011-0062-z. EDN:GHZZLS

5. 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

6. 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

7. Zikratov I.A., Viksnin I.I., Zikratova T.V. Multiagent Planning of Intersection Passage by Autonomous Vehicles. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*. 2016;16(5):839–849. (in Russ.) EDN:WRPHSP

8. 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

9. Strobel V., Ferrer E.C., Dorigo M. Managing Byzantine Robots via Blockchain Technology in a Swarm Robotics Collective Decision Making Scenario. *Proceedings of the 17th International Conference on Autonomous Agents and Multiagent Systems, AAMAS '14, 10–15 July 2018, Stockholm Sweden*. IFAAMAS; 2018. p.541–549.

10. Ivanov D.Ya. Methods of Swarm Intelligence for Control of Groups Of Small-Sized Unmanned Aerial Vehicles. *Izvestiya SFedU. Engineering Sciences*. 2011;3(116):221–229. (in Russ.) EDN:NPKHEP

11. Kalyaev I.A., Gaiduk A.R., Kapustyan S.G. *Models and algorithms for collective control in robot groups*. Moscow: FIZMATLIT Publ.; 2009. 280 p. (in Russ.) EDN:MUWSIT

12. Saenko I., Sokolov A., Lauta O., Gubsky P. Method of Target Distribution During Group Flight of Mini-UAVs to Targets. *Information and Space*. 2024;2:113–120. (in Russ.) EDN:CGIZBA

13. Valentini G., Brambilla D., Hamann H., Dorigo M. Collective Perception of Environmental Features in a Robot Swarm. *Proceedings of the 10th International Conference on Swarm Intelligence, 7–9 September 2016, Brussels, Belgium. Lecture Notes in Computer Science, vol.9882*. Cham: Springer; 2016. p.65–76. DOI:10.1007/978-3-319-44427-7_6

14. Fagiolini A., Pellinacci M., Valenti G., Dini G., Bicchi A. Consensus-based distributed intrusion detection for multi-robot systems. *Proceedings of the International Conference on Robotics and Automation, ICRA 2008, 19–23 May 2008, Pasadena, USA*. p.120–127. DOI:10.1109/ROBOT.2008.4543196

15. Valentini G., Hamann H. Time-variant feedback processes in collective decision-making systems: influence and effect of dynamic neighborhood sizes. *Swarm Intelligence*. 2015;9:153–176. DOI:10.1007/s11721-015-0108-8

16. Reina A., Valentini G., Hamann H., Dorigo M. A Design Pattern for Decentralised Decision Making. *PLoS ONE*. 2015;10. DOI:10.1371/journal.pone.0140950

17. Zikratov I.A., Zikratova T.V. Using Behavioral Models to Study Robot Societies. *Information and Space*. 2022;4:170–174. (in Russ.) EDN:DQASLC

18. Zikratova T.V. 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

19. Valentini G. Indirect Modulation of Majority-Based Decisions. *Studies in Computational Intelligence*. 2017;706:55–66. DOI:10.1007/978-3-319-53609-5_4

20. Valentini G., Hamann H., Dorigo M. Efficient Decision-Making in a Self-Organizing Robot Swarm: On the Speed Versus Accuracy Trade-Off. *Proceedings of the 14th International Conference on Autonomous Agents and Multiagent Systems, AAMAS '15, 4–8 May 2015, Istanbul, Turkey*. IFAAMAS; 2015. p.1305–1314

21. Valentini G., Hamann H., Dorigo M. Self-organized collective decision making: the weighted voter model. *Proceedings of the 13th International Conference on Autonomous Agents and Multiagent Systems, AAMAS '14, 5–9 May 2014, Paris, France*. IFAAMAS; 2014. p.45–52.

22. Valentini G. Achieving Consensus in Robot Swarms. *Studies in Computational Intelligence.* 2017;706. DOI:10.1007/978-3-319-53609-5

23. Valentini G., Ferrante E., Hamann H., Dorigo M. Collective decision with 100~Kilobots: speed versus accuracy in binary discrimination problems. *Autonomous Agents and Multi-Agent Systems*. 2015;30(3):553–580. DOI:10.1007/s10458-015-9323-3

24. Valentini G., Hamann H., Dorigo M. Self-Organized Collective Decision-Making in a 100-Robot Swarm. *Twenty-Ninth AAAI Conference on Artificial Intelligence*. 2015;29(1). DOI:10.1609/aaai.v29i1.9720

25. Ryabtsev S.S. A Method for Detecting Byzantine Robots Based on Data from the Collective Decision-Making Process in Swarm Robotic Systems. *Control, Communication and Security Systems*. 2022;3:105–137. (in Russ.) DOI:10.24412/2410-9916-2022-3-105-137. EDN:SVSCHG

26. 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

Статья поступила в редакцию 14.04.2025; одобрена после рецензирования 03.06.2025; принята к публикации 04.06.2025.
The article was submitted 14.04.2025; approved after reviewing 03.06.2025; accepted for publication 04.06.2025.

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
кандидат технических наук, 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 004.421
https://doi.org/10.31854/1813-324X-2025-11-3-119-128
EDN:UMCIKU

Использование криптографических алгоритмов для создания временного пропуска за счет технологии генерации QR-кодов

Юлия Юрьевна Калинина✉, jilietka@mail.ru
Юлия Александровна Смирнова, got-22@mail.ru

Астраханский государственный университет им. В.Н. Татищева,
Астрахань, 414056, Российская Федерация

Аннотация

В современных условиях безопасность высших учебных заведений требует комплексного подхода, включающего как физическую защиту, так и кибербезопасность. С ростом числа студентов, преподавателей и посетителей, а также увеличением угроз, таких как терроризм, вандализм и кибератаки, актуальной задачей становится внедрение эффективных систем контроля доступа. Одним из перспективных решений является система мониторинга временных пропусков на основе QR-кодов, обеспечивающая не только ограничение несанкционированного доступа, но и сбор данных о передвижении лиц на территории учебного заведения. ***Целью*** *данного исследования является разработка методики применения QR-кодов в системах контроля доступа высших учебных заведений с использованием современных криптографических алгоритмов, включая симметричное шифрование (AES-256), асимметричную криптографию на эллиптических кривых (ECC).*

Сущность *предлагаемого решения заключается в автоматизированной системе, включающей: электронные заявки на пропуск; автоматическую генерацию QR-кодов с зашифрованными данными; контроль сроков действия пропусков; мониторинг нарушений и интеграцию с Telegram-ботом для удобства пользователей. Принцип описанной методики* ***основан*** *на шифровании метаданных пропуска с последующей генерацией QR-кода, который может быть считан и проверен службой безопасности. Для обеспечения высокой степени защиты применяются алгоритмы AES-256 и ECC.*

Научная новизна *решения заключается в комбинированном использовании QR-кодов и современных криптографических методов, что обеспечивает высокий уровень безопасности и удобство применения в условиях высшего учебного заведения.*

Теоретическая значимость *работы состоит в разработке модели системы контроля доступа, адаптированной для образовательных учреждений, с учетом современных угроз и требований нормативных документов (например, Указа Президента РФ № 166 от 30.03.2022).*

Практическая значимость *подтверждается возможностью непосредственного внедрения системы в учебных заведениях. Решение позволяет не только повысить уровень безопасности, но и оптимизировать административные процессы за счет автоматизации выдачи пропусков и интеграции с мессенджером Telegram.*

Ключевые слова: *временные пропуска, контроль доступа, QR-код, шифрование AES-256, криптография на основе эллиптических кривых, автоматизация выдачи пропусков, комплексная безопасность, автоматизация выдачи пропусков*

Ссылка для цитирования: Калинина Ю.Ю., Смирнова Ю.А. Использование криптографических алгоритмов для создания временного пропуска за счет технологии генерации QR-кодов // Труды учебных заведений связи. 2025. Т. 11. № 3. С. 119–128. DOI:10.31854/1813-324X-2025-11-3-119-128. EDN:UMCIKU

Original article
https://doi.org/10.31854/1813-324X-2025-11-3-119-128
EDN:UMCIKU

Using Cryptographic Algorithms to Create a Temporary Pass Using QR Code Generation Technology

Yulia Yu. Kalinina ✉, jilietka@mail.ru
Yulia A. Smirnova, got-22@mail.ru

Tatishchev astrakhan state university,
Astrakhan, 414056, Russian Federation

Annotation

In modern conditions, the security of higher education institutions requires an integrated approach, including both physical protection and cybersecurity. With the growing number of students, faculty, and visitors, as well as increasing threats such as terrorism, vandalism, and cyberattacks, the implementation of effective access control systems is becoming an urgent task. One of the promising solutions is a system for monitoring temporary passes based on QR codes, which ensures not only the restriction of unauthorized access, but also the collection of data on the movement of persons on the territory of the educational institution. ***The purpose*** *of this study is to develop a methodology for using QR codes in access control systems of higher education institutions using modern cryptographic algorithms, including symmetric encryption (AES-256), asymmetric elliptic curve cryptography (ECC).*
The essence *of the proposed solution is an automated system that includes: electronic applications for admission; automatic; QR code generation.codes with encrypted data; control of the validity period of passes; monitoring violations and integration with the Telegram bot for the convenience of users. The principle of the described technique is* ***based on*** *the encryption of the metadata of the pass, followed by the generation of a QR code that can be read and verified by the security service. AES-256 and ECC algorithms are used to ensure a high degree of protection.*
The scientific novelty *of the solution lies in the combined use of QR codes and modern cryptographic methods, which ensures a high level of security and ease of use in a university setting.*
The theoretical significance *of the work consists in developing a model of an access control system adapted for educational institutions, taking into account modern threats and requirements of regulatory documents (for example, Decree of the President of the Russian Federation No. 166 dated 30.03.2022).*
The practical significance *is confirmed by the possibility of direct implementation of the system in educational institutions. The solution allows not only to increase the level of security, but also to optimize administrative processes by automating the issuance of passes and integrating with the Telegram messenger.*

Keywords: *temporary passes, access control, QR code, AES-256 encryption, elliptic curve cryptography, pass issuance automation, integrated security, pass issuance automation*

For citation: Kalinina Yu.Y., Smirnova Yu.A, Using Cryptographic Algorithms to Create a Temporary Pass Using QR Code Generation Technology. *Proceedings of Telecommunication Universities.* 2025;11(3):119–128. (in Russ.) DOI:10.31854/1813-324X-2025-11-3-119-128. EDN:UMCIKU

Введение

Системы безопасности в высших учебных заведениях (вузах) являются одной из ключевых задач и, согласно ГОСТ Р 53704-2009 [1], требуют комплексного подхода, что предполагает объединение разнообразных технических средств и организационных мер для достижения оптимального уровня защиты. Указанный стандарт регламентирует общие технические требования к системам безопасности, охватывающие видеонаблюдение, контроль доступа, пожарную и охранную сигнализацию, а также методы их испытаний и эксплуатации. В связи с увеличением числа студентов, преподавателей и посетителей, а также с ростом угроз безопасности, таких как

терроризм, вандализм и кибератаки, необходимость в эффективных системах безопасности становится все более актуальной. В условиях современного мира, где угрозы могут возникнуть в любой момент, создание безопасной образовательной среды становится приоритетом для всех учебных заведений.

Одним из важных аспектов обеспечения безопасности является контроль доступа, который можно реализовать через систему мониторинга временных пропусков. Эта система позволяет не только ограничить доступ к определенным зонам, но и отслеживать передвижение людей по территории учебного заведения. Внедрение современных технологий, таких как биометрические системы и электронные карты, значительно повышает уровень безопасности, позволяя быстро реагировать на потенциальные угрозы.

Важно отметить, что в связи с указом Президента РФ от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» вузы имеют возможность развивать отечественные решения в области безопасности, что не только обеспечивает систему защитой, но и способствует развитию местной экономики. Например, ряд университетов уже внедряет системы, разработанные российскими компаниями, что позволяет не только повысить уровень безопасности, но и поддержать отечественного производителя. Кроме того, важным элементом безопасности является обучение студентов и сотрудников правилам поведения в экстренных ситуациях. Проведение регулярных тренингов и семинаров по безопасности, а также информирование о возможных угрозах и способах их предотвращения способствует созданию более безопасной образовательной среды.

Комплексный подход к безопасности в вузах включает в себя не только технические решения, но и образовательные инициативы, направленные на повышение осведомленности и готовности всех участников учебного процесса. Это позволит создать безопасную и комфортную атмосферу для обучения и работы, что, в свою очередь, будет способствовать успешному развитию учебного заведения.

Проблематика безопасности в вузах

Вузы сталкиваются с различными угрозами, которые могут повлиять на безопасность студентов и сотрудников. Физические угрозы безопасности могут принимать различные формы и представляют собой серьезную опасность для студентов, преподавателей и инфраструктуры [2]. К числу таких угроз относятся терроризм, вандализм, физическое насилие, кражи и грабежи, пожары и чрезвычайные ситуации.

В последние годы участились случаи *террористических актов* в учебных заведениях – как физические атаки, так и угрозы, связанные с взрывчатыми веществами. Важно, чтобы вузы имели четкие планы действий в случае возникновения таких ситуаций, включая эвакуацию и взаимодействие с правоохранительными органами.

Вандализм может проявляться в повреждении имущества, граффити и других формах разрушения. Это не только приводит к финансовым потерям, но и создает неблагоприятную атмосферу в учебном заведении. Необходимо проводить профилактические мероприятия и вовлекать студентов в поддержание порядка.

Конфликты между студентами, случаи буллинга и другие формы *физического насилия* могут негативно сказаться на учебном процессе и психоэмоциональном состоянии учащихся. Вузы должны иметь программы по предотвращению насилия и поддержке пострадавших.

С увеличением числа студентов и посетителей возрастает риск *краж и грабежей* на территории учебного заведения. Установка камер видеонаблюдения и присутствие охраны могут помочь в снижении этого риска.

Пожары, наводнения и другие природные катастрофы могут угрожать безопасности студентов и сотрудников. Крайне важно иметь в вузах планы по эвакуации и проводить регулярные тренировки для подготовки к таким ситуациям.

В контексте обеспечения безопасности в вузах необходимо руководствоваться рядом государственных стандартов, которые играют ключевую роль в создании надежных систем безопасности, способных эффективно реагировать на современные вызовы и угрозы. ГОСТ Р ИСО/МЭК 17799-2005 [3] предоставляет рекомендации по управлению информационной безопасностью, включая политики, процедуры и практики, направленные на защиту информации. ГОСТ 34.003-90 [4] устанавливает требования к автоматизированным системам, включая их разработку, внедрение и эксплуатацию, что способствует созданию надежных и безопасных систем, которые могут быть использованы для управления безопасностью в вузах.

Соблюдение описанных стандартов обеспечивает защиту как физической, так и цифровой инфраструктуры учебных заведений, способствуя созданию безопасной и комфортной атмосферы для работы и обучения, а также способствует повышению уровня осведомленности и готовности всех участников образовательного процесса, что, в свою очередь, будет способствовать эффективному

управлению угрозами и минимизации рисков, обеспечивая защиту данных и инфраструктуры.

Для эффективного управления физическими угрозами безопасности в вузах необходимо внедрение комплексных систем безопасности (КСБ). КСБ – это комплекс технических средств, защищающих жизнь и здоровье персонала и посетителей, предотвращающих несанкционированное проникновение на охраняемую территорию, обеспечивающих сохранность материальных ценностей [5]. В рамках предметной области акцент делается на технические вспомогательные средства, так как они представляют собой ключевой элемент в обеспечении безопасности, минимизируя человеческий фактор и повышая общую эффективность систем. Аспекты КСБ, рассматриваемые в исследовании, представлены на рисунке 1.

Рис. 1. Аспекты комплексной системы безопасности

Fig. 1. Aspects of the Integrated Security System

В современных реалиях безопасности вузов киберугрозы играют не менее важную роль, чем физические [6]. С увеличением зависимости от технологий и цифровых систем вузы сталкиваются с новыми вызовами, связанными с защитой информации, конфиденциальностью данных и обеспечением эффективного пропускного режима.

С ростом числа студентов и преподавателей, а также с распространением онлайн-обучения и удаленных рабочих мест, соответственно увеличивается доступ к различным данным и системам вузов. Атаки на информационные системы могут включать в себя фишинг, установку вредоносного ПО и DDoS-атаки. Киберпреступники нацеливаются на учебные заведения, чтобы получить доступ к личной информации студентов и сотрудников, финансовым данным, а также для осуществления шантажа и вымогательства. Для защиты от таких угроз вузам необходимо внедрять современные системы контроля доступа, которые обеспечивают не только физическую безопасность, но и защищают данные на уровне информационной системы.

Системы мониторинга временных пропусков становятся важным инструментом для предотвращения несанкционированного доступа как в физическую инфраструктуру учебного заведения, так и к его цифровым ресурсам.

Интеграция системы мониторинга временных пропусков

Наиболее эффективным инструментом для повышения безопасности является система генерации [7] и мониторинга временных пропусков. Данные системы позволяют контролировать доступ на территорию вуза и отслеживать передвижение людей, что особенно актуально в условиях увеличения числа студентов и сотрудников, а также растущих угроз безопасности.

Преимущества предлагаемой системы:

1) улучшение контроля доступа: система обеспечивает выдачу временных пропусков только тем лицам, которые имеют на это право, что значительно снижает риск несанкционированного проникновения на территорию вуза; это достигается за счет использования современных технологий идентификации, таких как бесконтактные карты и биометрические системы;

2) сбор данных о передвижении: система может фиксировать время и место входа и выхода пользователей, что позволяет анализировать потоки людей; это особенно полезно для выявления аномалий или подозрительного поведения, т. е. может помочь в предотвращении инцидентов;

3) автоматические уведомления о нарушениях: в случае попытки несанкционированного доступа система может автоматически предупреждать охрану или других ответственных лиц; это позволяет быстро реагировать на потенциальные угрозы и повышает общую безопасность;

4) аналитика и отчеты: система может предоставлять отчеты о перемещениях пользователей, что позволяет администрации вуза анализировать данные и принимать обоснованные решения для улучшения безопасности.

В рамках интеграции системы мониторинга временных пропусков следует выделить несколько ключевых компонентов, являющихся основополагающими для эффективности системы:

– электронные заявки на пропуск (модуль позволяет сократить бумажный документооборот и ускорить процесс оформления пропусков; пользователи могут подавать заявки через специальные электронные формы, что значительно упрощает процесс согласования);

– автоматизация выдачи пропусков (система обеспечивает автоматическую генерацию временных пропусков с необходимой информацией: ФИО, фотография, должность и данные транспортного

средства; это позволяет быстро и эффективно выдавать пропуска без необходимости ручного ввода данных);

– контроль сроков доступа (модуль контроля сроков доступа отслеживает актуальность пропускных документов и уведомляет ответственных лиц о необходимости их продления; если документы не были продлены вовремя, доступ автоматически блокируется, что предотвращает несанкционированный вход);

– управление нарушениями (система ведет реестр нарушителей и нежелательных посетителей, фиксируя случаи нарушения пропускного режима; это позволяет оперативно реагировать на инциденты и блокировать им доступ);

– личные кабинеты пользователей (система предоставляет личные кабинеты для пользователей и сотрудников отдела безопасности, что упрощает процесс заказа и продления пропусков; посетители могут самостоятельно управлять своими заявками, а сотрудники получают возможность проверять информацию без необходимости сбора множества документов);

– генерация пропуска (система автоматически генерирует пропуск посетителю, если его заявка не требует дополнительной проверки сотрудником службы безопасности в случае предоставления определенных прав; пропуском является QR-код, содержащий основную информацию о посетителе и обоснование легитимности нахождения на территории университета).

Данные компоненты образуют комплексную систему, позволяющую не только организовать упрощенный процесс выдачи временных пропусков, но и значительно повысить уровень безопасности в учебном заведении. Наглядное представление архитектуры системы представлено на рисунке 2. Внедрение этих модулей станет важным шагом к обеспечению эффективного контроля доступа и управлению пропускным режимом.

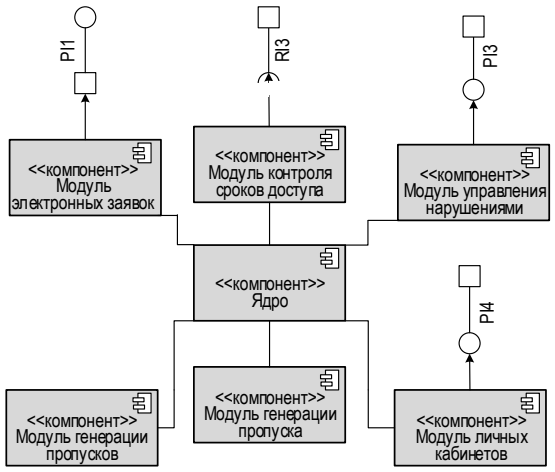


Рис. 2. Диаграмма компонентов UML

Fig. 2. UML Component Diagram

Использование QR-кодов в системе генерации временных пропусков

Современные технологии, такие как биометрические системы распознавания, карты доступа и многофакторная аутентификация, позволяют значительно увеличить уровень безопасности, что не только ограничивает доступ к ресурсам, но и защищает от потенциальных киберугроз, связанных с уязвимостями системы аутентификации и идентификации. Среди новейших технологий QR-коды являются эффективным и универсальным решением для генерации временных пропусков. QR-код (*от англ.* Quick Response code) – разновидность двумерных штриховых кодов, хранящий информацию в виде матрицы из черных и белых квадратов [8]. В отличие от традиционных штрих-кодов, могут хранить данные как горизонтально, так и вертикально, что позволяет поместить значительно больше информации, которая, как правило, представлена текстом, URL-адресами, контактной информацией и другими данными. QR-коды все чаще используются в качестве временных и разовых пропусков из-за простоты генерации, универсальности и совместимости с большим количеством современных устройств.

Основываясь на стандартах Российской Федерации, ключевым документом, определяющим технические требования к QR-кодам, является ГОСТ Р ИСО/МЭК 18004-2015 [9], который является полным аналогом международного ISO/IEC 18004 [10] и устанавливает единые требования к структуре кода, алгоритмам кодирования данных, методам коррекции ошибок и параметрам визуального представления. Стандарт регламентирует форматы данных, возможные версии кода, уровни коррекции ошибок, требования к размерам и алгоритмы маскирования. При этом ГОСТ не ограничивает сферы применения QR-кодов, что позволяет использовать их в различных областях.

Современные QR-коды можно разделить на несколько основных типов, в зависимости от структуры и максимального объема хранимой информации [11]:

– QR-код Модель 1 и Модель 2 – наиболее распространенный формат, поддерживающий кодирование до 7089 цифровых или 4296 буквенных символов (широко применяется в коммерческих и промышленных решениях);

– Micro QR – компактная версия, предназначенная для кодирования небольшого объема данных (до 35 цифровых символов); используются в условиях ограниченного пространства, например, при производстве и инвентаризации мелкогабаритных изделий, в том числе в машинном оборудовании;

– iQR-код – усовершенствованная версия, разработанная для увеличения плотности данных (до 40 тысяч цифровых символов) и поддержки как

квадратной, так и прямоугольной формы; данная особенность позволяет размещать большой объем информации в ограниченном пространстве);

– SQRC – визуально не отличается от классического формата QR-кода, но имеет функцию ограничения чтения, которая предотвращает доступ неавторизированных лиц к частной информации;

– Frame QR или рамочный код – формат, позволяющий разместить в центре QR-кода изображение или логотип компании.

В системах контроля и управления доступом использование QR-кодов Модели 2 для генерации временного пропуска обеспечивает максимальный баланс между размером изображения, объемом хранимых данных и надежностью считывания. Такой пропуск позволяет закодировать [12] *уникальный идентификатор* (случайно сгенерированный номер пропуска для однозначной идентификации попуска) и *метаданные* (информацию о посетителе: ФИО, контактный номер, электронную почту, а также период действия пропуска, причину нахождения на охраняемой территории, уровень доступа, согласно разработанной матрице доступа.

Сгенерированный пропуск отображается на смартфоне посетителя и доступен весь период действия. При сканировании считывающим устройством QR-код расшифровывается, и ответственному лицу предоставляется возможность проверки легитимности доступа. Пример сформированного пропуска представлен на рисунке 3.

Рис. 3. Сформированный пропуск в виде QR-кода

Fig. 3. Generated Pass in the Form of a QR Code

Перед созданием QR-кода необходимо подготовить данные, которые будут в него закодированы:

1) зашифрованные данные – метаданные пропуска, зашифрованные с использованием расширенного стандарта шифрования с 256-битным ключом (AES-256);

2) зашифрованный симметричный ключ – ключ AES, зашифрованный с помощью шифрования на основе эллиптических кривых (EEC);

3) дополнительные параметры – например, вектор инициализации (IV), используемый при шифровании AES, или метаданные для идентификации типа данных.

Полученные данные объединяются в единую строку или бинарный формат. Для удобства обработки их можно сериализовать, например, в формате JSON, или объединить в виде шестнадцатеричной строки. Далее, для генерации пропуска, можно использовать язык программирования Python и библиотеку qrcode, предоставляющую простой и гибкий интерфейс создания QR-кода и поддерживающую различные параметры, например размер, уровень коррекции ошибок и цветовое оформление.

QR-коды поддерживают несколько уровней коррекции ошибок, которые определяют, насколько устойчив код к повреждениям или искажениям: *L* (Low) – 7 % повреждений могут быть восстановлены; *M* (Medium) – 15 %; *Q* (Quartile) – 25%; *H* (High) – 30%.

Для систем контроля доступа рекомендуется использовать уровень коррекции ошибок не ниже *M*, чтобы обеспечить надежность считывания даже при частичном повреждении QR-кода.

Генерация QR-кода состоит из следующих шагов.

Шаг 1. Создание объекта QR-кода – инициализируется объект QR-кода с указанием параметров, таких как версия QR-кода, уровень коррекции ошибок и размер.

Шаг 2. Добавление данных – подготовленные зашифрованные данные добавляются в объект QR-кода.

Шаг 3. Генерация изображения – на основе добавленных данных создается изображение QR-кода. Это изображение может быть сохранено в файл или отображено на экране.

Шаг 4. Сохранение QR-кода в виде изображения (например, в формате PNG) для дальнейшего использования.

Шаг 5. Отправка QR-кода пользователю, которому необходимо предоставить доступ на территорию университета, с помощью Telegram-бота системы [13].

Генерация QR-кода является завершающим этапом в создании системы контроля доступа с использованием шифрования AES-256 и EEC. QR-код позволяет удобно и безопасно передавать зашифрованные данные, которые могут быть расшифрованы и проверены на стороне сервера. Такой подход обеспечивает высокий уровень безопасности и надежности, что делает его идеальным решением для современных систем контроля доступа.

Варианты шифрования данных для генерации QR-кодов

Для повышения безопасности временных пропусков на основе QR-кодов важно использовать надежные и современные методы шифрования, такие как AES-256 и EEC. Данные методы гарантируют, что закодированные в пропуска данные будут защищены от несанкционированного доступа, взлома и подделки, что гарантирует не только физическую, но и информационную безопасность при генерации пропусков.

AES-256 – симметричный алгоритм шифрования, широко используемый для защиты конфиденциальных данных [14]. Является одним из самых безопасных алгоритмов шифрования, что особенно важно для генерации пропусков, содержащих конфиденциальную информацию. Данный алгоритм также является предпочтительным для выбора при использовании QR-кода, как пропуска, так как:

– значительно упрощает процесс генерации и считывания пропуска – пара ключей заранее известна обеим сторонам процесса и ключ используется как для шифрования, так и для расшифровки данных;

– позволяет обрабатывать небольшие массивы данных, за счет работы с блоками объемом 128 бит, что важно для ограниченной вместимости QR-кода;

– скорость работы как на аппаратном, так и на программном уровне является достаточно высокой, что повышает производительность во время различных мероприятий или приемной кампании.

Для создания QR-кода с информацией о пропуске посетителя университета необходимо [15]:

1) сгенерировать случайный ключ, который будет использован для шифрования и расшифрования данных; длина ключа должна составлять 256 бит (32 байта);

2) преобразовать данные, необходимые для шифрования, в строку, а затем добавить отступы к полученной строке с помощью специальной функции для корректировки длины сообщения и корректной работы с блоками данных фиксированного размера (16 байт);

3) зашифровать данные с использованием сгенерированного ключа и режима шифрования, например, CBC (*аббр. от англ.* Cipher Block Chaining) – шифрование для симметричного блока с использованием механизма обратной связи; в процессе также генерируется вектор инициализации (IV) – произвольное число, использующееся с ключом шифрования для повышения безопасности;

4) закодировать зашифрованные данные и вектор инициализации в формат base64 для удобства хранения, передачи и корректной обработки в текстовом формате;

5) создать QR-код на основе закодированного и зашифрованного сообщения с помощью выбранного программного решения.

При необходимости расшифровать данные пользователь сканирует QR-код и получает зашифрованные данные, а также – вектор инициализации (VI). Используя ключ шифрования, сообщение расшифровывается и восстанавливается исходное сообщение.

AES-256 является одним из самых безопасных методов шифрования, однако, если речь идет о высоком уровне безопасности при меньших размерах ключей и более эффективном использовании ресурсов, EEC предпочтительнее [16].

EEC – ассиметричный метод шифрования, основанный на алгебраической структуре эллиптических кривых над конечными полями для создания ключей. Может быть эффективно использован для генерации пропусков, представленных QR-кодом, сочетая безопасность, производительность и размер.

Для создания QR-кода с зашифрованной информацией необходимо [17] выполнить следующие действия:

1) выбрать эллиптическую кривую (это может быть стандартная кривая для шифрования), например, именованную кривую SECP256R1 и базовую точку G;

2) сгенерировать случайное число d, выступающее в роли закрытого ключа (ключ, известный только администратору домена, использующийся для расшифровки информации в ассиметричном шифровании); число должно быть меньше порядка кривой n;

3) вычислить открытый ключ Q с использованием базовой точки G по формуле: $Q = d * G$;

4) определить данные, необходимые в QR-коде (уникальный идентификатор и метаданные), и преобразовать их в подходящий для шифрования формат (например, в двоичный массив);

5) создать случайное число k, использующееся в процессе шифрования в роли временного ключа;

6) вычислить точки C_1 и C_2. $C_1 = k * G$ и $C_2 = k * Q + msg$, где msg – преобразованные данные для шифрования;

7) сформировать QR-код на основе зашифрованного сообщения; для формирования пропуска используется как C_1, так и C_2, для генерации с помощью конкатенации двух точек и последующего использования для расшифровки.

При расшифровке QR-кода сотрудник сканирует полученный пропуск, считывает закодированные как C_1, так и C_2, восстанавливает сообщение с помощью закрытого ключа по формулам $P_k = d * C_1$, и $msg = C_2 - P_k$.

Заключение

Безопасность в вузах является одной из ключевых задач, требующих комплексного подхода. С ростом числа студентов, преподавателей и посетителей, а также с увеличением угроз внедрение современных систем безопасности становится неотъемлемой частью обеспечения безопасной образовательной среды. Одним из эффективных решений является система мониторинга временных пропусков, которая позволяет не только контролировать доступ на территорию учебного заведения, но и отслеживать передвижение людей, оперативно реагируя на потенциальные угрозы.

Важным аспектом обеспечения безопасности является также обучение студентов и сотрудников правилам поведения в экстренных ситуациях. Регулярные тренинги, семинары и информирование о возможных угрозах помогают создать культуру безопасности, что является неотъемлемой частью комплексного подхода.

Использование QR-кодов в качестве временных пропусков представляет собой современный и универсальный подход, сочетающий в себе удобство, высокий уровень безопасности и эффективность. QR-коды позволяют хранить зашифрованные данные, такие как идентификатор пользователя, срок действия пропуска и другие метаданные, что обеспечивает защиту от несанкционированного доступа и подделки. Применение методов шифрования, таких как AES-256 и EEC, гарантирует высокий уровень конфиденциальности и целостности данных.

Новизна предлагаемого решения заключается в принципиально новом подходе к организации системы безопасности, основанном на интеграции QR-кодов с многоуровневой схемой верификации. В отличие от систем, использующих RFID-карты или бумажные носители, предлагаемая методика основывается на динамически генерируемых QR-кодах с усиленной защитой на базе алгоритмов криптографии, что обеспечивает не только надежную защиту от подделки, но и возможность оперативной корректировки параметров доступа в режиме реального времени. Параметры кодирования изменяются в зависимости от уровня важности охраняемого объекта и основываются на матрице доступа [18].

Внедрение системы генерации временных пропусков на основе QR-кодов не только повышает уровень безопасности в вузах, но и упрощает процессы управления доступом. Автоматизация выдачи пропусков, контроль сроков действия, сбор данных и автоматические уведомления о нарушениях делают систему гибкой и адаптивной к различным сценариям использования. Предполагается, что внедрение описываемой методики может повысить безопасность в вузах на 30–40 %. Это связано с тем, что использование QR-кодов и современных методов шифрования позволяет снизить риск несанкционированного доступа и подделки пропусков. Кроме того, автоматизация процессов управления доступом и оперативное реагирование на потенциальные угрозы способствуют повышению эффективности системы безопасности.

С теоретической точки зрения, предлагаемая методика вносит значительный вклад в развитие методологии обеспечения безопасности в образовательных учреждениях и предлагает новую концепцию интеграции динамически генерируемых QR-кодов, что расширяет существующие подходы к управлению доступом и защите данных. Внедрение алгоритмов криптографии, таких как AES-256 и ECC, обеспечивает не только высокий уровень конфиденциальности и целостности данных, но и открывает новые перспективы для исследования в области информационной безопасности.

Таким образом, внедрение системы мониторинга временных пропусков на основе QR-кодов с использованием современных методов шифрования является важным шагом к созданию безопасной и комфортной образовательной среды. Это не только обеспечивает защиту от физических и киберугроз, но и способствует повышению эффективности управления доступом, что в конечном итоге положительно сказывается на репутации и успешном развитии учебного заведения.

Список источников

1. ГОСТ Р 53704-2009. Системы безопасности комплексные и интегрированные. Общие технические требования. М.: Стандартинформ, 2010.

2. Тимофеева О.А., Зайцев А.Н., Смурыгин А.В. Комплексное обеспечение безопасности образовательного учреждения как технология интегрированного обучения // V Международная научно-практическая конференция «Культура физическая и здоровье современной молодежи» (Воронеж, Российская Федерация, 15 сентября 2022 г.). Воронеж: Воронежский государственный педагогический университет, 2022. С. 216–220. EDN:DTHCAC

3. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. М.: Стандартинформ, 2006.

4. ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. М.: Издательство стандартов, 1990.

5. Картамышев А.В., Маренчук Ю.А., Рожков С.Ю., Жук Е.А. Обеспечение комплексной безопасности образовательного учреждения // IX (66-я) ежегодная научно-практическая конференция Северо-Кавказского федерального университета «Актуальные проблемы инженерных наук» (Ставрополь, Российская Федерация, 04–29 апреля 2022 г.). Ставрополь: Северо-Кавказский федеральный университет, 2022. С. 277–281. EDN:QPBQSJ

6. Загребина Е.И. К вопросу комплексной безопасности образовательных учреждений // Казанский педагогический журнал. 2015. № 1(108). С. 97–103. EDN:RXWADS

7. Калинина Ю.Ю. Разработка информационной системы автоматизации процесса создания временного пропуска на территорию Астраханского государственного университета им. В.Н. Татищева // VII Всероссийская научно-практическая конференция «Проблемы повышения эффективности научной работы в оборонно-промышленном комплексе России» (Знаменск, Российская Федерация, 11–12 апреля 2024 г.). Астрахань: Астраханский государственный университет им. В.Н. Татищева, 2024. С. 91–94. EDN:BQZIRB

8. QR Codes 101: A Beginner's Guide // QR-Code-Generator. URL: https://ru.qr-code-generator.com/qr-code-marketing/qr-codes-basics (Accessed 04 June 2025)

9. ГОСТ Р ИСО/МЭК 18004-2015. Информационные технологии. Автоматическая идентификация. Кодирование штриховое. Спецификация символа QR-код. М.: Стандартинформ, 2016.

10. ISO/IEC 18004:2015. Information technology – Automatic identification and data capture techniques – QR Code bar code symbology specification. Geneva: ISO, 2015.

11. Серебрякова С.Г. QR-код – будущее цифрового повествования? // XXIII Международный Балтийский коммуникационный форум «Вестник факультета социальных цифровых технологий» (Санкт-Петербург, Российская Федерация, 03–04 декабря 2021 г.). СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2021. С. 295–298. EDN:PHWWDE

12. Задорожный А.В. Использование QR-кода в процессе контроля посещаемости занятий // XI Международный молодежный форум «Образование. Наука. Производство» (Белгород, Российская Федерация, 01–20 октября 2019 г.). Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2019. С. 2928–2932. EDN:THNKCB

13. Калинина Ю.Ю., Смирнова Ю.А. Автоматизация процесса контроля доступа в университете с помощью Telegram-бота // V Международная научно-практическая конференция «Современные тенденции развития информационных технологий в научных исследованиях и прикладных областях» (Владикавказ, Российская Федерация, 25–26 апреля 2024 г.). Владикавказ: Северо-Кавказский горно-металлургический институт, 2024. С. 52–55. EDN:GBZBYA

14. Семенов С.Н., Сай С.В. Особенности алгоритма шифрования AES: Rijndael // Региональная научно-практическая конференция «ТОГУ-Старт: фундаментальные и прикладные исследования молодых» (Хабаровск, Российская Федерация, 12–16 апреля 2021 г.). Хабаровск: Тихоокеанский государственный университет, 2021. С. 345–350. EDN:AMLWHM

15. Волокитина Т.С. Программная реализация блочного шифрования с переменными ключами на основе шифра AES 256 // X Международный конкурс научно-исследовательских работ «Фундаментальные и прикладные научные исследования» (Уфа, Российская Федерация, 05 декабря 2022 г.). Уфа: Общество с ограниченной ответственностью "Научно-издательский центр "Вестник науки", 2022. С. 67–78. EDN:TMAWEA

16. Воробьев А.П., Кротова Е.Л., Воробьева Е.Ю. Преимущества криптографии на эллиптических кривых для решения задач аутентификации // Вестник УрФО. Безопасность в информационной сфере. 2024. № 2(52). С. 99–105. DOI:10.14529/secur240210. EDN:GZNHGR

17. Ольшанский В.К. Эллиптические кривые в современной криптографии // XVII Санкт-Петербургская международная конференция «Региональная информатика» (РИ-2020, Санкт-Петербург, Российская Федерация, 28–30 октября 2020 г.). Т. Часть 1. Санкт-Петербург: Региональная общественная организация "Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления", 2020. С. 351–352. EDN:BJESRU

18. Калинина Ю.Ю., Смирнова Ю.А., Демина Р.Ю. Методика и алгоритм интеллектуальной поддержки принятия управленческих решений в системе генерации временных пропусков на Территорию высших учебных заведений // Вестник Тамбовского государственного технического университета. 2025. Т. 31. № 1. С. 70–80. DOI:10.17277/vestnik.2025.01.pp.070-080. EDN NPFYUL

References

1. GOST R 53704-2009. *Complex and integrated security systems. General technical requirements*. Moscow: Standartinform 2010. (in Russ.)

2. Timofeeva O.A., Zaitsev A.N., Smurygin A.V. Comprehensive security of an educational institution as a technology of integrated learning. *Proceedings of the Vth International Scientific and Practical Conference on Physical culture and health of modern youth, 15 September, 2022, Voronezh, Russian Federation*. Voronezh: Voronezh State Pedagogical University Publ.; 2022. p.216–220. (in Russ.) EDN:DTHCAC

3. GOST R ISO/IEC 17799-2005. *Information technology. Code of practice for information security management*. Moscow: Standartinform Publ.; 2006. (in Russ.)

4. GOST 34.003-90. *Information technology. Set of standards for automated systems. Automated systems. Terms and definitions.* Moscow: Izdatelstvo standartov Publ.; 1990. (in Russ.)

5. Kartamyshev A.V., Marenchuk Yu.A., Rozhkov S.Y., Zhuk E.A. Ensuring the integrated security of an educational institution. *Proceedings of the IX (66th) Annual Scientific and Practical Conference of the North Caucasus Federal University on Actual Problems of Engineering Sciences, 04–29 April 2022, Stavropol, Russian Federation*. Stavropol: North Caucasus Federal University Publ.; 2022. p.277–281. (in Russ.) EDN QPBQSJ

6. Zagrebina E.I. To integrated safety educational organizations. *Kazan Pedagogical Journal*. 2015;1(108):97–103. (in Russ.) EDN:RXWADS

7. Kalinina Yu.Y. Development of an information system for automating the process of creating a temporary pass to the territory of the Astrakhan State University named after V.N. Tatishchev. *Proceedings of the VIIth All-Russian Scientific and Practical Conference on Problems of Increasing the Efficiency of Scientific Work in the Russian Military-Industrial Complex, 11–12 April 2024, Znamensk, Russian Federation*. Astrakhan: Astrakhan State University named after V.N. Tatishchev Publ.; 2024. p.91–94. (in Russ.) EDN:BQZIRB

8. QR-Code-Generator. QR Codes 101: A Beginner's Guide. URL: https://ru.qr-code-generator.com/qr-code-marketing/ qr-codes-basics [Accessed 04 June 2025]

9. GOST R ISO/IEC 18004-2015. Information technology. Automatic identification. Bar coding. Encyclopedia of QR code symbols. Moscow: Stratinform; 2016. (in Russ.)

10. ISO/IEC 18004:2015. Information technology. Methods of automatic identification and data collection. Specification of QR codes and barcodes. Geneva: ISO; 2015.

11. Serebryakova S.G. Can QR-Code Become the Future of Digital Storytelling? *Proceedings of the XXIIIth International Baltic Communication Forum «Bulletin of the Faculty of Social Digital Technologies», 03–04 December 2021, St. Petersburg, Russian Federation*. St. Petersburg: The Bonch-Bruevich Saint Petersburg State University of Telecommunications Publ.; 2021. p.295–298. (in Russ.) EDN:PHWWDE

12. Zadorozhny A.V. The use of a QR code in the process of monitoring class attendance. *Proceedings of the XIth International Youth Forum "Education. Science. Production", 01–20 October 2019, Belgorod, Russian Federation*. Belgorod: Belgorod State Technological University named after V.G. Shukhov Publ.; 2019. p.2928–2932. (in Russ.) EDN:THNKCB

13. Kalinina Yu.Y., Smirnova Yu.A. Automation of the access control process at the university using a Telegram bot. *Proceedings of the Vth International Scientific and Practical Conference on Current Trends in the Development of Information Technologies in Scientific Research and Applied Fields, 25–26 April 2024, Vladikavkaz, Russian Federation*. Vladikavkaz: North Caucasus Mining and Metallurgical Institute Publ.; 2024. p.52–55. (in Russ.) EDN:GBZBYA

14. Semenov S.N., Sai S.V. Features of the AES: Rijndael encryption algorithm. *Proceedings of the Regional Scientific and Practical Conference «TOGU-Start: Fundamental and Applied Research of Young People», 12–16 April 2021, Khabarovsk, Russian Federation*. Khabarovsk: Pacific State University Publ.; 2021. p.345–350. (in Russ.) EDN:AMLWHM

15. Volokitina T.S. Software implementation of block encryption with variable keys based on the AES 256 cipher. *Proceedings of the Xth International Research Competition on Basic and Applied scientific Research, 05 December 2022, Ufa, Russian Federation*. Ufa: Nauchno-izdatelskii tsentr Vestnik nauki Publ.; 2022. p.67–78. (in Russ.) EDN:TMAWEA

16. Vorobyov A.P., Krotova E.L., Vorobyova E.Y. Advantages of cryptography on elliptic curves for solving authentication problems. *Bulletin of the Ural Federal District. Security in the Information Sphere*. 2024;2(52):99–105. (in Russ.) DOI:10.14529/secur240210. EDN:GZNHGR

17. Olshansky V.K. Elliptic curves in modern cryptography. *Proceedings of the XVIIth St. Petersburg International Conference «Regional Informatics (RI-2020)», 28–30 October 2020, St. Petersburg, Russian Federation, vol.1*. St. Petersburg: St. Petersburg Society of Informatics, Computer Technology, Communication and Control Systems Publ.; 2020. p.351–352. (in Russ.) EDN:BJESRU

18. Kalinina Yu.Y., Smirnova Yu.A., Demina R.Yu. A method and algorithm of intelligent decision-making support system for generation of temporary access passes to the territory of higher educational institutions. *Bulletin of Tambov State Technical University*. 2025;31(1):70–80. (in Russ.) DOI:10.17277/vestnik.2025.01.pp.070-080. EDN:NPFYUL

Статья поступила в редакцию 14.04.2025; одобрена после рецензирования 21.05.2025; принята к публикации 02.06.2025.
The article was submitted 14.04.2025; approved after reviewing 21.05.2025; accepted for publication 02.06.2025.

Информация об авторах:

КАЛИНИНА Юлия Юрьевна
сотрудник кафедры информационных технологий Астраханского государственного университета им. В.Н. Татищева
https://orcid.org/0009-0009-8785-4634

СМИРНОВА Юлия Александровна
старший преподаватель кафедры информационных технологий Астраханского государственного университета им. В.Н. Татищева
https://orcid.org/0000-0002-3807-5062

Авторы сообщают об отсутствии конфликтов интересов.
The authors declare no conflicts of interests..

ДЛЯ ЗАМЕТОК

План издания научной литературы 2025 г., п. 11

Усл.-печ. л.	Формат	Заказ
16,25	$60\times84_{1/8}$	№ 1629

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