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

ТРУДЫ УЧЕБНЫХ ЗАВЕДЕНИЙ СВЯЗИ

Том 11. № 1
2025

Темы номера:

- Канал информационного обмена наземного сегмента гибридной сети связи
- Оптимизация использования ресурсов воздушных базовых станций
- Система радиосвязи с широкополосными сигналами в условиях присутствия ретранслированных помех

Vol. 11. Iss. 1
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. № 1

Proceedings of Telecommunication Universities

Vol. 11. Iss. 1

Санкт-Петербург

2025

Труды учебных заведений связи. 2025. Т. 11. № 1
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. 1
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.

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

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.**

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

ВЫХОДНЫЕ ДАННЫЕ / IMPRINT

Дата выхода в свет: 04.03.2025
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: 04.03.2025
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


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 004.7+004.738.2: 004.738.5
https://doi.org/10.31854/1813-324X-2025-11-1-7-17
EDN:FTRJGU

Исследование задержки кадров видеопотока в канале информационного обмена наземного сегмента гибридной сети связи при FPV-управлении БАС

Александр Александрович Березкин✉, berezkin.aa@sut.ru
Роман Михайлович Вивчарь, vivchar.rm@sut.ru
Александр Александрович Ченский, chenskii.aa@sut.ru
Руслан Валентинович Киричек, kirichek@sut.ru

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

Аннотация

В настоящем исследовании рассматриваются зависимости величины задержки и потери кадров видеопотока, сжатых нейросетевым кодеком, разработанным на основе нейросетевого вариационного автокодировщика, от размера передаваемых кадров при реализации каналов информационного обмена между беспилотной авиационной системой и станцией внешнего пилота в наземном сегменте гибридной орбитально-наземной сети связи с учетом расстояния между ними при использовании технологий передачи данных 3G и LTE.
Актуальность *исследования обусловлена необходимостью достижения заданного уровня качества обслуживания услуги управления беспилотными летательными аппаратами от первого лица в сетях связи.*
Используемые методы. *В ходе исследования натурным экспериментом измерены прикладные задержки передачи и потери кадров видеопотока FPV-управления при использовании нейросетевых кодеков. Прикладные задержки и потери учитывают сегментацию, восстановление пакетов и передачу нескольких UDP-пакетов для каждой полезной нагрузки. Дополнительно методом Розенблатта – Парзена восстановлены распределения плотности вероятности задержек.*
Результаты. *Получены оценки средних значений задержки передачи и потерь кадров видеопотока (сжатых нейросетевым кодеком) при использовании технологий передачи данных 3G и LTE с учетом различных расстояний между беспилотной системой и станцией внешнего пилота. Восстановлены распределения зависимостей задержек видеопотока от размера полезной нагрузки. Найден характер распределения задержки видеопотока, формируемого нейросетевым кодеком.* ***Новизна*** *полученных результатов заключается в исследовании характера задержек и потерь кадров видеопотока услуги FPV-управления, передаваемого через мобильные сети связи, на прикладном уровне модели OSI при использовании нейросетевых кодеков.*
Практическая значимость. *Полученные результаты могут быть примененены при моделировании каналов информационного обмена для FPV-управления с целью формирования оптимальной конфигурации используемых нейросетевых кодеков.*

Ключевые слова: *задержка видеопотока, кадры видеопотока, каналы информационного обмена, беспилотное воздушное судно, беспилотная авиационная система, управление от первого лица, FPV-управление, нейросетевой кодек*

Ссылка для цитирования: Березкин А.А., Вивчарь Р.М., Ченский А.А., Киричек Р.В. Исследование задержки кадров видеопотока в канале информационного обмена наземного сегмента гибридной сети связи при FPV-управлении БАС // Труды учебных заведений связи. 2025. Т. 11. № 1. С. 7–17. DOI:10.31854/1813-324X-2025-11-1-7-17. EDN:FTRJGU

Original research
https://doi.org/10.31854/1813-324X-2025-11-1-7-17
EDN:FTRJGU

Research of Video Stream Frame Delay in UAV FPV-Control Information Exchange Channel in Hybrid Communication Network Terrestrial Segment

Alexander A. Berezkin ✉, berezkin.aa@sut.ru
Roman M. Vivchar, vivchar.rm@sut.ru
Alexander A. Ченский, chenskii.aa@sut.ru
Ruslan V. Kirichek, kirichek@sut.ru

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

Annotation

This research considers the dependence of the delay and loss of video stream frames compressed by neural network codec developed on the basis of neural network variation auto-encoder on the size of transmitted frames in the realization of information exchange channels between unmanned aviation system and external pilot station in the ground segment of hybrid orbital-terrestrial communication network taking into account the distance between them when using 3G and LTE data transmission technologies are used. ***The Relevance*** *of the research is conditioned by the necessity to achieve a given level of service quality for FPV control of UAVs in communication networks.* ***Methods used.*** *In this research, the applied transmission delays and frame loss of FPV control video stream when using neural network codecs are measured by in-situ experiment. The applied delays and losses take into account segmentation, packet recovery and transmission of multiple UDP packets for each payload. Additionally, the Rosenblatt-Parzen method reconstructs the probability density distributions of delay probabilities.* ***Results.*** *Estimates of average values of transmission delay and frame loss of video stream (compressed by neural network codec) when using 3G and LTE data transmission technologies taking into account different distances between the unmanned system and the external pilot's station are obtained. The distributions of video stream delay dependencies on the payload size are reconstructed. The character of video stream delay distribution formed by neural network codec is found.* ***The Novelty*** *of the obtained results lies in the study of the nature of delays and frame losses of the FPV-control service video stream transmitted through mobile communication networks at the application layer of the OSI model when using neural network codecs.* ***Practical significance.*** *The results can be used in modeling of information exchange channels for FPV control in order to form the optimal configuration of the used neural network codecs.*

Keywords: *video stream latency, information link, channel of data exchange, channel of information exchange, unmanned aerial vehicle, unmanned aerial system, first person view control, FPV-control, neural codec*

For citation: Berezkin A.A., Vivchar R.M., Chenskiy A.A., Kirichek R.V. Research of Video Stream Frame Delay in UAV FPV-Control Information Exchange Channel in Hybrid Communication Network Terrestrial Segment. *Proceedings of Telecommunication Universities.* 2025;11(1):7–17. (in Russ.) DOI:10.31854/1813-324X-2025-11-1-7-17. EDN:FTRJGU

Введение

В настоящее время в различных сферах деятельности РФ нашли широкое применение беспилотные авиационные системы – БАС (статья 32 Воздушного кодекса РФ от 19.03.1997 № 60-ФЗ (ред. от 08.08.2024) «Воздушное судно»). БАС, например, широко применяются в сельском хозяйстве, строительстве, нефтегазовом секторе, метеорологии, кинематографе, МЧС, экологическом мониторинге, а также в военном деле [1]. В сельском хозяйстве беспилотные воздушные суда (БВС) обеспечивают учет животных [2], распыление инсектицидов, обра-

ботку животных от гнуса и т. п., в сфере строительства – непрерывный контроль стройплощадок и геодезические исследования [1]. В нефтегазовом секторе с помощью БВС возможен мониторинг состояния нефте- и газопроводов и определение источников утечек. При чрезвычайных ситуациях БАС позволяют проводить оценку последствий стихийной или техногенной катастрофы, обнаружение выживших, доставку продуктов питания, воды и медикаментов. В экологии существует ряд применений БАС: отслеживание и тушение пожаров [3], борьба с браконьерами, контроль лесного фонда, отслеживание таяния ледников, измерения загрязнения воздуха [1, 2].

В зависимости от используемой системы управления БАС делятся на: дистанционно-пилотируемые, дистанционно-управляемые, автоматические, дистанционно-управляемые авиационной системой и беспилотно-автоматические [4].

В Стратегии развития отрасли связи РФ до 2035 г., утвержденной распоряжением Правительства РФ от 24 ноября 2023 г. № 3339-р, указывается, что создаваемые гибридные орбитально-наземные сети связи (ГОНСС) потенциально позволят обеспечить возможность управления беспилотными летательными аппаратами в режиме реального времени на всей территории Российской Федерации. Для управления БАС ГОНСС могут состоять из двух интегрированных сегментов: наземного и спутникового. В зоне покрытия мобильных сетей связи управление БАС обеспечивает наземный сегмент. В отдаленных районах, где отсутствует покрытие мобильными сетями связи, либо мобильные сети связи не удовлетворяют требованиям по качеству обслуживания, управление будет обеспечивать спутниковый сегмент.

В настоящее время широкое распространение получили дистанционно-пилотируемые БАС, на основе управления от первого лица (*от англ.* First-Person-View, далее – FPV-управление) [5]. Однако использование подобных систем в ГОНСС существенно затруднено из-за наличия больших сетевых задержек передачи данных, особенно в космическом сегменте такой сети.

Для задачи FPV-управления несвоевременная актуальность кадров видеопотока приводит к временно́й задержке между реальной полетной обстановкой и полетной обстановкой, воспринимаемой оператором. В результате оператор оказывается не способен реагировать на нештатные ситуации. Это снижает вероятность успешного достижения цели функционирования БАС. Низкая интенсивность видеопотока на стороне станции внешнего пилота (СВП) приводит к формированию у оператора фрагментарной информации о полетной обстановке. Это влечет за собой возможность упущения ряда деталей, неверной оценки быстро меняющейся полетной обстановки и ограничения возможности реакции на нештатные ситуации. При этом существенное влияние на задержку и интенсивность FPV-видео-потока оказывает конфигурация используемых инструментов кодирования и декодирования видеопотока.

В настоящее время в составе систем кодирования видеопотока БАС, кроме широко используемых стандартизированных кодеков, работающих в пиксельном пространстве таких, как AVC/H264 [6] и HEVC/H265 [7], разрабатываются различные конфигурации нейросетевых кодеков, созданных на основе вариационных автокодировщиков различной конфигурации[1] [8, 9]. Они обеспечивают более высокую степень сжатия кадров видеопотока путем преобразования пиксельного пространства во внутреннее латентное пространство признаков нейросетевой модели. Однако такие видеопотоки специализированной структуры предусматривают использование специально разработанных каналов информационного обмена (КИО) для взаимодействия между БВС и СВП, входящих в состав БАС как в наземном, так и в космическом сегментах ГОНСС. Такие каналы предназначены для передачи видеопотока с камеры БВС и телеметрической информации (координат, скорости, курсового угла, высоты и т. д.) в направлении СВП, а также команд управления в обратном направлении.

Эффективность функционирования КИО непосредственным образом влияет на качество FPV-управления БАС и характеризуется задержкой между кадром полетной обстановки на стороне БВС и отображением данного кадра на терминале внешнего пилота, а также интенсивностью видеопотока. Задержка в КИО $t_{КИО}$ является задержкой прикладного уровня, так как учитывает передачу не только отдельного пакета, но и сегментацию полезной нагрузки на множество пакетов, которая выполняется на прикладном уровне.

Следовательно, становится актуальной задача выбора такой конфигурации нейросетевых кодеков, которая позволит повысить показатели эффективности функционирования КИО и тем самым обеспечить требуемое качество решения целевых задач БВС на FPV-управлении. Для решения такой задачи необходимо установить зависимость показателей эффективности функционирования КИО от используемой конфигурации нейросетевых кодеков. Зависимость может быть установлена путем имитационного моделирования процесса функционирования КИО. Однако при разработке такой модели необходимо учитывать зависимость величины прикладной задержки кадров видеопотока в

[1] Stable Diffusion // GitHub. URL: https://github.com/pesser/stable-diffusion (дата обращения 25.01.2025)

сети, а, следовательно, и показателей эффективности функционирования КИО, от размера полезной нагрузки (кадров видеопотока).

Целью настоящей работы является определение характеристик прикладной задержки передачи кадров FPV-видеопотока, сжатых нейросетевым кодеком [10, 11], от расстояния между БАС и оператором, и используемой технологии передачи данных (3G, LTE). Полученные результаты в дальнейшем позволят сформировать требования к используемым нейросетевым кодекам для FPV-управления БАС в наземном сегменте ГОНСС.

Описание эксперимента

Для исследования влияния размера кадров FPV-видеопотока, сжатых нейросетевым кодеком, на величину задержки их передачи в КИО наземного сегмента ГОНСС, был проведен эксперимент, заключающийся в передаче кадров различного размера между рядом регионов России и Санкт-Петербургом с использованием технологий 3G и LTE мобильных сетей связи. При этом точка, находящаяся в Санкт-Петербурге, выполняла роль СВП, а клиент, расположенный в других городах, – роль БВС.

Данные были получены из следующих городов Российской Федерации, где в скобках указано расстояние от БВС до СВП по прямой: Петергоф (23 км), Великий Новгород (166 км), Череповец (438 км), Москва (635 км), Архангельск (735 км), Апатиты (860 км), Оленегорск (930 км), Сочи (1926 км), Южно-Сахалинск (6660 км). Для передачи данных были использованы технологии мобильной связи 3-го поколения (3G) и беспроводной высокоскоростной связи (LTE). В качестве исследуемых потенциальных вариантов размеров полезной нагрузки (18 шт.) использовались следующие размеры: 100, 300, 500, 700, 1000, 2000, 3000, 4000, 5000, 7000, 10000, 15000, 20000, 30000, 50000, 70000, 100000 и 500000 байт.

Задержка в КИО $t_{\text{КИО}}$ (мс) включает в себя сетевую задержку $t_{\text{с}}$, задержку инкапсуляции t_{enc} и декапсуляции t_{dec} пакетов и может быть рассчитана по следующей формуле:

$$t_{\text{КИО}} = t_{\text{с}} + t_{enc} + t_{dec}.$$

При использовании в Интернете максимальной единицы передачи (MTU, *аббр. от англ.* Maximum Transmission Unit) сеть Ethernet на промежуточных узлах сети ограничена размером 1500 байт [12]. Средний размер бинарных сжатых последовательностей кадров видеопотока ряда конфигураций нейросетевого кодека [10, 11] превышает размер MTU. Соответственно, возникает необходимость в сегментации полезной нагрузки на уровне приложения FPV-управления [13]. Как известно, заголовок протокола сетевого уровня IPv4 равен 20 байтам, а IPv6 – 40 [14]. Предполагается, что с целью сокращения сетевых задержек передача кадров FPV-видеопотока осуществляется по протоколу сетевого уровня UDP с возможностью перехода на TCP при необходимости. Заголовок протокола UDP равен 8 байтам, а TCP – 20 [15]. На заголовок прикладного уровня для передачи видеопотока отводится 50 байт с 10-процентным резервированием.

Соответственно, формирование пакетов включает в себя разделение полезной нагрузки (кадра видеопотока) на части длиной до 1385 байт с добавлением заголовков пакета.

Потери кадров видеопотока, сжатых нейросетевым кодеком, отличаются от потери пакетов на уровне сети. Это обусловлено тем, что для восстановления кадра на приемной стороне необходимо получить все UDP-пакеты, содержащие части данного кадра.

Исходя из вышеизложенного, для определения уровня потери кадров можно использовать следующее выражение:

$$loss = \frac{frame}{all\_frame}(\%), \qquad (1)$$

где *frame* – количество успешно принятых и восстановленных на СВП кадров; *all_frame* – количество отправленных с БАС кадров; пакеты, которые не удалось получить в течение 5 секунд (таймаут подключения), можно считать потерянными.

В настоящей работе помимо задержек в КИО $t_{\text{КИО}}$ измеряются также уровни потерь в КИО как параметр, влияющий на интенсивность видеопотока на стороне СВП и, как следствие, на качество FPV-управления. Процесс функционирования КИО подвержен влиянию различных факторов неопределенности, что обусловливает стохастический характер данного процесса, а, следовательно, и случайное значение величины $t_{\text{КИО}}$ и уровня потери кадров. Поэтому, в процессе исследования влияния размера полезной нагрузки на указанный выше показатель, была проведена передача между БВС и СВП 10000 кадров каждого из размеров. Данное значение было выбрано, исходя из необходимости получения репрезентативной выборки значений величины $t_{\text{КИО}}$ с целью определения характеристик ее закона распределения.

Для определения величины $t_{\text{КИО}}$ и уровня потери кадров было разработано специальное программное обеспечение, представляющее собой набор скриптов Python 3.11 с использованием модулей стандартных библиотек, таких как `csv`, `socket`, `argparse`, `datetime`, `time`, `signal` и `struct`.

Данное программное обеспечение включает в себя клиентскую и серверную часть, принцип работы которых заключается в следующем. Для каж-

дого i-го варианта полезной нагрузки, $i = \overline{1,18}$, размером $payload_i$ байт, формируется N UDP-пакетов данных, в состав которых входит кадр видеопотока, сжатый нейросетевым кодеком:

$$\begin{cases} N = 1, & \dfrac{payload_i}{1385} < 1 \\ N = \left\lceil \dfrac{payload_i}{1385} \right\rceil, & \dfrac{payload_i}{1385} \geq 1 \end{cases}.$$

Процесс передачи видеокадра подразумевает успешную передачу всех N UDP-пакетов данных. Потеря как минимум одного пакета расценивается как потеря всего кадра целиком, что увеличивает задержку $t_{\text{КИО}}$.

Каждый пакет от 1 до N – 1 содержит 1385 байт, а N-й пакет содержит $payload_i - \left\lfloor \frac{payload_i}{1385} \right\rfloor$ байт. Для эмуляции заголовка прикладного уровня к каждому пакету дополнительно добавляются 20 технических байт. Пакеты отправляются по протоколу UDP с БВС на СВП с интервалом в 1 мс и таймаутом подключения, равным 5 секундам. Если все пакеты, относящиеся к полезной нагрузке некоторого кадра, получены, они упорядочиваются на стороне СВП и отправляются обратно на БВС. Возвращенные пакеты упорядочиваются на стороне БВС, после чего идет сравнение полезных нагрузок (рисунок 1).

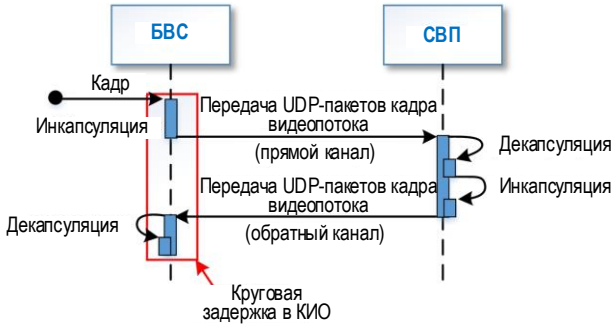


Рис. 1. Схема измерения задержки передачи одного кадра видеопотока

Fig. 1. One Video Stream Frame Latency Measuring Scheme

По результатам 10000 итераций передачи сжатых кадров видеопотока от БВС к СВП и обратно для каждого варианта расположения БВС была получена выборка значений величины $t_{\text{КИО}}$, а также количество успешно принятых и восстановленных на СВП кадров *frame*. Полученное значение *frame* позволило рассчитать уровень потери кадров видеопотока в КИО в соответствии с выражением (1). Путем обработки выборки значений величины $t_{\text{КИО}}$ был определен закон ее распределения, для чего был использован один из ядерных методов восстановления плотности вероятности – метод Розенблатта – Парзена.

В соответствии с методом Розенблатта – Парзена плотность вероятности случайной величины аппроксимируется следующим выражением [16]:

$$f(x) = \frac{1}{Kh} \sum_{k=1}^{K} Y\left(\frac{x - x_k}{h}\right),$$

где x_k – реализация случайной величины в k-ом опыте; h – ширина пропускания случайной величины; $Y\left(\frac{x-x_k}{h}\right)$ – ядерная функция; K = 10000 – общее количество опытов; в качестве ядерной функции была использована Гауссова функция [17, 18].

Важным этапом использования метода Розенблатта – Парзена является выбор ширины пропускания h, так как неправильный выбор этого параметра может повлиять на адекватность оценки плотности вероятности. Выбор оптимального значения ширины пропускания исходил из критерия минимизации интеграла квадрата отклонения истиной плотности вероятности от ее ядерной оценки [19]:

$$h^* = \underset{h \in \Delta}{\operatorname{argmin}} \left(\int_{-\infty}^{+\infty} f^2(x)\, dx - \frac{2}{Kh(K-1)} \sum_{k=1}^{K} \sum_{\substack{j=1 \\ j \neq k}}^{K} Y\left(\frac{x_k - x_j}{h}\right) \right),$$

где h^* – оценка полосы пропускания.

Полученные законы распределения величины $t_{\text{КИО}}$ передачи видеопотока наземного сегмента ГОНСС для каждого варианта полезной нагрузки позволили определить наиболее вероятное значение этой задержки, ее математическое ожидание и дисперсию. Это позволило в дальнейшем оценить влияние величины полезной нагрузки на данные параметры для различных случаев расположения БВС.

Результаты эксперимента

В результате проведенного эксперимента было определено, что величина прикладной задержки рассматриваемого КИО для любого варианта сочетания полезной нагрузки, расположения БВС и используемой технологии передачи данных подчиняется усеченному двухпараметрическому бета-распределению (рисунок 2). Это обусловлено тем, что данный закон распределения учитывает следующие особенности формирования задержки.

Особенность 1. Величина $t_{\text{КИО}}$ ограничена как сверху, так и снизу, т. е. всегда можно указать максимальную величину задержки $t_{\text{КИО}}^{\text{макс}}$, которая будет сформирована, несмотря на стечение самых неблагоприятных обстоятельств, и минимальную величину $t_{\text{КИО}}^{\text{мин}}$, которая будет обусловлена наиболее приятным стечением обстоятельств.

Особенность 2. Величина $t_{\text{КИО}}$ может принять любое значение в интервале $[t_{\text{КИО}}^{\text{мин}}, t_{\text{КИО}}^{\text{макс}}]$, т. е. является непрерывной случайной величиной.

Особенность 3. Среди всех задержек, которые могут наблюдаться при функционировании КИО, могут встречаться задержки, величина которых зависит от большого числа случайных факторов, каждый из которых в отдельности является малосущественным, а также – задержки, на продолжительность которых оказывает влияние небольшое число важных факторов.

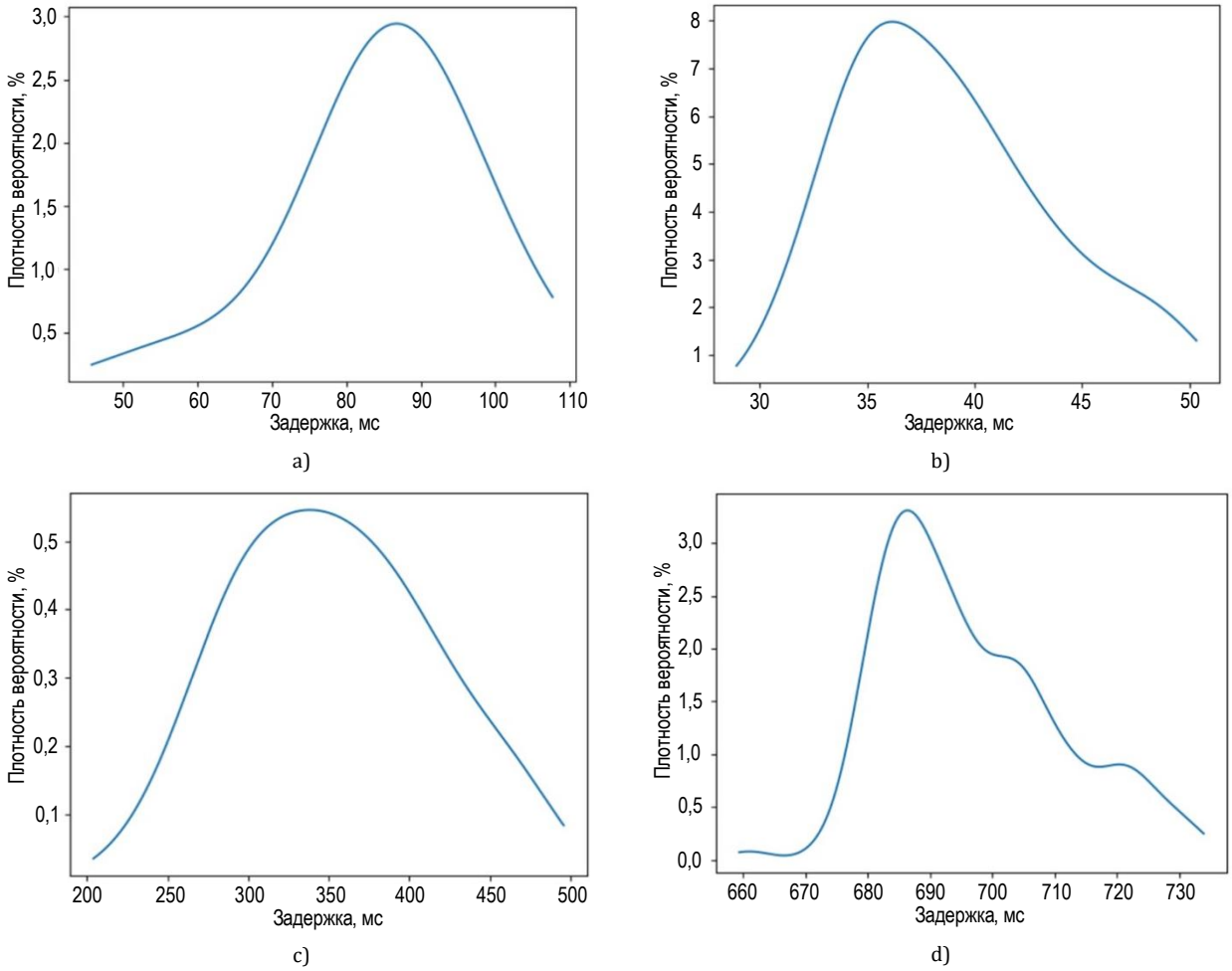


Рис. 2. Плотности вероятности величины прикладной задержки: a) Апатиты (3G, 100 байт); b) Архангельск (LTE, 5000 байт); c) Сочи (3G, 20000 байт); d) Южно-Сахалинск (LTE, 500 Кб)

Fig. 2. Probability Densities of the Application Delay Value: a) Apatity (3G, 100 bytes); b) Arkhangelsk (LTE, 5000 bytes); c) Sochi (3G, 20000 bytes); d) Yuzhno-Sakhalinsk (LTE, 500 Kb)

Первая особенность требует, чтобы на интервале $[t_{\text{КИО}}^{\text{мин}}, t_{\text{КИО}}^{\text{макс}}]$ закон распределения был усеченным, вторая – непрерывным, а третья – чтобы был таким, при котором наиболее вероятное значение времени устранения отказа могло располагаться в любом месте интервала $[t_{\text{КИО}}^{\text{мин}}, t_{\text{КИО}}^{\text{макс}}]$.

Среди практически применяемых распределений наиболее отвечающим этим требованиям является закон бета-распределения. Проверка данной гипотезы осуществлялась с использованием критерия Пирсона, сущность которого заключается в оценке меры расхождения χ^2 между теоретическими вероятностями p_i и наблюдаемыми частотами p_i^*. В результате проверки была вычислена мера расхождения $\chi^2 = 3{,}94$. При этом найденная по таблицам вероятность приближенно равна 0,56. Эта вероятность не является малой, поэтому гипотезу о том, что величина $t_{\text{КИО}}$ распределена по бета-закону можно считать правдоподобной.

Характеристиками закона бета-распределения являются параметры формы: α и β.

Анализ полученных плотностей вероятности позволил сделать вывод, что для значения данных параметров принимают следующие значения:

$$2 \le \alpha \le 9; 2 \le \beta \le 14. \qquad (2)$$

Для определения характеристик закона бета-распределения были использованы следующие выражения:

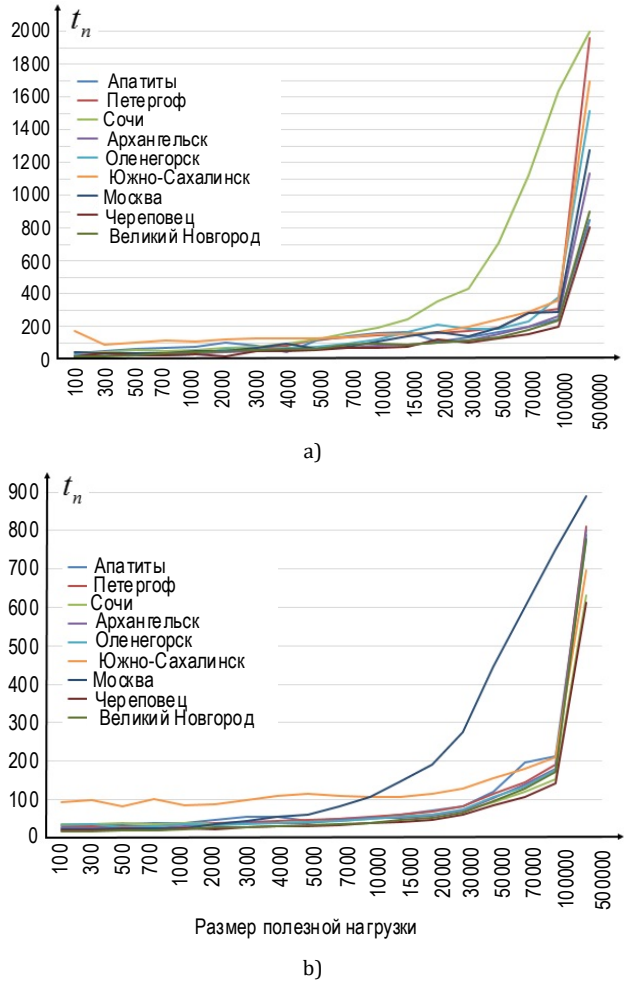
$$t_{\text{КИО}}^{\text{нв}} = t_{\text{КИО}}^{\text{мин}} + (t_{\text{КИО}}^{\text{макс}} - t_{\text{КИО}}^{\text{мин}}) \frac{\alpha - 1}{\alpha + \beta - 2}, \qquad (3)$$

$$\sigma = (t_{\text{КИО}}^{\text{макс}} - t_{\text{КИО}}^{\text{мин}}) \frac{\sqrt{\alpha\beta}}{(\alpha+\beta)\sqrt{\alpha+\beta+1}}, \qquad (4)$$

где $t_{\text{КИО}}^{\text{нв}}$ и σ – наиболее вероятная величина задержки и ее среднеквадратическое отклонение, определяемые из выборки.

Исходя из этого, при моделировании КИО для передачи FPV-видеопотока наземного сегмента ГОНСС целесообразно в качестве закона распределения величины прикладной задержки использовать бета-распределение с параметрами (2).

На рисунке 3 представлены зависимости математического ожидания размера прикладной задержки от размера передаваемой полезной нагрузки для различных расстояний между БВС и СВП, а также используемой технологии передачи данных.



a)

b)

Рис. 3. Зависимость размера прикладной задержки КИО от размера передаваемой полезной нагрузки для различных расстояний между БВС и СВП при использовании 3G (a) и LTE (b)

Fig. 3. Dependence of the Delay in the Information Exchange Link on the Transmitted Payload Size for Different Distances between the UAV and the Remote Pilot Station in 3G Network (a) and LTE (b)

Представленные графики показывают, что зависимости величины прикладной задержки от размера передаваемой полезной нагрузки имеют вид показательной возрастающей функции. При этом максимальная величина задержки при передаче полезной нагрузки объемом от 20000 до 500000 байт с использованием 3G в среднем в два раза превышает величину задержки с использованием технологии LTE для всех вариантов расстояний между БВС и СВП (рисунок 4).

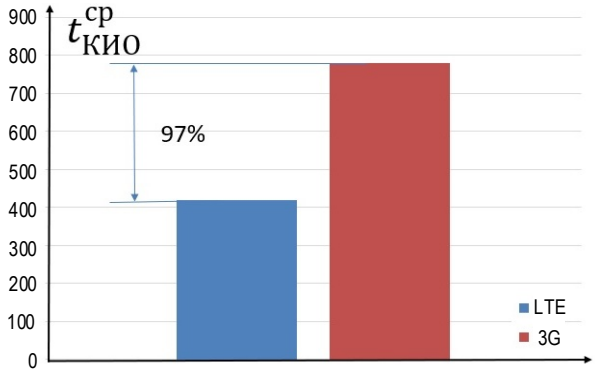


Рис. 4. Зависимость средней величины полезной нагрузки для всех вариантов расстояний между БВС и СВП от используемой технологии передачи данных

Fig. 4. Dependence of the Average Payload Value for All Variants of the Distances between the UAV and the Remote Pilot Station on the Data Transmission Technology Used

При передаче полезной нагрузки размером от 100 до 15000 байт величина $t_{\text{КИО}}$ остается неизменной (в среднем принимает значение 35 мс) для обеих технологий передачи данных и практически не зависит от расстояния. Исключением является только передача указанной полезной нагрузки на сверхдальнее расстояние (более 6000 км). Среднее значение величины $t_{\text{КИО}}$ в этом случае равно 100 мс.

Полученные результаты позволяют сделать вывод, что в связи с тем, что величина задержки остается неизменной как для полезной нагрузки размером 100 байт, так и 15000 байт, то целесообразно использовать конфигурации нейросетевых кодеков, которые формируют на выходе сжатые кадры видеопотока, размером не более 15000 байт. Следует отметить, что средние размеры сжатых кадров видеопотока при использовании нейросетевого кодека лежат на интервале [500; 9000] байт [11], что полностью укладывается в данное ограничение. В этой связи можно сделать вывод о том, что при передаче видеопотока в КИО наземного сегмента ГОНСС целесообразно использовать только одну конфигурацию нейросетевого кодека, обеспечивающую лучшее качество восстанавливаемого кадра видеопотока [10, 11].

Анализ графика на рисунке 3b показывает, что задержка в КИО при нахождении БВС в г. Москва в сети 4G существенно выше задержки из других исследуемых локаций. Это может быть обусловлено

существенно большей плотностью населения (таблица 1)[2] и частотой использования мобильной связи населением в определенный момент времени, что обеспечивает большую нагрузку на сеть сотовой связи и увеличивает задержку передачи данных прикладных протоколов.

ТАБЛИЦА 1. Плотность населения в исследуемых регионах

TABLE 1. Population Density in Reviewed Regions

Локация	Субъект Федерации	Плотность населения, чел/км^2
Москва	Город федерального значения Москва	4940,5
Сочи	Краснодарский край	77,24
Петергоф	Ленинградская область	24,26
Великий Новгород	Новгородская область	10,75
Череповец	Вологодская область	8,5
Южно-Сахалинск	Сахалинская область	5,4
Апатиты	Мурманская область	4,5
Оленегорск	Мурманская область	4,5
Архангельск	Архангельская область	1,69

Анализ графика, представленного на рисунке 4, показывает, что структура самой местности[3] при пролете БВС может оказывать влияние на $t_{КИО}$, что видно на примере г. Сочи (рисунок 5).

В результате эксперимента также было выявлено, что уровень потери кадров видеопотока (рисунок 6) для случаев передачи полезной нагрузки в диапазоне от 100 до 15000 байт не зависит от расстояния и технологии передачи данных и составляет в среднем менее одного процента (без учета временных разрывов соединений). Для больших размеров полезной нагрузки (более 15000 байт) расстояние между БВС и СВП и используемая технология передачи данных начинает играть существенную роль. Так, для полезной нагрузки размером 50000 байт при передаче ее на расстояние более 1500 км с использованием технологии 3G уровень потерь кадров видеопотока в КИО может достигать 90 %.

Приведенные результаты исследования могут быть учтены при моделировании процесса функционирования КИО в наземном сегменте ГОНСС с целью выбора оптимальной конфигурации нейросетевых кодеков, которая позволит повысить показатели эффективность функционирования КИО.

[2] Регионы России. Социально-экономические показатели // Росстат. URL: https://rosstat.gov.ru/folder/210/document/13204 (дата обращения 26.01.2025)

[3] Топографическая карта Сочи. URL: https://ru-ru.topographic-map.com/map-h97cgp/Сочи/?base=2 (дата обращения: 26.01.2025)

Рис. 5. Гористость в исследуемых регионах

Fig. 5. Mountainousness in the Examined Regions

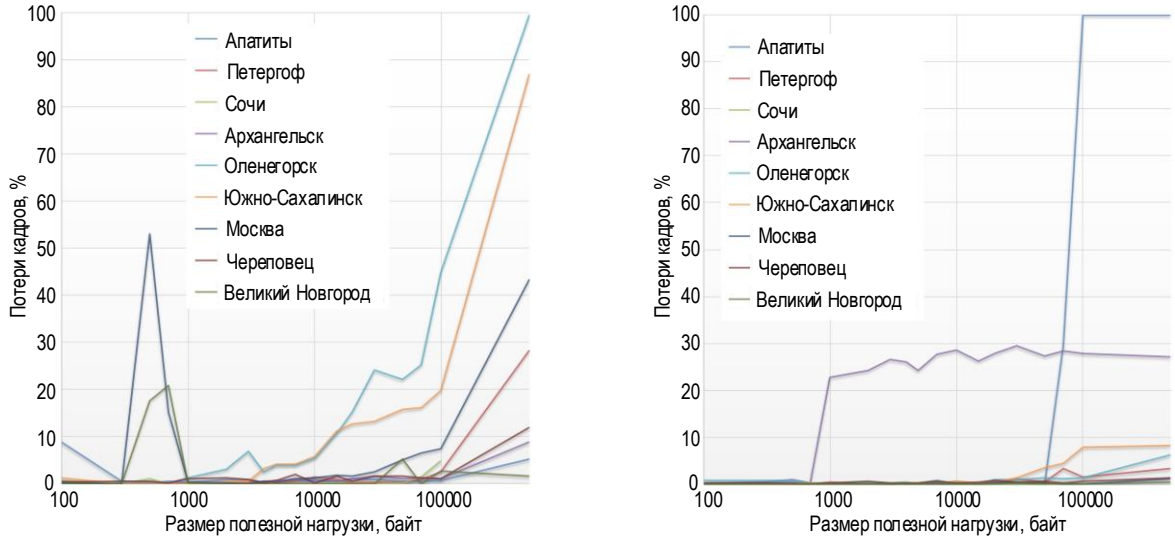


Рис. 6. Зависимость потерь кадров от размера полезной нагрузки в сетях 3G (a) и 4G (b)

Fig. 6. Dependence of Frame Loss Rate from the Payload in 3G (a) and 4G (b) Networks

Заключение

В результате проведенных исследований были получены следующие результаты.

Во-первых, величина задержки в КИО $t_{КИО}$ для передачи FPV-видео-потока (прикладной задержки) для любого варианта сочетания полезной нагрузки, расположения БВС и используемой технологии передачи данных подчиняется усеченному двухпараметрическому бета-распределению.

Во-вторых, зависимость величины $t_{КИО}$ от размера передаваемой полезной нагрузки имеет вид показательной возрастающей функции.

В-третьих, при передаче полезной нагрузки размером от 100 до 15000 байт величина $t_{КИО}$ остается неизменной для обеих технологий передачи данных (3G, LTE) и практически не зависит от расстояния между БВС и СВП, что обуславливает целесообразность использования при организации передачи видеопотока, формируемого нейросетевым кодеком, кадров размером до 15000 байт.

В-четвертых, для случаев передачи полезной нагрузки в диапазоне от 100 до 15000 байт уровень потери кадров не зависит от расстояния между БВС и СВП и технологии передачи данных, и составляет в среднем менее одного процента, в то время как для больших размеров полезной нагрузки данные характеристики играют более существенную роль.

Учет полученных результатов при моделировании функционирования КИО позволит осуществить выбор оптимальной конфигурации нейросетевых кодеков с целью повышения эффективности функционирования КИО. Кроме этого, полученные результаты могут быть полезны при организации каналов FPV-управления на основе стандартных видеокодеков.

Авторы выражают благодарность советнику ректора Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича Гурьеву Юрию Михайловичу, а также директору филиала ФГБУ ИАЦ Судебного департамента в Сахалинской области Гвоздовскому Дмитрию Геннадьевичу за помощь в сборе данных для проведения исследования.

Список источников

1. Просвирина Н.В. Анализ и перспективы развития беспилотных летательных аппаратов // Московский экономический журнал. 2021. № 10. С. 560–575. DOI:10.24411/2413-046X-2021-10619. EDN:PPWXEF

2. Мещанинова Е.Г., Николюкина В.О. Перспективы использования БПЛА при осуществлении земельного надзора // Экономика и экология территориальных образований. 2018. Т. 2. № 3. С. 122–128. DOI:10.23947/2413-1474-2018-2-3-122-128. EDN:UVLPBE

3. Курносенко Д.В. Перспективы применения беспилотных летательных аппаратов (БПЛА) при тушении лесных пожаров // Молодые ученые в решении актуальных проблем безопасности. 2023. С. 280–281. EDN:RULHAI

4. Чмелев В.С., Калюка В.И., Дмитренко М.Е. Обзор систем управления беспилотных летательных аппаратов общего пользования // Научно-практическая конференция «Технологии. Инновации. Связь» (Санкт-Петербург, Российская Федерация, 19 апреля 2021 г.). СПб.: ВАС, 2022. С. 279–286. EDN:KZXWEH

5. Гончерова Н.П., Примачук В.С. Беспилотные летательные аппараты в современном мире. Краткий обзор и перспективы развития // Символ науки. 2023. № 6-2. С. 12–14. EDN:WXXJBD
6. ITU-T H.264. Advanced Video Coding for Generic Audio-Visual Services. 2003.
7. ISO/IEC 23008-2. High Efficiency Video Coding. 2013.
8. Mousavi A., Patel A.B., Baraniuk R.G. A deep learning approach to structured signal recovery // Proceedings of the 53rd Annual Allerton Conference on Communication, Control, and COMPUTING (Allerton, Monticello, USA, 29 September – 02 October 2015). IEEE, 2016. PP. 1336–1343. DOI:10.1109/ALLERTON.2015.7447163
9. Li Y., Mandt S. Disentangled Sequential Autoencoder // arXiv:1803.02991v2. 2018. DOI:10.48550/arXiv.1803.02991
10. Березкин А.А., Ченский А.А., Киричек Р.В., Захаров А.А. Исследование конфигураций нейросетевых кодеков для адаптивной системы сжатия кадров FPV-видеопотока при управлении беспилотными системами. Часть I. Методика // Электросвязь. 2024. № 9. С. 42–51. DOI:10.34832/ELSV.2024.58.9.004. EDN:MWXFXN
11. Березкин А.А., Ченский А.А., Киричек Р.В., Захаров А.А. Исследование конфигураций нейросетевых кодеков для адаптивной системы сжатия кадров FPV-видеопотока при управлении беспилотными системами. Часть II. Эксперимент // Электросвязь. 2024. № 10. С. 59–69. DOI:10.34832/ELSV.2024.59.10.009. EDN:IWGJLY
12. Behnam M., Marau R., Pedreiras P. Analysis and optimization of the MTU in real-time communications over Switched Ethernet // Proceedings of the 16th International Conference on Emerging Technologies and Factory Automation (ETFA2011, Toulouse, France, 05–09 September 2011). IEEE, 2011. PP. 1–7. DOI:10.1109/ETFA.2011.6059021
13. Rajkumar K., Swaminathan P. Combining TCP and UDP for secure data transfer // Indian Journal of Science and Technology. 2015. Vol. 8. Iss. S9. PP. 285–291. DOI:10.17485/ijst/2015/v8iS9/65569
14. Garcia N.M., Freire M.M., Monteiro P.P. The Ethernet Frame Payload Size and Its Effect on IPv4 and IPv6 Traffic // Proceedings of the International Conference on Information Networking (Busan, South Korea, 23–25 January 2008). IEEE, 2008. PP. 1–5. DOI:10.1109/ICOIN.2008.4472813
15. Milanovic A., Srbljic S., Sruk V. Performance of UDP and TCP communication on personal computers // Proceedings of the 10th Mediterranean Electrotechnical Conference. Information Technology and Electrotechnology for the Mediterranean Countries (MeleCon 2000, Lemesos, Cyprus, 29–31 May 2000). IEEE, 2000. Vol. 1. PP. 286–289. DOI:10.1109/MELCON.2000.880422
16. Вивчарь Р.М., Птушкин А.И., Соколов Б.В. Методика многокритериального оценивания эффективности функционирования стохастических сложных технических систем // Авиакосмические приборостроение. 2022. № 7. С. 3–14. DOI:10.25791/aviakosmos.7.2022.1286. EDN:XCYDAI
17. Поршенев С.В., Копосов А.С. Использование аппроксимации Розенблатта-Парзена для восстановления функции распределения непрерывной случайной величины с ограниченным одномодальным законом распределения // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2013. № 92. С. 1–27. EDN:RNEGGN
18. Parzen E. On Estimation of a Probability Density Function and Mode // The Annals of Mathematical Statistics. 1962. Vol. 33. Iss. 3. PP. 1065–1076. DOI:10.1214/aoms/1177704472
19. Bowman A.W., Hall P., Titterington D. M. Cross-validation in nonparametric estimation of probabilities and probability densities // Biometrika. 1984. Vol. 71. Iss. 2. PP. 341–351. DOI:10.1093/biomet/71.2.341. EDN:ILOHEZ

References

1. Prosvirina N. Analysis and Prospects for the Development of Unmanned Aircraft. *Moscow Economic Journal*. 2021;10: 560–575. (in Russ.) DOI:10.24411/2413-046X-2021-10619. EDN:PPWXEF
2. Meschaninova E.G., Nikolukina V.O. Prospects for the Use of UAVs in the Implementation of the Land Supervision. *Economy and Ecology of Territorial Entities.* 2018;2(3):122–128. (in Russ.) DOI:10.23947/2413-1474-2018-2-3-122-128. EDN:UVLPBE
3. Kurnosenko D.V. Prospects for the Use of Unmanned Aerial Vehicles (UAVs) in Forest Fire Suppression. *Molodye uchenye v reshenii aktual'nyh problem bezopasnosti*. 2023;280–281. (in Russ.) EDN:RULHAI
4. Chmelev V.S., Kalyuka V.I., Dmitrenko M.E. Overview of Control Systems Unmanned Aerial Apparatus for General Use. *Proceedings of the Scientific and Practical Conference "Technologies. Innovations. Communications", 19 April 2021, Saint Petersburg, Russian Federation.* Saint Petersburg: Military Telecommunication Academy Publ.; 2022. p.279–286. (in Russ.) EDN:KZXWEH
5. Goncherova N.P., Primachuk V.S. Unmanned Aerial Vehicles in the Modern World. Brief overview and development prospects. *Simbol of Science*. 2023;6-2:12–14. (in Russ.) EDN:WXXJBD
6. ITU-T H.264. *Advanced Video Coding for Generic Audio-Visual Services*. 2003.
7. ISO/IEC 23008-2. *High Efficiency Video Coding*. 2013.
8. Mousavi A., Patel A.B., Baraniuk R.G. A deep learning approach to structured signal recovery. *Proceedings of the 53rd Annual Allerton Conference on Communication, Control, and COMPUTING, Allerton, 29 September – 02 October 2015, Monticello, USA*. IEEE; 2016. p.1336–1343. DOI:10.1109/ALLERTON.2015.7447163
9. Li Y., Mandt S. Disentangled Sequential Autoencoder. *arXiv:1803.02991v2*. 2018. DOI:10.48550/arXiv.1803.02991
10. Berezkin A.A., Chenskiy A.A., Kirichek R.V., Zaharov A.A. Research of Neural Network Codec Configurations for Adaptive FPV Video Stream Frame Compression System When Controlling Unmanned Systems. Part I. Methodology. *Elektrosvjaz'*. 2024;9:42–51. (in Russ.) DOI:10.34832/ELSV.2024.58.9.004. EDN:MWXFXN
11. Berezkin A.A., Chenskiy A.A., Kirichek R.V., Zaharov A.A. Research of Neural Network Codec Configurations for Adaptive FPV Video Stream Frame Compression System When Controlling Unmanned Systems. Part II. Experiment. *Elektrosvjaz'*. 2024;10:59–69. (in Russ.) DOI:10.34832/ELSV.2024.59.10.009. EDN:IWGJLY

12. Behnam M., Marau R., Pedreiras P. Analysis and optimization of the MTU in real-time communications over Switched Ethernet. *Proceedings of the 16th International Conference on Emerging Technologies and Factory Automation, ETFA2011, 05–09 September 2011, Toulouse, France*. IEEE; 2011. p.1–7. DOI:10.1109/ETFA.2011.6059021
13. Rajkumar K., Swaminathan P. Combining TCP and UDP for secure data transfer. *Indian Journal of Science and Technology*. 2015;8(S9):285–291. DOI:10.17485/ijst/2015/v8iS9/65569
14. Garcia N.M., Freire M.M., Monteiro P.P. The Ethernet Frame Payload Size and Its Effect on IPv4 and IPv6 Traffic. *Proceedings of the International Conference on Information Networking, 23–25 January 2008, Busan, South Korea*. IEEE; 2008. p.1–5. DOI:10.1109/ICOIN.2008.4472813
15. Milanovic A., Srbljic S., Sruk V. Performance of UDP and TCP communication on personal computers. *Proceedings of the 10th Mediterranean Electrotechnical Conference. Information Technology and Electrotechnology for the Mediterranean Countries, MeleCon 2000, 29–31 May 2000, Lemesos, Cyprus*. IEEE; 2000. vol.1. p.286–289. DOI:10.1109/MELCON.2000.880422
16. Vivchar R.M., Ptushkin A.I., Sokolov B.V. The Technique for Multi-Criteria Evaluation of the Performance of Stochastic Complex Technical Systems. *Aerospace Instrument-Making.* 2022;7:3–14. (in Russ.) DOI:10.25791/aviakosmos.7.2022.1286. EDN:XCYDAI
17. Porshenev S.V., Koposov A.S. Using Rozenblatt-Parzen Approximaion for Recovering a Cumulative Distribution Function of Continuous Random Variable With a Bounded Single-Mode Distribution Rule. *Polythematic online scientific journal of Kuban State Agrarian University*. 2013;92:1–27. (in Russ.) EDN:RNEGGN
18. Parzen E. On Estimation of a Probability Density Function and Mode. *The Annals of Mathematical Statistics*. 1962;33(3):1065-1076. DOI:10.1214/aoms/1177704472
19. Bowman A.W., Hall P., Titterington D. M. Cross-validation in nonparametric estimation of probabilities and probability densities. *Biometrika*. 1984;71(2):341–351. DOI:10.1093/biomet/71.2.341. EDN:ILOHEZ

Статья поступила в редакцию 26.01.2025; одобрена после рецензирования 18.02.2025; принята к публикации 24.02.2025.
The article was submitted 26.01.2025; approved after reviewing 18.02.2025; accepted for publication 24.02.2025.

Информация об авторах:

БЕРЕЗКИН Александр Александрович
кандидат технических наук, доцент кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
https://orcid.org/0000-0002-1748-8642

ВИВЧАРЬ Роман Михайлович
кандидат технических наук, доцент кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
https://orcid.org/0000-0003-3865-9102

ЧЕНСКИЙ Александр Александрович
инженер центра перспективных проектов и разработок Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
https://orcid.org/0009-0005-0832-8590

КИРИЧЕК Руслан Валентинович
доктор технических наук, профессор, ректор Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, заслуженный деятель науки Санкт-Петербурга
https://orcid.org/0000-0002-8781-6840

Киричек Р.В. является главным редактором 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.

Kirichek R.V. has been an editor-in-chief of the journal "Proceedings of Telecommunication Universities" since 2023, but has nothing to do with the decision to publish this article. The article has passed the review procedure accepted in the journal. The authors have not declared any other conflicts of interest.

Научная статья
УДК 621.391
https://doi.org/10.31854/1813-324X-2025-11-1-18-25
EDN:IZZZMV

Численное моделирование алгоритма гибридного прекодирования в миллиметровом диапазоне с использованием модели канала с открытым исходным кодом

Александр Александрович Калачиков ✉, 330rts@gmail.com
Сергей Леонидович Ремизов, selere1@gmail.com
Иван Иванович Резван, rezvan@sibsutis.ru

Сибирский государственный университет телекоммуникаций и информатики,
Новосибирск, 630102, Российская Федерация

Аннотация

Актуальность. *Использование многоантенных технологий в виде прекодирования сигналов является базовым условием повышения спектральной эффективности в современных системах мобильной связи в сочетании с переходом в диапазон миллиметровых волн. Условия распространения в миллиметровом диапазоне обуславливают обязательное использование антенных решеток в системах связи для компенсации потерь распространения и направленной передачи и приема сигналов пользователей. При передаче нескольких параллельных пространственных потоков данных пользователя используется прекодирование сигналов для реализации пространственного мультиплексирования и повышения спектральной эффективности системы. Рассматривается гибридная архитектура построения многоантенной системы и прекодирования, состоящая из аналоговой и цифровой частей. Но уменьшение количества радиочастотных трактов приводит к снижению возможности пространственного мультиплексирования по сравнению с полностью цифровой системой. В связи с этим является важной задача выбора оптимального количества радиочастотных трактов для получения максимального пространственного мультиплексирования с учетом текущих условий распространения сигналов и пространственной корреляции канала связи.*
Целью *исследования является определение влияния на спектральную эффективность выбора количества используемых радиочастотных трактов в системе гибридного прекодирования.*
Методы *исследования заключаются в имитационном моделировании алгоритма гибридного прекодирования. Для решения задачи численного моделирования гибридного прекодирования используются реализации канала MIMO миллиметровых волн, полученные при помощи открытого программного пакета модели канала QuaDRiGa.*
Результаты *представлены в виде функций распределения спектральной эффективности системы гибридного прекодирования, полученные на основе реализаций канала в определенном сценарии распространения.*
Новизна *состоит в численном определении параметров канала многоантенной системы связи в миллиметровом диапазоне и в использовании распределения собственных чисел матриц канала, полученных в модели, для оценки количества радиочастотных трактов, требуемых для достижения максимальной в данных условиях спектральной эффективности системы связи с гибридным прекодированием.*

Ключевые слова: *гибридное прекодирование в миллиметровом диапазоне, модель канала QuaDRiGa 3GPP, пространственное мультиплексирование, системы связи MIMO*

Ссылка для цитирования: Калачиков А.А., Ремизов С.Л., Резван И.И. Численное моделирование алгоритма гибридного прекодирования в миллиметровом диапазоне с использованием модели канала с открытым исходным кодом // Труды учебных заведений связи. 2025. Т. 11. № 1. С. 18–25. DOI:10.31854/ 1813-324X-2025-11-1-18-25. EDN:IZZZMV

Original research
https://doi.org/10.31854/1813-324X-2025-11-1-18-25
EDN:IZZZMV

Numerical Simulation of the Hybrid Precoding Algorithm in Millimeter Wave Band Using the Open Source Channel Model

Alexander A. Kalachikov ✉, 330rts@gmail.com
Sergey L. Remizov, selere1@gmail.com
Ivan I. Rezvan, rezvan@sibsutis.ru

Siberian State University of Telecommunications and Information Sciences,
Novosibirsk, 630102, Russian Federation

Annotation

Relevance. *The use of multi-antenna technologies in the form of signal precoding is a basic condition for increasing spectral efficiency in modern mobile communication systems in combination with the transition to the millimeter wave frequency band. Propagation conditions in the millimeter wave require the use of antenna arrays in communication systems to compensate for propagation losses and directional transmission and reception of user signals. When transmitting multiple parallel spatial user data streams, signal precoding is used to implement spatial multiplexing and improve the spectral efficiency of the system. A hybrid architecture for constructing a multi-antenna system and precoding, consisting of analog and digital parts, is considered. But reducing the number of radio frequency paths leads to a decrease in the possibility of spatial multiplexing compared to a completely digital system. In this regard, it is important to select the optimal number of radio frequency paths to obtain maximum spatial multiplexing, taking into account the current conditions of signal propagation and spatial correlation of the communication channel.*
The purpose *of the study is to determine the effect on the spectral efficiency of the choice of the number of used radio frequency paths in a hybrid precoding system.*
The research methods *consist of simulation modeling of a hybrid precoding algorithm. To solve the problem of numerical modeling of hybrid precoding, implementations of a MIMO channel of millimeter waves are used, obtained using the open channel model software package QuaDRiGa.*
The results *are presented in the form of distribution functions of the spectral efficiency of the hybrid precoding system, obtained on the basis of channel implementations in a certain propagation scenario.*
The novelty *lies in the numerical determination of the channel parameters of a multi-antenna communication system in the millimeter range and the use of the distribution of eigenvalues of the obtained channel implementations to study the influence of the number of radio frequency paths on the spectral efficiency of a communication system with hybrid precoding achievable under given conditions.*

Keywords: *hybrid precoding, millimeter-wave (mmWave) frequency bands, QuaDRiGa 3GPP channel model, multi-stream spatial multiplexing*

For citation: Kalachikov A.A., Remizov S.L., Rezvan I.I. Numerical Simulation of the Hybrid Precoding Algorithm in Millimeter Wave Band Using the Open Source Channel Model. *Proceedings of Telecommunication Universities.* 2025;11(1):18–25. (in Russ.) DOI:10.31854/1813-324X-2025-11-1-18-25. EDN:IZZZMV

1. Введение

Постоянно растущая потребность в высокой скорости передачи данных для большого количества абонентов в современных системах мобильной связи может быть реализована с применением нескольких базовых технологий. Спектральная эффективность системы мобильной связи увеличивается с применением многоантенной технологии MIMO, реализующей пространственное мультиплексирование. Конкретное увеличение спектральной эффективности в этом случае зависит от возможности реализации пространственной обработки сигналов и максимально точного использования свойств радиоканала.

Для повышения спектральной эффективности наиболее перспективным является переход в область миллиметрового частотного диапазона 30–300 ГГц в сочетании с применением многоантенных систем большой размерности (*от англ.* massive MIMO) на стороне базовой станции (БС) и использовании нескольких антенн в мобильном терминале пользователя. Канал с многолучевым распространением в диапазоне миллиметровых волн характеризуется высокими потерями на распространение, и для компенсации этих потерь необходимо использовать антенну, состоящую из большого количества элементов (антенную решетку), и последующую обработку сигналов с антенных элементов, обеспечивающую достаточный выигрыш решетки за счет когерентного сложения сигналов. Выигрыш состоит в увеличении отношения сигнал / шум. Технология MIMO с большим количеством антенных элементов позволяет обеспечить высокий выигрыш антенной решетки и увеличить отношение сигнал / шум для возможности организации одновременной передачи нескольких потоков данных в выделенном частотно-временно́м ресурсе (пространственного мультиплексирования) с пространственным разделением этих потоков данных, что значительно повышает спектральную эффективность системы связи [1–3].

В современных системах мобильной связи в диапазоне частот меньше 6 ГГЦ прекодирование реализовано в цифровом виде, векторы прекодирования вычисляются по заданным алгоритмам и применяются для формирования передаваемого сигнала раздельно для каждого антенного элемента. Каждому антенному элементу соответствует свой канал формирования сигналов, содержащий радиочастотный (РЧ) тракт. В диапазоне миллиметровых волн такая архитектура приводит к повышению стоимости и энергопотребления. Операцию прекодирования проводят раздельно в аналоговой и цифровой форме, аналоговое прекодирование реализуют в виде фазовращателей, цифровая часть прекодирования вычисляется для выбранных аналоговых векторов. Такая архитектура позволяет использовать сокращенное число РЧ трактов в сочетании с цифровым прекодированием. Гибридное прекодирование аппроксимирует оптимальную цифровую матрицу прекодирования произведением последней и аналоговой матрицы прекодирования, реализованной на основе аналоговых фазовращателей. Аппроксимация оптимального прекодера строится по текущей структуре пространственной многолучевости радиоканала [4, 5].

В статье рассматривается задача построения системной модели для определения характеристик гибридного прекодирования в диапазоне миллиметровых длин волн, состоящей из модели канала и многоантенной системы, реализующей алгоритм гибридного прекодирования. С использованием построенной модели системы определяются характеристики гибридного прекодирования в практических условиях развертывания системы связи с различными параметрами. Для получения реализаций канала, достоверно отражающей реальные условия распространения миллиметрового диапазона, используется модель канала с открытым исходным кодом и параметрами из результатов измерений в указанных условиях распространения.

2. Модель системы

Рассматриваемая система связи использует многоантенную технологию MIMO в сочетании с OFDM-сигналом, состоящим из N_F поднесущих. БС оборудована N_T передающими антеннами, мобильный терминал (МТ) пользователя оборудован N_R приемными антеннами. При передаче нескольких пространственных слоев данных формируется N_s потоков данных. Передатчик использует N_{RF} радиотрактов, предполагается выполнение условия $N_s \leq$ $\leq N_{RF} \leq N_T$. Используется цифровой прекодер с матрицей прекодирования $\mathbf{F}_{BB}$ размерностью $N_{RF} \times N_s$. Весовые векторы цифрового прекодера вычисляются для каждой поднесущей OFDM-сигнала в частотной области и применяются к вектору передаваемых символов $\mathbf{s}$ размером $N_s \times 1$ с использованием N_{RF} радиотрактов (рисунок 1).

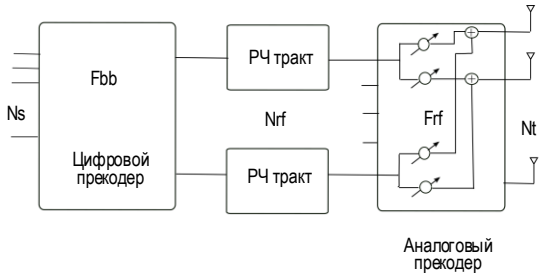


Рис. 1. Архитектура системы на основе гибридного прекодирования

Fig. 1. Architecture of Hybrid Precoder

После преобразования во временну́ю область и переноса сигнала на несущую частоту выполняется аналоговое прекодирование. Аналоговый прекодер $\mathbf{F}_{RF}$ размерностью $N_T \times N_{RF}$ реализован в виде набора фазовращателей и функционирует в РЧ диапазоне.

Передаваемый сигнал записывается в виде выражения:

$$\mathbf{x} = \mathbf{F}_{RF}\mathbf{F}_{BB}\mathbf{s}. \quad (1)$$

При использовании полностью подключенной архитектуры каждый РЧ тракт подключается ко всем антеннам через аналоговые фазовращатели.

Принятый сигнал записывается в следующем виде:

$$\mathbf{y} = \sqrt{\rho}\mathbf{H}\mathbf{F}_{RF}\mathbf{F}_{BB}\mathbf{s} + \mathbf{n}, \quad (2)$$

где $\mathbf{y}$ – вектор принятого сигнала размером $N_R \times 1$; $\mathbf{H}$ – матрица комплексных коэффициентов передачи канала размером $N_R \times N_T$; ρ – средняя мощность принятого сигнала; $\mathbf{n}$ – вектор комплексного нормального шума с нулевым средним значением и дисперсией σ_n^2 [5].

2.1. Модель канала миллиметрового диапазона

Свойства распространения в радиоканале миллиметрового диапазона отличаются небольшим числом многолучевых компонент вследствие малого уровня переотражений и высокого поглощения сигналов в данном диапазоне. В пространственно-временно́й модели канала используется ограниченное количество переотражений и рассеивателей в среде распространения, которые формируют пути распространения, группируемые в кластеры.

Канал $\mathbf{H}$ БС и МТ может быть описан в виде линейной комбинации управляющих векторов антенной решетки (векторов отклика антенной решетки) на стороне передачи и приема соответствующим пространственным путем распространения:

$$\mathbf{H} = \sum_{l=1}^{N_p} \alpha_l \, \mathbf{a_r}(\varphi_l^r, \theta_l^r) \mathbf{a_t}(\varphi_l^t, \theta_l^t), \qquad (3)$$

где N_p – количество путей распространения; α_l – комплексный коэффициент передачи канала, соответствующий пути l; векторы $\mathbf{a_r}(\varphi_l^r, \theta_l^r)$ и $\mathbf{a_t}(\varphi_l^t, \theta_l^t)$ – векторы отклика антенной решетки на стороне передачи и приема для направлений приема $(\varphi_l^r, \theta_l^r)$ и передачи $(\varphi_l^t, \theta_l^t)$ путей распространения l; угол φ_l^r – азимут принимаемого сигнала; угол θ_l^r – угол места принимаемого сигнала.

Векторы отклика антенной решетки $\mathbf{a_r}(\varphi_l^r, \theta_l^r)$ и $\mathbf{a_t}(\varphi_l^t, \theta_l^t)$ определяются структурой антенной решетки и длиной волны. Для планарной антенной решетки с равномерным расположением антенных элементов и количеством элементов по вертикали N_v и горизонтали N_h вектор антенной решетки вычисляется по выражению (4), где $k = \frac{2\pi}{\lambda}$ – волновое число: λ – длина волны; d – расстояние между антенными элементами [6].

$$\mathbf{a}(\varphi, \theta) = \frac{1}{\sqrt{N_v N_h}} \left[1, \dots, e^{kd\left((N_v - 1)\sin(\varphi)\sin(\theta) + (N_h - 1)\cos(\theta)\right)}\right]. \qquad (4)$$

2.2. Алгоритм гибридного прекодирования

Данный алгоритм гибридного прекодирования использует свойства ограниченного количества пространственных многолучевых компонент канала в диапазоне миллиметровых волн для аппроксимации оптимальной цифровой матрицы прекодирования. Текущее состояние канала в виде матрицы коэффициентов передачи $\mathbf{H}$ предполагается известным на стороне передатчика. На практике частотная характеристика канала измеряется при помощи пилотных поднесущих в составе OFDM-сигнала.

Вычисление матриц гибридного прекодирования основано на минимизации расстояния Евклида между гибридным прекодером в виде произведения матрицы цифрового прекодирования $\mathbf{F}_{BB}$ и матрицы аналогового РЧ прекодирования $\mathbf{F}_{RF}$ и полностью цифровым оптимальным прекодером $\mathbf{F}_{opt}$, вычисленными по текущим реализациям канала $\mathbf{H}$.

Оптимальный прекодер вычисляется при помощи сингулярного разложения матрицы канала $\mathbf{H} = \mathbf{U}\Sigma\mathbf{V}^*$, где матрицы $\mathbf{U}$ и $\mathbf{V}$ – левая и правая матрицы сингулярных векторов; Σ – диагональная матрица сингулярных чисел. Векторы прекодирования оптимального прекодера выбираются из матрицы $\mathbf{V}$ в виде подматрицы $\mathbf{F}_{opt} = \mathbf{V}_1$ размерностью $N_T \times N_s$.

Свойство разреженности канала миллиметрового диапазона позволяет выбрать компоненты аналогового прекодера $\mathbf{F}_{RF}$ из набора векторов отклика антенной решетки, соответствуюших основным многолучевым компонентам канала и в результате этого получить пространственное согласование с каналом и максимальный выигрыш антенной решетки. Выбор соответствующих векторов отклика производится через вычисление проекций векторов отклика на матрицу оптимального прекодера и выбор соответствующих N_s векторов отклика антенной решетки с максимальной величиной проекции.

После выбора N_s аналоговых векторов прекодирования вычисляются весовые векторы цифрового прекодера $\mathbf{F}_{BB}$. Данные векторы находятся как решение задачи по методу наименьших квадратов $\mathbf{F}_{BB} = (\mathbf{F}_{RF}^* \mathbf{F}_{RF})^{-1} \mathbf{F}_{RF} \mathbf{F}_{opt}$.

Полученный гибридный прекодер $\mathbf{F}_H = \mathbf{F}_{RF}\mathbf{F}_{BB}$ аппроксимирует оптимальный цифровой прекодер, вычисленный по текущей реализации канала. Операция вычисления прекодирования состоит в выборе набора N_{RF} векторов отклика антенной решетки, наиболее соответствующих текущим усло-

виям распространения в многолучевом канале, согласованных с угловым рассеянием компонент в канале и нахождению их оптимальной линейной комбинации $\mathbf{F}_{RF}\mathbf{F}_{BB}$ с цифровыми весовыми векторами прекодирования [6].

Количество реализуемых пространственных потоков зависит от текущих условий распространения в канале. Для оценки количества независимых пространственных потоков используется распределение собственных чисел матрицы $\mathbf{HH}^H$; индекс матрицы H обозначает комплексное сопряжение и транспонирование матрицы. Большие значения собственных чисел матрицы $\mathbf{HH}^H$ соответствуют пространственным каналам с большим коэффициентом передачи, количество таких каналов соответствует рангу матрицы канала и может использоваться для определения числа пространственных потоков, реализуемых в данных условиях распространения [7].

В качестве критерия эффективности гибридного прекодирования в системе с MIMO используется величина спектральной эффективности. Спектральная эффективность для текущей реализации канала **H** на выбранной поднесущей сигнала-OFDM и используемым гибридным прекодером вычисляется как (Бит/с/Гц):

$$R = \log_2\left(\left|\mathbf{I}_{N_s} + \frac{\rho}{N_s}\mathbf{H}\mathbf{F}_{RF}\mathbf{F}_{BB}\mathbf{F}_{RF}^H\mathbf{F}_{BB}^H\mathbf{H}^H\right|\right). \qquad (5)$$

Средняя спектральная эффективность вычисляется по большому числу реализаций канала [8, 9].

3. Результаты моделирования

Характеристики прекодирования определяются в виде средней спектральной эффективности, полученной в результате численного моделирования канала и вычисления весовых векторов прекодирования по полученным реализациям канала. Параметры моделирования представлены в таблице 1.

ТАБЛИЦА 1. Параметры моделирования

TABLE 1. Simulation Parameters

Модель канала	QuaDRiGa, версия 2.2
Сценарий развертывания	3GPP 38.901 UMi NLoS
Центральная частота	28 ГГЦ
Максимальное число многолучевых компонент	20
Количество поднесущих	2048
Полоса частот	400 МГц
Количество антенн БС	64
Тип антенны	Планарная антенная решетка
Количество антенн абонента	16
Количество РЧ трактов	4, 8
Отношение сигнал / шум	14 дБ

Для моделирования канала используется программный пакет с открытым исходным кодом QuaDRiGa, выпущенный в Fraunhofer HHI и реализованный на основе многочисленных измерений радиоканала в различных частотных диапазонах [10, 11]. Модель позволяет получить достоверные реализации канала для проведения моделирования различных алгоритмов обработки сигналов.

Результаты моделирования показаны на рисунках 2–4. На рисунке 2 показана функция распределения (CDF) первых четырех наибольших из 16 собственных значений матрицы $\mathbf{HH}^H$. Количество ненулевых собственных значений показывает ранг канала и количество собственных пространственных каналов, реализуемых в данных условиях распространения. Каждый собственный канал может осуществлять пространственную передачу для одного потока данных, и значение собственной величины определяет отношение сигнал / шум в этом пространственном канале. Наибольшие собственные значения соответствуют пространственным каналам с наибольшими коэффициентами передачи. По графику функции распределения можно определить распределение величин собственных значений, отличных от нуля. В данных условиях распространения на основе полученного множества реализаций канала количество реализуемых пространственных потоков с достаточным коэффициентом передачи не превышает трех, так как остальные собственные значения не превышают величины 0,1 в нормированном виде.

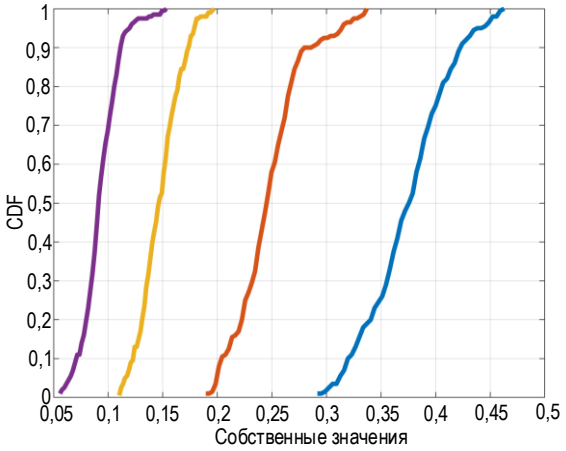
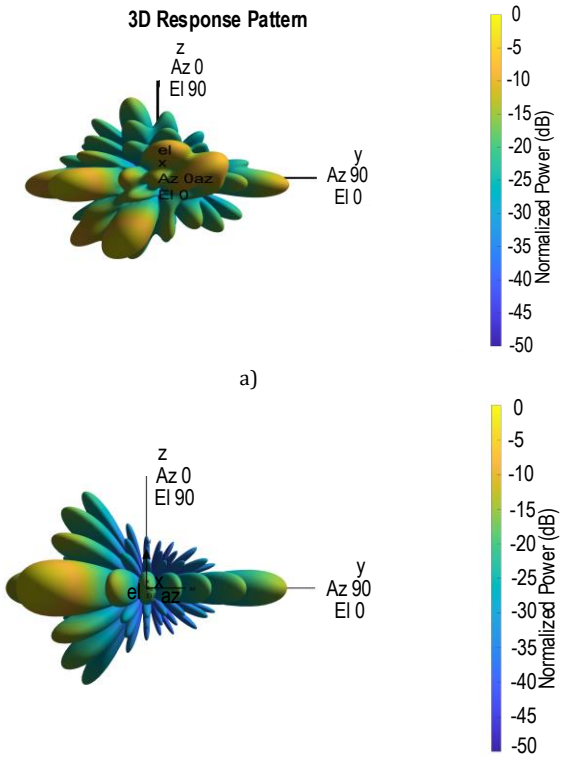


Рис. 2. Распределение наибольших четырех собственных значений

Fig. 2. CDF of First Four Maximum Eigenvalues

Рисунок 3а показывает синтезированную диаграмму направленности антенны в проекции Y–Z с применением вычисленного оптимального вектора прекодирования при передаче одного пространственного потока. Диаграмма направленности для антенной решетки – из 64 элементов, оптимальный весовой вектор прекодирования вычислен по

реализации канала с максимальным числом многолучевых компонент, равным 20. Среди этих компонент можно выделить 3–4 луча с различными направлениями и большим уровнем коэффициента передачи (4 максимума диаграммы направленности).



a)

b)

Рис. 3. Диаграммы направленности, полученные с использованием оптимального цифрового (a) и гибридного (b) прекодеров

Fig. 3. Array Pattern for Fully Digital (a) and Hybrid Precoder (b)

Гибридный прекодер [4] используется для оценки спектральной эффективности системы MIMO OFDM mmWave диапазона. Рисунок 3b показывает синтезированную диаграмму направленности антенны из 64 элементов в проекции *Y–Z* с применением вычисленного произведения аналогового и цифрового прекодеров по гибридной схеме при передаче одного пространственного потока. Весовой вектор гибридного прекодирования вычислен по реализации канала с максимальным числом многолучевых компонент, равным 20. В данных условиях развертывания системы гибридный прекодер аппроксимирует оптимальный цифровой прекодер и полученная диаграмма направленности соответствует пространственным лучам канала, по которым выбираются компоненты аналогового прекодера с последующим вычислением их комбинации.

На рисунке 4a показаны графики функции распределения средней спектральной эффективности для различного числа РЧ трактов в системе (при передаче двух независимых пространственных потоков для двух и четырех РЧ трактов). Оптимальный цифровой прекодер позволяет получить максимальную спектральную эффективность, аппроксимация в виде гибридного прекодера обеспечивает более низкую спектральную эффективность в этих условиях, и расстояние между кривыми больше при использовании двух РЧ трактов. В случае применения четырех РЧ трактов расстояние уменьшается, гибридный прекодер $\mathbf{F}_{RF}\mathbf{F}_{BB}$ дает более близкую аппроксимацию оптимального прекодера $\mathbf{F}_{opt}$, так как увеличивается количество векторов отклика антенной решетки. Это позволяет более точно выбрать вектор отклика для направления путей распространения с большим коэффициентом передачи.

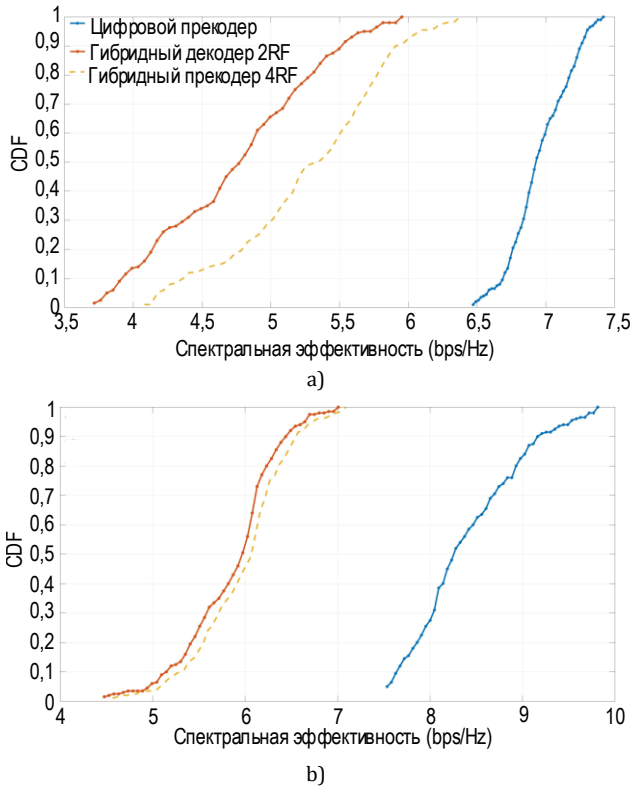


Рис. 4. Функция распределения спектральной эффективности при двух (a) и четырех (b) пространственных потоках данных

Fig. 4. CDF of the Sum Rate for Two (a) and Four (b) Spatial Layers

На рисунке 4b показана функция распределения спектральной эффективности при передаче четырех пространственных потоков и использовании 4 и 8 РЧ трактов. При таких системных параметрах при передаче четырех пространственных потоков произведение матрицы аналогового прекодера и матрицы цифрового прекодера $\mathbf{F}_{RF}\mathbf{F}_{BB}$ более точно аппроксимируют оптимальный прекодер и обеспечивают бóльшую спектральную эффективность, чем система с 2 и 4 РЧ трактами. Но спектральная

эффективность гибридного прекодера при увеличении количества РЧ трактов увеличивается незначительно, т. к. количество основных путей распространения не превышает четырех, что также отражается в распределении собственных чисел.

4. Заключение

Представлены результаты численного моделирования алгоритма гибридного прекодирования в системе MIMO миллиметрового диапазона. Моделирование канала миллиметрового диапазона выполнено для типового сценария малой зоны обслуживания в условиях городской застройки с использованием программного пакета QuaDRiGa. Результаты моделирования показывают, что спектральная эффективность с использованием гибридного прекодирования увеличивается, если количество пространственных потоков увеличивается, но не превышает ранга канала. Показателем количества реализуемых пространственных потоков является значения максимальных собственных чисел матрицы канала. При увеличении числа РЧ трактов спектральная эффективность увеличивается при наличии достаточного числа многолучевых компонент радиоканала с высоким коэффициентом передачи, которые соответствуют собственным числам матрицы канала.

Список источников

1. Roh W., Seol J.Y., Park J., Lee B, Lee J., Yungsoo K. Millimeter-wave beamforming as an enabling technology for 5G cellular communications: Theoretical feasibility and prototype results // IEEE Communications Magazine. 2014. Vol. 52. Iss. 2. PP. 106–113. DOI:10.1109/MCOM.2014.6736750
2. Molisch A.F., Ratnam V.V., Han S., Li Z., Nguyen S.L.H. Hybrid Beamforming for Massive MIMO: A survey // IEEE Communications Magazine. 2017. Vol. 55. Iss. 9. PP. 134–141. DOI:10.1109/MCOM.2017.1600400
3. Носов В.И. Методы повышения помехоустойчивости систем радиосвязи с использованием технологии MIMO и пространственно-временной обработки сигналов. Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2014. 316 с. EDN:VRTAXT
4. Sun S., Rappaport T.S., Shafi M., Tang P., Zhang J., Smith P.J. Propagation Models and Performance Evaluation for 5G Millimeter-Wave Bands // IEEE Transactions on Vehicular Technology. 2018. Vol. 67. Iss. 9. PP. 8422–8439. DOI:10.1109/TVT.2018.2848208. EDN:YIPMFV
5. El Ayach O., Rajagopal S., Abu-Surra S., Pi Z., Jr. Heath R.W. Spatially Sparse Precoding in Millimeter Wave MIMO Systems // IEEE Transactions on Wireless Communications. 2014. Vol. 13. Iss. 3. PP. 1499–1513. DOI:10.1109/TWC.2014.011714.130846
6. Heath R.W., Gonzalez-Prelcic N., Rangan S., Roh W., Sayeed A.M. An Overview of Signal Processing Techniques for Millimeter Wave MIMO Systems // IEEE Journal of Selected Topics in Signal Processing. 2016. Vol. 10. Iss. 3. PP. 436–453. DOI:10.1109/JSTSP.2016.2523924
7. Rappaport T.S., Gutierrez F., Ben-Dor E., Murdock J.N., Qiao Y., Tamir J.I. Broadband Millimeter-Wave Propagation Measurements and Models Using Adaptive-Beam Antennas for Outdoor Urban Cellular Communications // IEEE Transactions on Antennas and Propagation. 2013. Vol. 61. Iss. 4. PP. 1850–1859. DOI:10.1109/TAP.2012.2235056
8. Sohrabi F., Yu W., Hybrid digital and analog beamforming design for large-scale antenna arrays // IEEE Journal of Selected Topics in Signal Processing. 2016. Vol. 10. Iss. 3. PP. 501–513. DOI:10.1109/JSTSP.2016.2520912
9. Payami S., Ghoraishi M., Dianati M. Hybrid beamforming for large antenna arrays with phase shifter selection // IEEE Transactions on Wireless Communications. 2016. Vol. 15. Iss. 11. PP. 7258–7271. DOI:10.1109/TWC.2016.2599526
10. Jaeckel S., Raschkowski L., Boerner K., Thiele L. QuaDRiGa: A 3-D Multicell Channel Model with Time Evolution for Enabling Virtual Field Trials // IEEE Transactions on Antennas Propagation. 2013. Vol. 62. Iss. 6. PP. 3242–3256. DOI:10.1109/TAP.2014.2310220
11. Jaeckel S., Raschkowski L., Boerner K., Thiele L., Burkhardt F., Eberlein E. QuaDRiGa – Quasi Deterministic Radio Channel Generator. User Manual and Documentation. Tech. Rep. v2.2.0. Berlin: Fraunhofer Heinrich Hertz Institute, 2019.

References

1. Roh W., Seol J.Y., Park J., Lee B, Lee J., Yungsoo K. Millimeter-wave beamforming as an enabling technology for 5G cellular communications: Theoretical feasibility and prototype results. *IEEE Communications Magazine*. 2014;52(2):106–113. DOI:10.1109/MCOM.2014.6736750
2. Molisch A.F., Ratnam V.V., Han S., Li Z., Nguyen S.L.H. Hybrid Beamforming for Massive MIMO: A survey. *IEEE Communications Magazine*. 2017;55(9):134–141. DOI:10.1109/MCOM.2017.1600400
3. Nosov V.I. *Methods of Increasing the Noise Immunity of Radio Communication Systems Using MIMO Technology and Space-Time Signal Processing*. Novosibirsk: Siberian State University of Telecommunications and Informatics Publ.; 2014. 316 p. (in Russ.) EDN:VRTAXT
4. Sun S., Rappaport T.S., Shafi M., Tang P., Zhang J., Smith P.J. Propagation Models and Performance Evaluation for 5G Millimeter-Wave Bands. *IEEE Transactions on Vehicular Technology*. 2018;67(9):8422–8439. DOI:10.1109/TVT.2018.2848208. EDN:YIPMFV
5. El Ayach O., Rajagopal S., Abu-Surra S., Pi Z., Jr. Heath R.W. Spatially Sparse Precoding in Millimeter Wave MIMO Systems. *IEEE Transactions on Wireless Communications*. 2014;13(3):1499–1513. DOI:10.1109/TWC.2014.011714.130846

6. Heath R.W., Gonzalez-Prelcic N., Rangan S., Roh W., Sayeed A.M. An Overview of Signal Processing Techniques for Millimeter Wave MIMO Systems. *IEEE Journal of Selected Topics in Signal Processing*. 2016;10(3):436–453. DOI:10.1109/JSTSP.2016.2523924.

7. Rappaport T.S., Gutierrez F., Ben-Dor E., Murdock J.N., Qiao Y., Tamir J.I. Broadband Millimeter-Wave Propagation Measurements and Models Using Adaptive-Beam Antennas for Outdoor Urban Cellular Communications. *IEEE Transactions on Antennas and Propagation.* 2013;61(4):1850–1859. DOI:10.1109/TAP.2012.2235056

8. Sohrabi F., Yu W., Hybrid digital and analog beamforming design for large-scale antenna arrays. *IEEE Journal of Selected Topics in Signal Processing*. 2016;10(3):501–513. DOI:10.1109/JSTSP.2016.2520912

9. Payami S., Ghoraishi M., Dianati M. Hybrid beamforming for large antenna arrays with phase shifter selection. *IEEE Transactions on Wireless Communications*. 2016:15(11):7258–7271. DOI:10.1109/TWC.2016.2599526

10. Jaeckel S., Raschkowski L., Boerner K., Thiele L. QuaDRiGa: A 3-D Multicell Channel Model with Time Evolution for Enabling Virtual Field Trials. *IEEE Transactions on Antennas Propagation*. 2013;62(6):3242–3256. DOI:10.1109/TAP.2014.2310220

11. Jaeckel S., Raschkowski L., Boerner K., Thiele L., Burkhardt F., Eberlein E. *QuaDRiGa – Quasi Deterministic Radio Channel Generator. User Manual and Documentation. Tech. Rep. v2.2.0*. Berlin: Fraunhofer Heinrich Hertz Institute; 2019.

Статья поступила в редакцию 23.12.2024; одобрена после рецензирования 10.02.2025; принята к публикации 13.02.2025.
The article was submitted 23.12.2024; approved after reviewing 10.02.2025; accepted for publication 13.02.2025.

Информация об авторах:

КАЛАЧИКОВ Александр Александрович
кандидат технических наук, доцент кафедры радиотехнических систем Сибирского государственного университета телекоммуникаций и информатики
https://orcid.org/0000-0003-1235-6314

РЕМИЗОВ Сергей Леонидович
кандидат технических наук, доцент военного учебного центра Сибирского государственного университета телекоммуникаций и информатики
https://orcid.org/0009-0003-7836-2087

РЕЗВАН Иван Иванович
кандидат технических наук, доцент, доцент кафедры радиотехнических систем Сибирского государственного университета телекоммуникаций и информатики
https://orcid.org/0009-0002-6875-7061

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-2025-11-1-26-33
EDN:EHOZQY

Система радиосвязи с широкополосными сигналами в условиях присутствия ретранслированных помех

Валерий Иванович Коржик ✉, korzhik.vi@sut.ru
Рафаэль Рифгатович Биккенин, bikkenin.rr@sut.ru

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

Аннотация

В настоящее время помехоустойчивость приема в условиях действия преднамеренных помех, похожих на передаваемые сигналы, играет решающую роль при передаче данных, содержащих важную информацию. В системах радиосвязи с широкополосными сигналами, называемых также сигналами с расширенным спектром, обеспечивалась защита от преднамеренных помех, формируемых постановщиком в условиях априорной неопределенности о передаваемых сигналах. Однако в настоящее время противодействующая сторона способна выявить параметры этих сигналов (вид модуляции, скорость передачи, длительность посылок и др.). Поэтому необходима разработка новых методов защиты от современных угроз для безопасной и помехоустойчивой передачи сообщений, в том числе и при создании ретранслированных помех.

***Цель** статьи – повышение помехоустойчивости передачи широкополосных сигналов при действии ретранслированных помех, мощность которых превышает мощность применяемых сигналов.*

***Сущность** предлагаемого решения заключается в использовании для передачи информации широкополосных фазочастотномодулированных сигналов, формируемых при помощи независимых непредсказуемых псевдослучайных последовательностей, различных на передаваемой и непередаваемой частотах. Мгновенные фазы сигналов при этом рандомизируются независимо при передаче на битовых интервалах. С применением современного математического аппарата выводится соотношение для расчета вероятности битовой ошибки. Доказывается, что при правильно выбранных параметрах вероятности битовых ошибок приближаются к величинам, при которых возможно эффективное применение кодов, корректирующих независимые ошибки, что позволит обеспечить надежную доставку важной информации в заданные сроки.*

***Научная новизна** решения состоит в применении для защиты передаваемой информации непредсказуемой псевдослучайной последовательности также на непередаваемой в текущий момент частоте, в рандомизированном сдвиге фазы на каждом битовом интервале при формировании широкополосного сигнала и, кроме того, в оптимизации параметров предлагаемой системы радиосвязи.*

***Теоретическая значимость** состоит в корректном выводе формул для расчета вероятности битовой ошибки и оценке возможности дальнейшего применения корректирующих кодов.*

***Практическая значимость** заключается в возможности проектирования широкополосных систем радиосвязи, обладающих необходимой помехоустойчивостью при действии ретранслированных помех с энергетическим превосходством над легитимными сигналами.*

Ключевые слова: *широкополосные сигналы, ретранслированные помехи, псевдослучайные последовательности, некогерентный прием, коды корректирующие ошибки*

Ссылка для цитирования: Коржик В.И., Биккенин Р.Р. Система радиосвязи с широкополосными сигналами в условиях присутствия ретранслированных помех // Труды учебных заведений связи. 2025. Т. 11. № 1. С. 26–33. DOI:10.31854/1813-324X-2025-11-1-26-33. EDN:EHOZQY

Original research
https://doi.org/10.31854/1813-324X-2025-11-1-26-33
EDN:EHOZQY

Wireless System Using Spread Spectrum Signals under the Conditions of Possible Jamming by Retransmitted Interference

Valery I. Korzhik✉, korzhik.vi@sut.ru
Rafael R. Bikkenin, bikkenin.rr@sut.ru

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

Annotation

Presently, it is very important to design wireless systems that are resistant to jamming by adversary. It is well known technology to execute so called spread spectrum signals in order to prevent such attacks, especially under the conditions when enemy is superior i1n power against legitimate users. Moreover, adversary is able to estimate legitime signal parameter (type of modulation, duration of intervals ctr) However, such approach be vulnerable in the case of the use by adversary so called retransmitted interferences.

The purpose *of this article is to increase the efficiency of spread spectrum signals transmission under the action of retransmitted interference, the power of which exceeds the power of the legitimate signals.*

The essence *of the proposed solution is to use spread spectrum phase-frequency modulated signals for information transmission, generated using independent unpredictable pseudorandom sequences that are different at the transmitted and non-transmitted frequencies. Instant phases are randomized independently for bit intervals at the transmitting side. Theoretically, using appropriated mathematical technique, the formula is derived for calculating of the bit error probability for the proposed system with different choice of its parameters. It is proved that for correctly selected parameters, the probabilities of bit errors are approaching to such values that occurs qcceptable to use next* error correcting codes, *which will ensure reliable delivery of important information.*

The scientific novelty *of our method consists in the use an unpredictable pseudorandom sequence at a frequency that is not currently being transmitted, in a randomized phase shift at each bit interval when forming a broadband signal, as well as in optimizing the parameters for the proposed radio communication system, that improved significantly further use of error-correcting code.*

The theoretical significance *consists in the correct proof of the formula for the bit error probabilities and further estimation the conditions for application of error correction codes.*

The practical significance *lies in design of interference proof wireless communication system that after some further elaboration of synchronization system and error correction codes, can be applied in practice under very hard interference environment.*

Keywords: *spread spectrum signals, retransmitted interference, pseudorandom sequences, non-coherent receiver, error correcting codes*

For citation: Korzhik V.I., Bikkenin R.R. Wireless System Using Spread Spectrum Signals under the Conditions of Possible Jamming by Retransmitted Interference. *Proceedings of Telecommunication Universities.* 2025;11(1):26–33. (in Russ.) DOI:10.31854/1813-324X-2025-11-1-26-33. EDN:EHOZQY

Введение

Построение систем связи, защищенных от воздействия преднамеренных помех, остается актуальной задачей и в настоящее время. Давно известно [1–4], что эффективным средством защиты от таких помех является использование так называемых *широкополосных сигналов* (ШПС) или иначе – *сигналов с расширенным спектром*. В данной статье рассматриваются только методы *прямого расширения спектра*. В этом случае каждый бит сообщения передается при помощи последовательного генерирования *псевдослучайной последовательности* (ПСП) бит с дополнительной — типично фазовой или частотной модуляцией каждого элемента (*чипа*) этой последовательности.

В работах [1–4] было показано, что, по крайней мере, при когерентном приеме фазомодулированных двоичных сигналов на каждом чипе и невозможности оценки фаз сигналов в каждом чипе постановщиком помех вероятность ошибок принимаемого сообщения P_e будет экспоненциально убывать к нулю при возрастании параметра $q\sqrt{n}$, где $q = U_c^2/U_п^2$ – отношение сигнал / шум в точке приема, а n – база ШПС. Отсюда следует, что при невозможности оценки фаз сигналов в каждом чипе постановщиком помех при условии, что $q \ll 1$, т. е., когда постановщик помех имеет значительное преимущество по мощности по сравнению с легальным пользователем, за счет увеличения базы сигнала n можно обеспечить любую приемлемую для легального пользователя вероятность ошибки бита P_e. (Однако, заметим, что при этом происходит обратно пропорциональное n уменьшение скорости передачи сообщений).

Совершенно другой сценарий возникает при возможности создания противником так называемой *ретранслированной модулированной помехи.* В этом случае постановщик помех за минимально короткое время способен обнаружить работающую легитимную станцию, определить параметры ее сигнала (вид модуляции, скорость передачи, длительность посылок и др.), по которым сформировать помеху, а затем настроить свой передатчик и осуществить его излучение. Интервал времени, затрачиваемый на последние процедуры, называется временем реакции станции помех $T_р$. В современных станциях помех $T_р \leq 100$ мкс [5].

При определенных условиях, создавая ретранслированную помеху, постановщик помех имеет возможность демодулировать каждый чип легитимного сигнала на интервале значительно меньшем, чем длительность этого чипа T_{ch}, и затем модулировать оставшуюся часть этого чипа случайным образом, сохраняя или инвертируя ее. Схема такого сценария показана на рисунке 1, где d_{12} – расстояние от передающей легитимной станции до станции помех; d_{13} – от передающей до приемной станции легитимных пользователей; d_{23} – от передатчика станции помех до легитимной приемной станции.

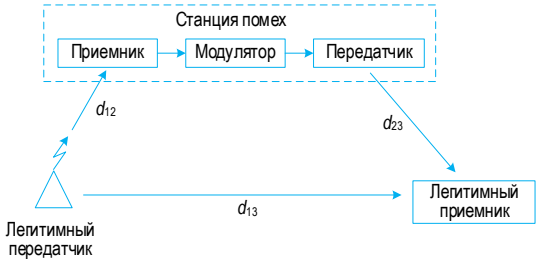


Рис. 1. Схема сценария создания ретранслированных помех широкополосному сигналу

Fig. 1. A Scheme of a Scenario for Retransmitted Interference Creating against Legitimate Spread Spectrum Signal

Тогда условие малого запаздывания ретранслированной помехи относительно легитимного сигнала можно записать в следующем виде:

$$T_р + \frac{(d_{12} + d_{23} - d_{13})}{C} \ll T_{ch},$$

где C – скорость распространения радиоволн (света); T_{ch} – длительность одного чипа.

Рассмотрим, для примера, частный, но практически реальный случай, когда $d_{12} = 1$ км, $d_{23} = 0{,}5$ км, а «треугольник» распространения радиоволн представим, как треугольник с углом 90 °, напротив стороны длиной d_{13}. Тогда $d_{13} = \sqrt{d_{12}^2 + d_{23}^2}$. (Очевидно, что и для любого заданного треугольника расчет расстояния d_{13} не представляет труда). Для рассматриваемого случая получим, что $d_{13} \approx 1{,}12$ км, а $T_р + (d_{12} + d_{23} - d_{13})/C \approx 101$ мкс. Если длительность чипа ШПС равна $T_{ch} = 1$ мс, что соответствует скорости битовой передачи информации $v = 1/(nT_{ch})$, то при этом запаздывание помех относительно полезного сигнала оказывается примерно равным $T_{ch}/10$, т. е. допустимой величине. (Конечно, при другом расположении станций относительно друг друга запаздывание помехи может оказаться и значительно больше, чем $T_{ch}/10$). Рассмотрим далее наиболее благоприятный случай для постановщика помех, когда время запаздывания принимается равным нулю.

В следующих разделах настоящей статьи рассматривается математическая модель системы радиосвязи, предлагаются новые передающие и приемные части алгоритмов, использующих ШПС, рассчитывается вероятность ошибки бита для данного метода и формулируются дополнительные задачи, которые необходимо решить для практической реализации предлагаемой системы защиты ШПС от преднамеренных ретранслированных помех. (Заметим, что данная статья является значительным расширением работы тех же авторов, опубликованной в трудах Международной научно-технической конференции [6]).

2. Описание алгоритмов модуляции и демодуляции для ШПС, защищенных от преднамеренных ретранслированных помех

Модулятор формирует сигналы $S_i(t), i = 0, 1$, $t \in (0, T_b)$ для передачи по радиоканалу двоичного символа $i = 0$ или $i = 1$ на битовом интервале $(0, T_b)$ по следующему правилу:

$$S_i(t) = \begin{cases} U_s\, \pi(t) \sin \omega_0 t, \text{для } i = 0 \\ U_s\, \pi'(t) \sin \omega_1 t, \text{для } i = 1 \end{cases}, \qquad (1)$$

где U_s – амплитуда сигнала; ω_0 – несущая частота при передаче бита $i = 0$; ω_1 – несущая частота при передаче бита $i = 1$:

$$\pi(t) = \sum_{j=1}^{n} a_j\, \pi(t - jT_{ch}),$$

$$\pi'(t) = \sum_{j=1}^{n} a'_j\, \pi(t - jT_{ch}),$$

$$\pi(t - jT_{ch}) = \begin{cases} 1, t \in [(j-1)T_{ch}, jT_{ch}] \\ 0, t \overline{\in} [(j-1)T_{ch}, jT_{ch}] \end{cases},$$

где T_{ch} – длительность «чипа» ШПС; $a_j \in \pm 1$ – j-й элемент ПСП на передаваемой частоте; $a'_j \in \pm 1$ – j-й элемент ПСП на непередаваемой на данном бите частоте; $n = T_b/T_{ch}$ – количество «чипов» на битовом интервале в ШПС (база).

Важнейшим требованием, предъявляемым к ПСП a'_j, $j = 1, 2, \dots, n$, является *непредсказуемость* данной последовательности, если известна ПСП на передаваемой частоте $a_j, j = 1, 2, \dots, n$, а также непредсказуемость ПСП, если известны все предыдущие элементы ПСП. (К пояснению данного требования авторы еще вернуться при обсуждении процедуры демодуляции).

Канал связи между легитимными пользователями и канал для передачи помехи будем описывать моделью постоянного (незамирающего) канала со случайной фазой ВЧ-несущей. Таким образом, предполагается, что здесь реализуется модель канала *прямой видимости*, т. е. без многолучевости и замираний. Тогда сигнал, принимаемый легитимным демодулятором, будет иметь вид:

$$Z(t) = \mu S_i(t, \varphi_{s_i}) + n_i(t), i = (0, 1), 0 \le t \le T_b, \quad (2)$$

где $\mu S_i(t, \varphi_{s_i})$ – сигнал, представленный в (1); φ_{s_i} – случайная фаза, добавляемая в канале связи; μ – коэффициент затухания сигнала в канале связи; $n_i(t)$ – преднамеренная помеха, создаваемая на передаваемой (или непередаваемой) частоте.

(Заметим, что постановщику помех очевидно известно, на какой частоте передается сигнал для каждого чипа).

Поскольку при обработке на приеме принимаемой смеси ШПС с помехой возникает эффект «обеления» помехи, т. е. она приобретает свойства, подобные естественному шуму, оптимальным демодулятором для легитимного канала связи можно считать оптимальный некогерентный (квадратурный) приемник [7], использующий известные ПСП, как для передаваемой, так и для непередаваемой частот, алгоритм которого имеет вид (3), где $rect(x) = \begin{cases} 0, x \ge 0 \\ 1, x < 0 \end{cases}$.

Наилучшая стратегия помехи для данной легитимной системы ШПС связи состоит в следующем: с вероятностью 1/2 находится битовый интервал и на нем не передается помеха, и с вероятностью также 1/2 выбирается битовый интервал и на нем создается инверсная помеха на передаваемой частоте и шумовая помеха на непередаваемой частоте. Это следует из результатов [8], где доказано, что оптимальная помеха как простым, так и сложным сигналам с дискретной фазовой модуляцией, синтезированная без учета информации о начальных фазах передаваемых сигналов, представляет собой также фазомодулированное колебание со значениями информационной фазы, изменяющимися на 180 ° с постоянной величиной амплитуды и со случайной начальной фазой, равномерно распределенной на интервале от 0 до 2π, несущая частота и длительность посылок которой совпадают с соответствующими параметрами сигнала, а моменты смены информационной фазы или полярности элементов помехи и сигнала на входе подавляемого приемника совпадают по времени. При энергетическом превосходстве такой помехи над сигналом в приемнике будет регистрироваться помеха вместо передаваемого сигнала.

После подстановки получаемых в таких случаях принимаемого полезного сигнала с помехой $Z(t)$ в (3) и проведения несложных тригонометрических преобразований находим решающее правило легитимного приемника (4), где $U_п$ – амплитуда помехи; $\varphi = \varphi_s - \varphi_п$ – разность фаз сигнала и помехи; $\varepsilon, \hat{\varepsilon}$ – взаимно независимые гауссовские случайные величины (в силу *центральной предельной теоремы теории вероятностей*), имеющие нулевые математические ожидания и дисперсии $\sigma^2 = U_п^2 T_{ch}^2 n/4$.

$$i = rect\left[\left(\sum_{j=1}^{n} a_j \int_{T_{ch}(j-1)}^{T_{ch}j} Z(t)\cos\omega_0 t dt\right)^2 + \left(\sum_{j=1}^{n} a_j \int_{T_{ch}(j-1)}^{T_{ch}j} Z(t)\sin\omega_0 t dt\right)^2 - \right.$$
$$\left. - \left(\sum_{j=1}^{n} a'_{j+1} \int_{T_{ch}(j-1)}^{T_{ch}j} Z(t)\cos\omega_1 t dt\right)^2 - \left(\sum_{j=1}^{n} a'_{j+1} \int_{T_{ch}(j-1)}^{T_{ch}j} Z(t)\sin\omega_1 t dt\right)^2\right]. \quad (3)$$

$$i = rect\left[\frac{n^2 T_{ch}^2}{4}(U_s^2 + U_п^2 + 2U_s U_п \cos\varphi) - (\varepsilon^2 + \hat{\varepsilon}^2)\right]. \quad (4)$$

Вероятность регистрации бита $i = 1$, когда в действительности передавался бит $i = 0$, равна вероятности того события, что выражение в скобках в формуле (4) будет отрицательным и зависящим от φ, т. е. иметь вид (5), где $\eta = (\varepsilon^2 + \hat{\varepsilon}^2)$; $A = \frac{n^2 T_{ch}^2}{4}(U_s^2 + U_п^2 + 2U_s U_п \cos\varphi)$.

Предполагая (как и раньше), что ε и $\hat{\varepsilon}$ – независимые гауссовские величины с параметрами $(0, \sigma^2)$, получаем, что $\eta = (\varepsilon^2 + \hat{\varepsilon}^2)$ будет случайной величиной, распределенной по *экспоненциальному закону*, т. е. η имеет плотность вероятности (6).

Подставляя (6) в (5), вычисляя интеграл и учитывая, что $\sigma^2 = U_п^2 T_{ch}^2 n/4$, получим (7), где $q_0 = U_s^2/U_{п0}^2$ – отношение мощностей *сигнал / шум* на передаваемой частоте ω_0; $q_1 = U_s^2/U_{п1}^2$ – отношение мощностей *сигнал / шум* на непередаваемой частоте ω_1.

Предполагая, что разность фаз φ сигнала и помехи равномерно распределена на интервале от 0 до 2π, получаем в (8) вероятность ошибки P_e, усредняя $P_e(\varphi)$ на указанном интервале. (В дальнейшем это утверждение обосновывается тем, что, как будет отмечено впоследствии, эта фаза принудительно рандомизируется на каждом битовом интервале в передатчике. И тогда, как известно, при любых начальных распределениях φ, суммарная фаза будет иметь равномерное распределение на интервале от 0 до 2π. В (8) $I_0\left(\frac{nq_1}{\sqrt{q_0}}\right)$ – модифицированная функция Бесселя первого рода и нулевого порядка [9]:

$$I_0\left(\frac{nq_1}{\sqrt{q_0}}\right) = \frac{1}{2\pi}\int_0^{2\pi} \exp\left[\left(\frac{nq_1}{\sqrt{q_0}}\cos\varphi\right)\right] d\varphi.$$

Найдем оптимальное значение q_0, которое обеспечивает постановщику помех наибольшую вероятность ошибки P_e. Введем в (8) новую переменную $y = 1/\sqrt{q_0}$. Тогда вместо (8) получим (9).

Для нахождения максимума $P_e(y)$ вычислим производную от (9) и приравняем ее к нулю (10), что эквивалентно решению уравнения (11). (Заметим, что при выводе (10) авторы воспользовались известным фактом [9], что:

$$\frac{dI_0(y)}{dy} = I_1(y),$$

где $I_1(y)$ – модифицированная функция Бесселя первого рода первого порядка).

После простых преобразований (11) получим окончательно уравнение (12), где $a = nq_1$.

Численное решение уравнения (12) дает при $a \geq 5$ приближенный результат $y \approx 1$, т. е. $q_0 \approx 1$. Заметим, что выбор $q_0 = 1$ является физически очевидным, поскольку создание противофазной помехи при совпадении ПСП сигнала на передаваемой частоте и этой помехи, позволит приблизить к нулю сумму сигнала и такой помехи только при одинаковых значениях их амплитуд и фаз.

$$P_e(\varphi) = Pr\left[\frac{n^2 T_{ch}^2}{4}(U_s^2 + U_п^2 + 2U_s U_п \cos\varphi) - (\varepsilon^2 + \hat{\varepsilon}^2) \leq 0\right] = Pr\{\eta \geq A\}. \quad (5)$$

$$w(\eta) = \begin{cases} \frac{1}{2\sigma^2}\exp(-\eta/2\sigma^2), \eta \geq 0 \\ 0, \eta < 0. \end{cases} \quad (6)$$

$$P_e(\varphi) = \int_A^\infty \omega(\eta)\, d\eta = \int_A^\infty \frac{1}{2\sigma^2} e^{-\frac{\eta}{2\sigma^2}}\, d\eta = e^{-\frac{A}{2\sigma^2}} = \exp\left[-\frac{n}{2}\left(q_1 + \frac{q_1}{q_0} + 2\frac{q_1}{\sqrt{q_0}}\cos\varphi\right)\right]. \quad (7)$$

$$P_e = \frac{1}{2\pi}\int_0^{2\pi} \exp\left[-\frac{n}{2}\left(q_1 + \frac{q_1}{q_0} + 2\frac{q_1}{\sqrt{q_0}}\cos\varphi\right)\right] d\varphi = \exp\left[-\frac{n}{2}\left(q_1 + \frac{q_1}{q_0}\right)\right]\frac{1}{2\pi}\int_0^{2\pi} \exp\left(\frac{nq_1}{\sqrt{q_0}}\cos\varphi\right) d\varphi =$$
$$= \exp\left[-\frac{n}{2}\left(q_1 + \frac{q_1}{q_0}\right)\right] I_0\left(\frac{nq_1}{\sqrt{q_0}}\right). \quad (8)$$

$$P_e(y) = \exp\left[-\frac{nq_1}{2}(1 + y^2)\right] I_0(nq_1 y). \quad (9)$$

$$\frac{dP_e(y)}{dy} = -\exp\left[-\frac{nq_1}{2}(1 + y^2)\right] I_0(nq_1 y) nq_1 y + \exp\left[-\frac{nq_1}{2}(1 + y^2)\right] I_1(nq_1 y) nq_1 = 0. \quad (10)$$

$$-I_0(nq_1 y) nq_1 y + I_1(nq_1 y) nq_1 = 0. \quad (11)$$

$$I_1(ay) = y I_0(ay). \quad (12)$$

Что же касается непередаваемой частоты (ω_1, при передаче бита $i = 0$), то на ней необходимо создать максимальный отклик приемника для обеспечения ошибки на этом битовом интервале: постановщик помех должен стремиться к выбору максимальной величины q_1. Однако для противодействия получения постановщиком помех максимального отклика на непередаваемой частоте, т. е. максимизации величин $(\varepsilon^2 + \hat{\varepsilon}^2)$, при демодуляции сигнала необходимо, чтобы ПСП $a'_j, j = \overline{1,n}$ на непередаваемой частоте не совпадала бы с ПСП $a_j, j = \overline{1,n}$ на передаваемой частоте этого бита и, более того, знание постановщиком помех ПСП a_j (за счет свойств ретрансляции) никак не помогало бы предсказанию a'_j. Иначе на приеме будет выполняться когерентное сложение сигналов на чипах (см. последние два элемента в круглых скобках (3)). И тогда отклик на непередаваемой частоте увеличится и не будет иметь плотности вероятности (6).

Поскольку, с одной стороны, такой метод заведомо приводит к увеличению вероятности ошибки бита P_e, а, с другой стороны, его легко исключить, обеспечив независимость ПСП a_j и a'_j на передаваемой и на непередаваемой частотах, соответственно, то расчет P_e для такого случая мы производить не будем.

Описанный выше алгоритм защиты от ретранслированных помех имеет одну негативную особенность, заключающуюся в том, что ошибки, возникающие среди передаваемых бит, могут оказаться сильно коррелированными. Это приведет к сложностям при использовании кодов, корректирующих независимые ошибки. Если же для ослабления этого фактора произвести декорреляцию ошибок при помощи, например *перемежения* битовых символов [7], то такой подход может привести к значительной задержке принимаемых сигналов. Поэтому мы предлагаем ввести на передаче принудительные фазовые сдвиги сигналов на каждом битовом интервале, причем обеспечить статистическую независимость этих фазовых сдвигов при помощи дополнительного чисто случайного генератора. Тогда можно будет полагать, что модель ошибок при использовании корректирующих кодов будет соответствовать биномиальной модели, что существенно упростит выбор кодов, исправляющих лишь независимые ошибки.

Упрощая формулу (8) для случая $q_0 = 1$, получим:

$$P_e = \exp\left[-\frac{n}{2}\left(q_1 + \frac{q_1}{q_0}\right)\right] I_0\left(\frac{nq_1}{\sqrt{q_0}}\right) = \\ = \exp(-nq_1) I_0(nq_1) = \exp(-a) I_0(a), \quad (13)$$

где $a = nq_1$.

В таблице 1 представлены результаты расчета вероятностей битовых ошибок P_e, полученных при использовании формулы (13) и выборе оптимизированного параметра $q_0 \approx 1$, а также для различных значений параметра $a = nq_1$.

ТАБЛИЦА 1. Результаты вычислений вероятностей битовой ошибки P_e по (13) при $q_0 = 1$ и различных значениях параметра $a = nq_1$

TABLE 1. Results of the Bit Error Probability Calculation by (13) under and Different Values

a	10	20	50	100	1000	5000	10000
P_e	0,13	0,0905	0,057	0,0399	0,012	0,00564	0,00399

Результаты, представленные в таблице 1, показывают, что, например, даже при двухкратном превосходстве по мощности помехи над полезным сигналом, когда $q_1 = 0{,}5$, а база легитимного сигнала $n = 100$, параметр $a = 50$, и ему будет тогда соответствовать вероятность ошибки $P_e \approx 0{,}057$.

Согласно формуле Шеннона, для пропускной способности двоичного симметричного канала без памяти [10] выражение для расчета пропускной способности можно записать в следующем виде:

$$C = 1 + P_e \log_2 P_e + (1 - P_e)\log_2(1 - P_e). \quad (14)$$

Подставляя $P_e \approx 0{,}057$ в (14), получим $C \approx 0{,}449$, что дает надежду на повышение достоверности при использовании даже жесткого декодирования корректирующими кодами (например, LDPC, *аббр. от англ.* Low-Density Parity-Check Code, кодами с малой плотностью проверок на четность [11, 12] или турбокодами [11, 13]) без катастрофического снижения скорости передачи данных по легитимному каналу.

Произведем ориентировочный расчет времени задержки передачи данных для предложенного метода. Ранее в статье было отмечено, что можно ожидать битовой скорости до 10 кбит/с в канале связи. Тогда длительность одного чипа будет равна 0,1 мс, и, следовательно, длительность соответствующей передачи одного бита при $n = 100$ оказывается 10 мс. Если теперь выбрать корректирующий код с длиной блока 100 и кодовой скоростью 0,4 (см. выражение (14)), получим, что 40 бит данных могут быть надежно (при адекватном выборе кода) переданы легитимному корреспонденту примерно за время 1 с. Конечно, это достаточно большая величина, при которой могут быть надежно приняты разве лишь короткие сообщения. Но такая оценка позволяет понять, насколько эффективны ШПС при возможности создания ретранслированных помех. Очевидно, что такая оценка может быть уточнена с учетом реальных параметров сигналов и ограничений на требуемое время доставки определенных объемов данных.

3. Заключение

В предложенной вниманию читателей журнала «Труды учебных заведений связи» статье авторы предлагают систему ШПС в условиях радиоэлектронного подавления и, в частности, для наиболее тяжелого ее сценария – создания ретранслированной помехи, которая при превосходстве ее мощности над мощностью сигналов способна полностью подавить легитимную линию связи, использующую традиционные методы ШПС. Такой сценарий не принадлежит к фантазиям авторов, а соответствует реальной ситуации, когда станция помех расположена достаточно близко от подавляемого приемника.

Хотя использование фазомодулированных и частотно-модулированных сигналов, по-видимому, не является новым, однако авторы полагают, что применение непредсказуемой ПСП на непередаваемой частоте может претендовать на некоторую оригинальность. Также оригинальным является рандомизированный сдвиг фаз на каждом битовом интервале, что существенно улучшает дальнейшее применение корректирующих ошибки кодов.

Заметим, что теоретический расчет вероятностей битовых ошибок P_e по формуле (13), а также оптимизация параметра q_0, являются новыми результатами. Причем важно отметить, что достоверность получения этих результатов не требует никакой дополнительной экспериментальной проверки исходной модели, поскольку нормализация помехи $(\varepsilon^2 + \hat{\varepsilon}^2)$ в (4) достаточно надежно обеспечивается при хороших свойствах датчика ПСП и достаточно большой базе сложного сигнала n, а равномерная случайность и взаимная независимость на битовых интервалах фазы φ выполняется принудительно при помощи хорошего генератора шума.

Конечно, было бы интересно проверить всю предложенную модель системы связи в условиях ретранслированных помех при помощи имитационного компьютерного моделирования, но, как было только что отмечено, это не является необходимым для подтверждения достоверности теоретических выводов.

Заметим, однако, что прежде, чем пытаться реализовать данную систему на практике, необходимо тщательно проработать алгоритм синхронизации по битовым и блоковым интервалам в условиях помех, в том числе и специально ориентированных на подавление именно такой системы связи [14, 15]. Наконец, для того, чтобы окончательно убедиться в отсутствии дополнительных уязвимостей предлагаемой системы связи от воздействия радиоэлектронного подавления, необходимо проверить, не сможет ли постановщик помех с высокой точностью оценить мгновенную фазу передаваемого легитимного сигнала, поскольку в противном случае он сумеет создать в точности противофазную помеху (см. $\varphi = \pi$ в формуле (5)), и тогда реализуется полный «обрыв» легитимного канала передачи данных.

Интересно отметить, что в отличие от случая применения ШПС при отсутствии ретранслированных помех (т. е. при «невычислимости» ПСП постановщиком помех), вероятность битовой ошибки P_e достаточно быстро убывает с ростом базы сигнала n (см. [1–4]). В то же время, как видно из таблицы 1, при фиксированной величине q_1 вероятность ошибки P_e с ростом n убывает сравнительно медленно. По-видимому, это та «цена», которую необходимо «заплатить» за присутствие ретранслированной помехи. Тем не менее P_e, хоть и медленно, но, все же монотонно убывает, что позволяет обеспечить надежную связь при дальнейшем использовании корректирующих кодов.

Список источников

1. Proakis J. Digital Communications. N.Y.: McGraw-Hill, 1995.
2. Dixon R.C. Spread Spectrum Systems. John Willy and Sons, 1979.
3. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. Пер. с англ. М.: Вильямс, 2007. 1104 с.
4. Голдсмит А. Беспроводные коммуникации. Пер. с англ. М.: Техносфера, 2011. 904 с. EDN:QMWIPL
5. Борисов В.И., Зинчук В.М., Лимарев А.Е. [и др.] Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты. М.: Радио и связь, 2003. 384 с. EDN:QMMHCF
6. Korjik V., Bikkenin R. Performance analysis of the enhanced PN spread spectrum system in the presence of jamming by modulated retransmitted signal // Proceedings of the 5th International Symposium on Spread Spectrum Techniques and Applications (Sun City, South Africa, 04–04 September 1998). IEEE, 1998. PP. 809–811. DOI:10.1109/ISSSTA.1998.722490
7. Финк Л.М. Теория передачи дискретных сообщений. М.: Советское радио, 1970. 728 с.
8. Агафонов А.А., Ложкин К.Ю., Поддубный В.Н. Методология и результаты синтеза и оценки эффективности преднамеренных помех приемникам дискретных сигналов // Радиотехника и электроника. 2003. Т. 48. № 8. С. 956–962. EDN:OOQISJ
9. Справочник по специальным функциям с формулами, графиками и таблицами / Под ред. М. Абрамовица и И. Стиган. Пер. с англ. М.: Наука, 1979. 832 с.
10. Шеннон К.Э. Работы по теории информации и кибернетике. Пер. с англ. М.: Изд-во иностр. лит., 1963. 830 с.
11. MacKay D.J.C., Neal R.M. Near Shannon Limit Performance of Low-Density Parity Check Codes // Electronics Letters. 1996. Vol. 32. Iss. 18. DOI:10.1049/el:19961141

12. MacKay D.J.C. Information Theory, Inference and Learning Algorithms. Cambridge University Press, 2003. 640 p.
13. Berrou C., Glavieux A., Thitmajshima P. Near optimum error correcting coding and decoding: Turbo-codes // IEEE Transactions on Commutations. 1996. Vol. 44. Iss. 10. PP. 1261–1271. DOI:10.1109/26.539767
14. Журавлев В.И. Поиск и синхронизация в широкополосных системах. М.: Радио и связь, 1986. 240 с. EDN:WIYMEJ
15. Борисов В.И., Зинчук В.М., Лимарев А.Е., Мухин Н.П., Нахмансон Г.С. Помехозащищенность систем радиосвязи с расширением спектра сигналов модуляцией несущей псевдослучайной последовательностью. М.: Радио и связь, 2003. 640 с.

References

1. Proakis J. *Digital Communications*. N.Y.: McGraw-Hill; 1995.
2. Dixon R.C. *Spread Spectrum Systems*. John Willy and Sons; 1979.
3. Sklar B. *Digital Communications. Fundamentals and Applications*. Prentice Hall; 2001.
4. Goldsmith A. *Wireless Communications*. Cambridge University Press; 2005.
5. Borisov V.I., Zinchuk V.M, Limarev A.E., Muhin N.P., Shestopalov V.I. ECM-Resistance of Frequency-Hopping of Spread – Spectrum Communications Systems. Moscow: Radio and Communications Publ.; 2003. 384 p. (in Russ.) EDN:QMMHCF
6. Korjik V., Bikkenin R. Performance analysis of the enhanced PN spread spectrum system in the presence of jamming by modulated retransmitted signal. *Proceedings of the 5th International Symposium on Spread Spectrum Techniques and Applications*, 04–04 September 1998, Sun City, South Africa. IEEE; 1998. p.809–811. DOI:10.1109/ISSSTA.1998.722490
7. Fink L.M. *Theory of Transmission of Discrete Messages.* Moscow: Soviet Radio Publ.; 1970. 728 p. (in Russ.)
8. Agafonov A.A., Lozhkin K.Yu., Poddubny V.N. Methodology and Results of Synthesis and Estimation of the Efficiency of Malicious Interferences for Discrete Signal Receivers. *Journal of Radio Electronics.* 2003;48(8):956–962. (in Russ.) EDN:OOQISJ
9. Abramowitz M. Stegun I.A. *Handbook of Mathematical Functions with Formulas, Graphs and Mathematical Tables*. National Bureau of Standards Applied Mathematics Series. 55. Issued June 1964.
10. Shannon C.E. A mathematical theory of communication. *Bell System Technical Journal*. 1948;27:379–423 and 623–656.
11. MacKay D.J.C., Neal R.M. Near Shannon Limit Performance of Low-Density Parity Check Codes. *Electronics Letters*. 1996;32(18). DOI:10.1049/el:19961141
12. MacKay D.J.C. *Information Theory, Inference and Learning Algorithms*. Cambridge University Press; 2003. 640 p.
13. Berrou C., Glavieux A., Thitmajshima P. Near optimum error correcting coding and decoding: Turbo-codes. *IEEE Transactions on Commutations*. 1996;44(10):1261–1271. DOI:10.1109/26.539767
14. Zhuravlev V.I. *Search and Synchronization in Spread Spectrum Systems*. Moscow: Radio and Communications Publ.; 1986. 240 p. (in Russ.) EDN:WIYMEJ
15. Borisov V.I., Zinchuk V.M., Limarev A.E., Mukhin N.P., Nakhmanson G.S. Noise Immunity of radio communication systems with Spread Spectrum Signal by Carrier Pseudorandom Sequence Modulation. Moscow: Radio and Communications, Publ.; 2003. 640 p. (in Russ.)

Статья поступила в редакцию 24.01.2025; одобрена после рецензирования 03.02.2025; принята к публикации 17.02.2025.
The article was submitted 24.01.2025; approved after reviewing 03.02.2025; accepted for publication 17.02.2025.

Информация об авторах:

КОРЖИК Валерий Иванович
доктор технических наук, профессор, профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
https://orcid.org/0000-0002-8347-6527

БИККЕНИН Рафаэль Рифгатович
доктор технических наук, профессор, профессор кафедры электроники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича

Коржик В.И. 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.

Korzhik V.I. 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
https://doi.org/10.31854/1813-324X-2025-11-1-34-43
EDN:OIKCAN

Аналитическое описание квазиравномерной последовательности импульсов первого типа

Юрий Александрович Никитин, nikitin.ua@sut.ru

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

Аннотация

В настоящее время системы пассивного цифрового синтеза частот находят все более широкое применение в возбудителях радиопередающих устройств и в гетеродинах радиоприемных устройств систем радиолокации, радионавигации и радиосвязи. В основе таких систем лежит конечный автомат – устройство или программа, которая может изменять свои состояния в дискретные моменты времени, целократные тактовому интервалу, имеют конечное число устойчивых состояний, т. е. обладают конечной памятью. Поэтому ***актуальна*** *задача аналитического описания состояний таких автоматов в любой наперед заданный момент времени.*

Цель *настоящей работы заключается в компактном описании функций переходов и функций выходов автоматов, используемых в системах пассивного цифрового синтеза частот. Существенной особенностью анализа и проектирования таких автоматов является требование к минимизации уровня функциональной фазоимпульсной модуляции выходного потока импульсов, т. е. минимизация временно́й ошибки между потоком формируемых импульсов и идеально равномерным (гипотетическим) потоком импульсов требуемой частоты. Квазипериодическую последовательность импульсов с минимальным временны́м уклонением от гипотетической последовательности называют квазиравномерной импульсной последовательностью. Кроме того, цель настоящей работы заключается в корректном доказательстве оптимальности квазиравномерной последовательностью с точки зрения минимума функциональной фазоимпульсной модуляции выходного потока импульсов.*

Методы *исследования основываются на использовании теоретико-числовых преобразований основного параметра автомата – его коэффициента деления N = P/Q, где P и Q, соответственно, число тактовых и выходных импульсов на периоде неравномерности выходного потока квазиравномерной последовательности.*

Результат. *Получены* ***новые*** *аналитические выражения для описания состояний автомата в любом наперед заданном моменте времени, выражения для мгновенной (текущей) фазы автомата и мгновенной (текущей) частоты следования квазиравномерной импульсной последовательности на его выходе. Такие выражения удобны для анализа и расчета автоматов, используемых в системах пассивного цифрового синтеза частот.*

Теоретическая значимость *заключается в разработке метода описания состояний оптимального конечного автомата во временно́й области и получение соответствующих аналитических выражений.*

Ключевые слова: *синтез частот, конечный автомат, функция переходов, функция выходов, цепная дробь, рациональное число, квазиравномерная последовательность импульсов, функциональная фазоимпульсная модуляция*

Ссылка для цитирования: Никитин Ю.А. Аналитическое описание квазиравномерной последовательности импульсов первого типа // Труды учебных заведений связи. 2025. Т. 11. № 1. С. 34–43. DOI:10.31854/1813-324X-2025-11-1-34-43. EDN:OIKCAN

Original research
https://doi.org/10.31854/1813-324X-2025-11-1-34-43
EDN:OIKCAN

Quasi-Uniform Sequence Analytical Description of the First Type Pulses

Yury A. Nikitin, nikitin.ua@sut.ru

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

Annotation

At present, passive digital frequency synthesis systems are increasingly used in exciters of radio transmitting devices and in heterodynes of radio receiving devices of radar, radio navigation and radio communication systems. Such systems are based on a finite state machine - a device or program that can change its states at discrete moments of time, integer multiples of the clock interval, have a finite number of stable states, i.e. have a finite memory. Therefore, the problem of analytical description of the states of such machines at any predetermined moment of time is ***relevant****.*
The purpose *of this work is to compactly describe the transition functions and output functions of machines used in passive digital frequency synthesis systems. An essential feature of the analysis and design of such machines is the requirement to minimize the level of functional phase-pulse modulation of the output pulse flow, i.e. minimization of the time error between the flow of generated pulses and the ideally uniform (hypothetical) flow of pulses of the required frequency. A quasi-periodic pulse sequence with a minimum time deviation from the hypothetical sequence is called a quasi-uniform pulse sequence. In addition, the purpose of this work is to correctly prove the optimality of a quasi-uniform sequence from the point of view of the minimum functional phase-pulse modulation of the output pulse flow.*
The research methods *are based on the use of number-theoretical transformations of the main parameter of the machine - its division coefficient N = P / Q, where P and Q, respectively, are the number of clock and output pulses in the period of non-uniformity of the output flow of the quasi-uniform sequence.*
Result*. New analytical expressions for describing the states of the machine at any predetermined moment of time, expressions for the instantaneous (current) phase of the machine and the instantaneous (current) frequency of the quasi-uniform pulse sequence at its output are obtained. Such expressions are convenient for analyzing and calculating machines used in passive digital frequency synthesis systems.*
The theoretical significance *lies in the development of a method for describing the states of an optimal finite state machine in the time domain and obtaining the corresponding analytical expressions.*

Keywords: *frequency synthesis, finite state machine, transition function, output function, continued fraction, rational number, quasi-uniform pulse sequence, functional phase-pulse modulation*

For citation: Nikitin Yu.A. Quasi-Uniform Sequence Analytical Description of the First Type Pulses. *Proceedings of Telecommunication Universities.* 2025;11(1):34–43. (in Russ.) DOI:10.31854/1813-324X-2025-11-1-34-43. EDN:OIKCAN

Конечным автоматом (КА) в теории алгоритмов называется математическая абстракция, позволяющая описывать пути изменения состояния объекта в зависимости от его текущего состояния и входных данных при условии, что общее возможное количество состояний конечно [1–5].

Наибольший интерес для синтеза частот представляют оптимальные автоматы в том смысле, что временна́я ошибка между одноименными перепадами (точками на числовой оси) на выходе автомата и ближайшими к ним перепадами идеально равномерной последовательности (ИРП) той же требуемой частоты не превышает длительности тактового интервала и является минимально возможной величиной для класса цифровых структур. Такие автоматы назовем *оптимальными*. На их выходе формируется квазиравномерная последовательность (КРП) импульсов (одноименных перепа-

дов), которую также можно рассматривать в виде точек на числовой оси.

В технике синтеза частот КА реализуют с помощью простейших элементов – триггеров, счетчиков импульсов, накапливающих сумматоров, поглотителей импульсов, регистров и т. д. [6]. В цифровых синтезаторах частоты в области тактовых частот $f_{опВЧ}$ до единиц–десятков мегагерц КА можно выполнить программно, до сотен мегагерц – с помощью программируемых логических матриц, а на еще более высоких тактовых частотах – только аппаратно на сверхбыстродействующей логике.

Заметим, что одноименные перепады на выходе автомата появляются в дискретные моменты времени, кратные его тактовому интервалу $T_{опВЧ}$. Но синтезируемая частота $f_{выхНЧ} = 1/T_{выхНЧ}$ с номером Q в общем случае не целократна тактовой частоте $f_{опВЧ}$ с номером $P > Q$, т. е. коэффициент деления автомата $N = P/Q$ есть рациональное число в виде неправильной дроби. Например, для случая $P = 16$, $Q = 7$ и $N = 16/7 = 2 + 2/7$ на рисунке 1 показаны временны́е ошибки КРП относительно импульсов ИРП, что приводит к появлению функциональной фазоимпульсной модуляции.

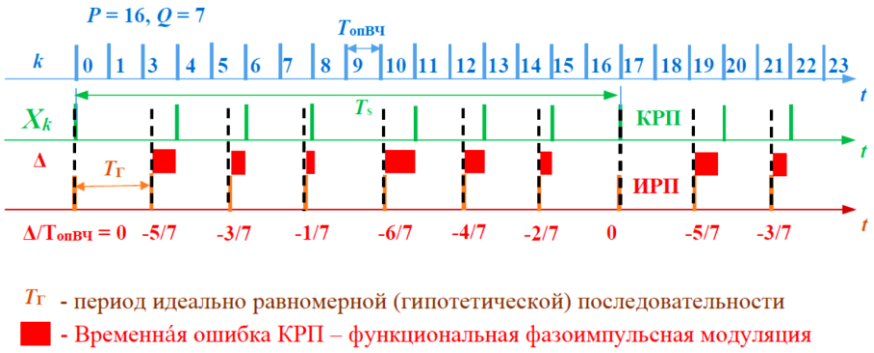


Рис. 1. Функциональная фазоимпульсная модуляция КРП на выходе КА

Fig. 1. Functional Phase-Pulse Modulation of the Quasi-Uniform Pulse (QUS) at the Output of the Finite State Machine (FSM)

КА могут иметь несколько выходов, например, выход переполнения ρ_k и выход текущей суммы S_k (рисунок 2), и по своим разным выходам соответствовать автоматам разных типов.

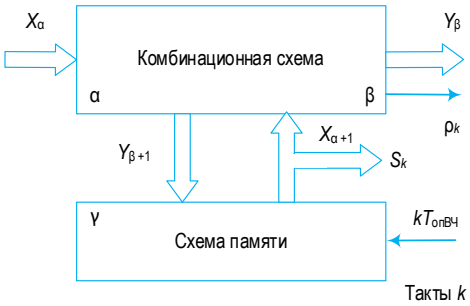


Рис. 2. Формальная структура КА

Fig. 2. Formal Structure of the FSM

При описании автомата полагаем, что он функционирует в дискретные равноотстоящие моменты времени, которые занумерованы целыми положительными числами, и других меток времени не имеет. Интервал времени $T_{опВЧ} = 1/f_{опВЧ}$ назовем тактом автомата, формальная структура последнего приведена на рисунке 2. Длительность такта автомата должна превышать интервал времени $T_{КА}$ между соседними моментами достижения автоматом устойчивых состояний.

Таким образом, для текущего дискретного времени T_k на входе КА можно записать в следующем виде:

$$T_k = 0,1,\ldots,\left\lfloor k\left(\frac{t}{T_{опВЧ}}\right)\right\rfloor,\ldots,T_k \geq T_{КА},$$

где t – текущее время; $\lfloor * \rfloor$ – оператор выделения целой части числа, меньшей или равной ему; $k = 0, 1, 2,\ldots$ – натуральное число.

Автомат с X_α входами и X_β выходами можно представить в виде соединения комбинационной схемы или логического преобразователя с размерностью по входу и выходу α и β, соответственно, и схемы (элемента) памяти в цепи обратной связи размерности γ. При этом состояния входа и выхода комбинационной схемы – суть состояния входа и выхода КА, а его внутренними состояниями и, возможно, состояниями выхода являются состояния схемы памяти, поскольку выходами КА, наряду с выходами комбинационной схемы, также могут служить и выходы схемы памяти.

Важным параметром автомата является его коэффициент деления $N = f_{опВЧ}/f_{выхНЧ} = P/Q$ (рациональное число), разложение которого в цепную дробь по алгоритму Евклида имеет вид:

$$N = \frac{P}{Q} = N_0 + \frac{1}{q_1 + \frac{1}{q_2 + \cdots \frac{1}{q_r}}},$$

где $N_0 \in \mathbb{Z}$; $q, q_2, \ldots q_{r-1}, q_r \in \mathbb{N}$; r – длина цепной дроби; $\mathbb{Z}$ – подгруппа целых чисел, $\mathbb{N}$ – множество натуральных чисел.

Любое рациональное число $N = P/Q$ представимо в виде цепной дроби *единственным* образом. Коэффициенты этой дроби являются неполными частными в алгоритме Евклида [7–10].

Решение уравнения с целочисленными коэффициентами (диофантова уравнения):

$$nP + mQ + d = 0$$

с помощью теоретико-числовых преобразований записывается в виде:

$$\begin{cases} n = (-1)^{r-1} dQ_{r-1} - Qz, \\ m = (-1)^{r} dP_{r-1} + Pz, \end{cases}$$

где $z \in \mathbb{Z}$; P_{r-1}, Q_{r-1} – соответственно, числитель и знаменатель предпоследнего частного при разложении рационального числа N в цепную дробь по алгоритму Евклида.

В устройствах цифрового синтеза частот КА можно представить в виде дискретной параметрической цепи – черного ящика, функционирующего по определенному, но жесткому и наперед заданному алгоритму, задаваемому пользователем. Существенная особенность автоматов, используемых для синтеза частот – периодичность процессов на их выходах. Поэтому количество повторяющихся состояний автомата не будет превышать числа P, где P – количество тактовых интервалов на периоде неравномерности структуры потока выходных импульсов Q (точек на числовой оси). Другими словами, P – это емкость автомата (число его устойчивых состояний).

Заметим, что описание формируемых КА колебаний – его функций выходов ρ_k и переходов S_k, – как во временнóй области, так и с точки зрения их спектрального состава, представляет значительный теоретический и практический интерес, позволяет понимать закономерности работы КА и строить его математические модели, ориентированные на решение задач цифрового – пассивного или активного – синтеза частот [6, 11, 12].

Квазиравномерные последовательности и их описание

Описать работу автомата в интересах синтеза частот можно с помощью КРП импульсов или точек на числовой оси. Покажем, что коэффициент деления N оптимального КА можно реализовать с помощью двух ближайших к N целочисленных значений.

Теорема 1. Для получения на выходе оптимального КА минимальной временнóй ошибки между импульсами синтезируемой последовательности относительно ближайших к ним импульсов ИРП требуемой частоты, не превышающей длительности единичного периода, достаточно двух ближайших к N целочисленных коэффициентов.

Действительно, если предположить, что коэффициент деления автомата $N = P/Q$ реализуется двумя ближайшими целочисленными значениями:

$$N \in (\lfloor N \rfloor, \lceil N \rceil), \tag{1}$$

можно записать:

$$\lfloor N \rfloor \le N < \lceil N \rceil, \tag{2}$$

где $\lceil N \rceil = \lfloor N \rfloor + 1$; $N = \lfloor N \rfloor + \{N\}$; $0 \le \{N\} < 1$.

Однако $\lfloor N \rfloor \le \lfloor N \rfloor + \{N\} < \lfloor N \rfloor + 1$, значит:

$$0 \le \{N\} < 1. \tag{3}$$

Следовательно, формула (1) справедлива, и теорема 1 доказана.

Представить КРП точек на выходе оптимального автомата можно двумя способами. При первом способе описания автомата выходная КРП логических перепадов или точек на числовой оси представляется в виде парциальных целочисленных коэффициентов деления автомата $\lfloor iN \rfloor = \lfloor iP/Q \rfloor$, усреднение которых на периоде неравномерности T_s дает требуемое значение выходного периода $T_{\text{выхНЧ}}$, выраженного в долях тактового периода $T_{\text{опВЧ}}$:

$$N = \frac{T_{\text{выхНЧ}}}{T_{\text{опВЧ}}}, \quad T_s = PT_{\text{опВЧ}} = QT_{\text{выхНЧ}},$$

$$\overline{T_{\text{выхНЧ}}} = \frac{1}{Q}\sum_{i=0}^{Q-1}\left\lfloor i\frac{P}{Q}\right\rfloor T_{\text{опВЧ}}.$$

Рассмотрим этот вопрос подробнее.

КРП первого типа

КРП точек первого типа на выходе математической модели КА может быть получена следующим образом [13, 14]. Расположим на оси безразмерного времени, на которой за единицу принят интервал $T_{\text{опВЧ}}$, равномерную последовательность точек с целочисленными номерами $n \in (-\infty, ..., -1, 0, 1, ..., \infty)$ в моменты времени:

$$\frac{t}{T_{\text{опВЧ}}} = \Psi_n = n\frac{P}{Q}.$$

Назовем ее порождающей последовательностью точек для искомой КРП первого типа. Выделим по обе стороны каждой из точек порождающей последовательности область значений ϑ (назовем ее интервалом захвата), удовлетворяющую одному из условий:

$$\begin{cases} \Psi_n + \varepsilon - 1 \le \vartheta < \Psi_n + \varepsilon, & (4.1) \\ \Psi_n + \varepsilon - 1 < \vartheta \le \Psi_n + \varepsilon, & (4.2) \\ \Psi_n + \varepsilon \le \vartheta < \Psi_n + \varepsilon + 1, & (4.3) \\ \Psi_n + \varepsilon < \vartheta \le \Psi_n + \varepsilon + 1, & (4.4) \end{cases}$$

где $\varepsilon = 0{,}5$; Ψ_n – текущая (мгновенная) фаза ИРП точек; ϑ – текущая (мгновенная) фаза КРП точек.

В выражениях (4.1) и (4.3) интервал захвата замкнут слева, а в выражениях (4.2) и (4.4.) интервал захвата замкнут справа, и во всех случаях в нем все-

гда окажется одно и только одно целочисленное значение $\vartheta = \vartheta_n$. Точка оси, соответствующая этому целочисленному значению, и будет точкой формируемой КРП, имеющей номер n.

Теорема 2. КРП точек первого типа, сформированные в соответствии с (4) и, более того, при любых значениях ε, идентичны по структуре и отличаются друг от друга лишь сдвигом во времени на целое число номеров n.

Для доказательства этого утверждения напишем аналитические выражения для ϑ_n, попадающих в интервал захвата и соответствующие всем четырем строкам формулы (4):

$$\begin{cases} \vartheta_n = \lfloor\lfloor \Psi_n + \varepsilon \rfloor, & (5.1) \\ \vartheta_n = \lceil \Psi_n + \varepsilon \rceil, & (5.2) \\ \vartheta_n = \lfloor \Psi_n + \varepsilon \rfloor, & (5.3) \\ \vartheta_n = \lceil\lceil \Psi_n + \varepsilon \rceil. & (5.4) \end{cases}$$

где $\lfloor\lfloor * \rfloor$ – операция выделения целой части рационального числа X, строго меньшей этого числа; например:

$$\lfloor 3{,}7 \rfloor = 3; \lfloor -3{,}7 \rfloor = -4; \lfloor 3{,}0 \rfloor = 3; \lfloor -3{,}0 \rfloor = -3;$$

однако:

$$\lfloor\lfloor 3{,}0 \rfloor = 2 \text{ и } \lfloor\lfloor -3{,}0 \rfloor = -4;$$

$\lceil * \rceil$ – целая часть рационального числа X, бóльшая или равная ему; $\lceil\lceil * \rceil$ – целая часть числа X, строго превышающая его не более, чем на единицу.

При дробных значениях X имеют место равенства: $\lfloor\lfloor X \rfloor = \lfloor X \rfloor$; $\lceil X \rceil = \lceil\lceil X \rceil$. При целочисленных значениях X соотношения иные: $\lfloor X \rfloor = X$; $\lfloor\lfloor X \rfloor = X - 1$; $\lceil X \rceil = X$; $\lceil\lceil X \rceil = X + 1$. Нетрудно установить, что каждая из четырех рассматриваемых функций (5) может быть выражена через любую из трех других в соответствии с таблицей 1.

ТАБЛИЦА 1. Способы выделения целой части аргумента *X*

TABLE 1. Methods for Extracting the Integer Part of the Argument X

–	$\lfloor X \rfloor$	$\lceil X \rceil$	$\lfloor\lfloor X \rfloor$	$\lceil\lceil X \rceil$
$\lfloor X \rfloor$	–	$-\lceil -X \rceil$	$-\lfloor\lfloor -X \rfloor - 1$	$\lceil\lceil X \rceil - 1$
$\lceil X \rceil$	$\lfloor -X \rfloor$	–	$\lfloor\lfloor X \rfloor + 1$	$-\lceil\lceil -X \rceil + 1$
$\lfloor\lfloor X \rfloor$	$-\lfloor -X \rfloor - 1$	$\lceil X \rceil - 1$	–	$-\lceil\lceil -X \rceil$
$\lceil\lceil X \rceil$	$\lfloor X \rfloor + 1$	$-\lceil -X \rceil - 1$	$-\lfloor\lfloor -X \rfloor$	–

С учетом сказанного примем за исходные формулы:

$$\begin{cases} \vartheta_n = \left\lfloor\left\lfloor n\dfrac{P}{Q} + \varepsilon \right\rfloor\right., & (6.1) \\ \vartheta_n = \left\lceil n\dfrac{P}{Q} + \varepsilon \right\rceil, & (6.2) \\ \vartheta_n = \left\lfloor n\dfrac{P}{Q} + \varepsilon \right\rfloor, & (6.3) \\ \vartheta_n = \left\lceil\left\lceil n\dfrac{P}{Q} + \varepsilon \right\rceil\right.. & (6.4) \end{cases}$$

Поскольку значения ϑ_n в (6) отличаются, в соответствии с таблицей 1, на целое число – единицу, теорема 2 доказана.

Теорема 3. КРП точек первого типа, сформированные в соответствии с (5) и описываемые формулами (6), инвариантны начальному сдвигу (начальной фазе) и могут быть приведены к общему виду:

$$\vartheta_n = \left\lfloor\left\lfloor \frac{nP - R}{Q} \right\rfloor\right., \qquad (7)$$

где $R = \lfloor\lfloor Q\varepsilon \rfloor$ в случаях (4.2 и 4.4) и $R = \lfloor Q\varepsilon \rfloor$ в случаях (4.1 и 4.3).

Предварительно докажем следующие равенства:

$$\left\lfloor \frac{\lfloor xN \rfloor}{N} \right\rfloor = \lfloor x \rfloor, \qquad (8)$$

$$\left\lfloor\left\lfloor \frac{\lfloor\lfloor xN \rfloor}{N} \right\rfloor\right. = \lfloor\lfloor x \rfloor, \qquad (9)$$

$$\left\lfloor\left\lfloor \frac{M+1}{N} \right\rfloor\right. = \left\lfloor \frac{M}{N} \right\rfloor, \qquad (10)$$

где $N \geq 2$ – произвольное натуральное число; M – произвольное целое число.

И в дополнение пара очевидных равенств:

$$\begin{cases} \lfloor\lfloor N \rfloor \pm \lfloor M \rfloor\rfloor = \lfloor N \rfloor \pm \lfloor M \rfloor, \\ \lfloor N \pm \lfloor M \rfloor\rfloor = \lfloor N \rfloor \pm \lfloor M \rfloor. \end{cases} \qquad (11)$$

Известно [7–9], что любое рациональное число можно представить в виде выражения:

$$x = \lfloor x \rfloor + \{x\} = \lceil x \rceil - 1 + \{x\},$$

где $\lfloor x \rfloor$ – целая часть x, меньшая или равная ему; $0 \leq \{x\} < 1$ – дробная часть x; $\lceil x \rceil$ – целая часть x, бóльшая или равная ему; $0 < 1 - \{x\} \leq 1$ – дробная часть x.

Так как $x \times N = \lfloor x \rfloor N + \{x\}N$, то $\lfloor xN \rfloor = \lfloor\lfloor x \rfloor N \rfloor + \lfloor\{x\}N \rfloor$,

$$\frac{\lfloor xN \rfloor}{N} = \frac{x\lfloor xN \rfloor}{xN} = \lfloor x \rfloor + \frac{\lfloor x \rfloor\{xN\}}{xN},$$

причем $\lfloor x \rfloor\{xN\} < xN$.

Следовательно:

$$\left\lfloor \frac{\lfloor x \rfloor xN + \lfloor x \rfloor\{xN\}}{xN} \right\rfloor = \left\lfloor \lfloor x \rfloor + \frac{\lfloor x \rfloor}{xN} - \frac{\lfloor xN \rfloor}{xN} \right\rfloor = \lfloor\lfloor x \rfloor\rfloor = \lfloor x \rfloor,$$

и равенство (8) справедливо.

В соответствии с таблицей 1 возможны различные варианты разбиения рационального числа на целую и дробную части.

Согласно таблице 1 справедливы соотношения:

$$\lfloor\lfloor xN \rfloor + 1 = -\lfloor -xN \rfloor \text{ и } \lfloor\lfloor -\lfloor -xN \rfloor/N \rfloor = -\lfloor\lfloor -xN \rfloor/N \rfloor - 1.$$

Последнее выражение, в соответствии с (8), и таблицей 1 равно $-\lfloor -x \rfloor - 1$ или $\lfloor\lfloor x \rfloor$, поэтому равенство (9) справедливо.

Таким образом, очевидно, что:

$$\frac{M+1}{N} = \frac{M}{N} + \frac{1}{N} = \left\lfloor \frac{M}{N} \right\rfloor + \left\{ \frac{M}{N} \right\} + \frac{1}{N}.$$

При целом M выражение можно записать как:

$$\frac{1}{N} \le \left\{ \frac{M}{N} \right\} \le \frac{N-1}{N}.$$

Следовательно:

$$\frac{2}{N} \le \left\{ \frac{M}{N} \right\} + \frac{1}{N} \le 1.$$

Однако:

$$\frac{1}{N} \le \left\{ \frac{M}{N} \right\} < 1 \text{ или } 0 \le \left\{ \frac{M}{N} \right\} < 1 - \frac{1}{N},$$

т. е. при $N \ge 2$:

$$\left\lfloor \left\lfloor \frac{M+1}{N} \right\rfloor \right\rfloor = \left\lfloor \frac{M}{N} \right\rfloor,$$

и справедлива формула (10).

После сказанного выражение можно записать в следующем виде:

$$\left\lfloor n\frac{P}{Q} + \varepsilon \right\rfloor = \left\lfloor \left\lfloor \frac{\left(n\frac{P}{Q} + \varepsilon\right)Q}{Q} \right\rfloor \right\rfloor = \left\lfloor \frac{nP + \lfloor Q(+\varepsilon) \rfloor}{Q} \right\rfloor =$$

$$= \left\lfloor \left\lfloor \frac{(nP + \lfloor Q\varepsilon \rfloor + 1)}{Q} \right\rfloor \right\rfloor = \left\lfloor \left\lfloor \frac{nP - \lfloor \lfloor Q\varepsilon \rfloor}{Q} \right\rfloor \right\rfloor = \left\lfloor \left\lfloor \left(\frac{nP - R}{Q}\right) \right\rfloor \right\rfloor,$$

где $\lfloor\lfloor Q\varepsilon \rfloor = R$.

Аналогично нетрудно показать, что:

$$\left\lfloor \left\lfloor n\frac{P}{Q} + \varepsilon \right\rfloor \right\rfloor = \left\lfloor \left\lfloor \left(\frac{nP - R}{Q}\right) \right\rfloor \right\rfloor.$$

Осталось доказать следующее. Если даны две пары КРП первого типа с одинаковыми P и Q, но с различными значениями временнóго сдвига ε, т. е. R и различными способами получения по (6), то всегда можно найти такую постоянную разность номеров $n = n_2 - n_1$, при которой разность моментов времени $\vartheta = \vartheta_{n2} - \vartheta_{n1}$ (выраженная в единичных интервалах), которые были найдены для КРП 2 и КРП 1 по формуле (7), будет также постоянной величиной (12).

$$\vartheta = \left\lfloor \left\lfloor \frac{n_2P - R_2}{Q} \right\rfloor \right\rfloor = \left\lfloor \left\lfloor \frac{(n_1+n)P - R_2}{Q} \right\rfloor \right\rfloor = \left\lfloor \left\lfloor \frac{n_1P - (R_2 - nP)}{Q} \right\rfloor \right\rfloor = \varphi_{n1} + \varphi =$$
$$= \left\lfloor \left\lfloor \frac{n_1P - R_1}{Q} \right\rfloor \right\rfloor + \varphi = \left\lfloor \left\lfloor \frac{n_1P - R_1}{Q} + \varphi \right\rfloor \right\rfloor = \left\lfloor \left\lfloor \frac{n_1P - (R_1 - Q\varphi)}{Q} \right\rfloor \right\rfloor. \quad (12)$$

Очевидно, что последнее равенство имеет место, если $R_2 - nP = R_1 - Q\vartheta_n$, т. е. при $R = R_2 - R_1 = nP - Q\vartheta_n$. Последнее выражение представляет собой диофантово уравнение (уравнение в целых числах) первой степени, которое при взаимно простых P и Q всегда разрешимо в целых n и ϑ_n [9].

Решения этого диофантова уравнения записываются в виде:

$$\begin{cases} \vartheta = |S+1| + R_Z, \\ S = (-1)^{r-1}(\pm x)R_{r-1}, \\ n = |V+1| - Q_Z, \\ V = (-1)^{r-1}(\pm x)Q_{r-1}, \end{cases}$$

где $z = 0, \pm1, \pm2, \ldots$; $R = |L \pm x|$; $x = 0, 1, 2, \ldots L - 1$; r – число членов разложения числа $N = P/Q$ в цепную дробь по алгоритму Евклида.

Таким образом, КРП точек первого типа инвариантна начальному сдвигу – теорема 3 доказана.

Каноническая форма записи КРП точек первого типа

Доказанная независимость структуры КРП точек первого типа от значений ε делает выражение (7) предельно общей и, вместе с тем, наиболее простой формой задания КРП точек первого типа и поэтому может быть названа *канонической*. Два целых взаимно простых числа P и Q, т. е. $(P,Q) = 1$, полностью определяют структуру КРП точек первого типа, а целое число R определяет смещение этой последовательности на оси времени. Согласно (7), момент времени ϑ_n является целочисленной (дискретной) функцией своего номера n. Представляет интерес выяснение и другой зависимости – определение номера n точки ϑ_n, ближайшей слева от заданного момента времени (предшествующей ему). Иными словами, представляет интерес смена аргумента и функции в (7).

Теорема 4. Номер точки n, соответствующий значению дискретной функции ϑ_n из (7), определяется формулой:

$$n = \left\lfloor \frac{\vartheta_n Q + R}{P} \right\rfloor. \qquad (13)$$

Для доказательства данного утверждения рассмотрим график, приведенный на рисунке 3, линейной непрерывной функции ϑ непрерывного аргумента, который, очевидно, является графиком обратной функции n от непрерывного аргумента ϑ:

$$n = \frac{\vartheta Q + R}{P}.$$

Чтобы найти целочисленные значения ϑ_{n1}, соответствующие, согласно (7), некоторому целочисленному значению n_1, необходимо из точки n_1 на оси ординат восстановить перпендикуляр к этой оси до пересечения с наклонной прямой (точки a, b, c на рисунке 3). Целочисленное значение ϑ, ближайшее к ординате точки a снизу, будет, согласно (7) точкой ϑ_{n1}.

Поскольку в (7)

$$\frac{d\vartheta}{dn} = \frac{P}{Q} > 1,$$

то исключено, чтобы двум соседним целочисленным значениям n соответствовало одно и то же целочисленное значение ϑ_n.

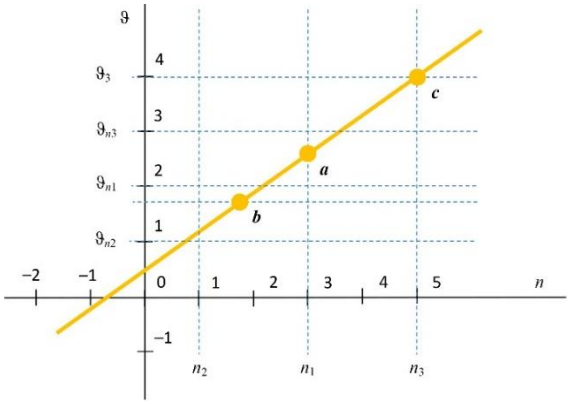


Рис. 3. График функции ϑ

Fig. 3. Graph of the Function ϑ

Ввиду вышеизложенного выберем произвольное значение ϑ и проведем из соответствующей точки оси ординат горизонтальную прямую до пересечения с наклонной прямой (точка b на рисунке 3). Очевидно, что значение n_2, ближайшее слева от абсциссы точки b, определяет момент времени ϑ_{n2}, ближайший слева от выбранного времени ϑ, все значения которого соответствуют, согласно (13), целочисленным n.

Особого рассмотрения требует случай, когда ϑ имеет целочисленное значение ϑ_3, а точка пересечения c имеет целочисленную же абсциссу n_3. Дело в том, что, согласно (7), точке n соответствует не ϑ_3, а ϑ_{n3}. Следовательно, n_3 действительно является номером точки, предшествующей ϑ_3. Таким образом, теорема 4 доказана.

Логическая КРП первого типа

На основе информации, полученной в предыдущем разделе, целесообразно отказаться от оси непрерывного времени и вместо целочисленных значений $t = \vartheta_n$ рассматривать номера границ между единичными интервалами тактовой частоты. Будем обозначать эти номера k, появление точки, принадлежащей КРП первого типа, – единицей, а ее отсутствие – нулем. В результате КРП точек первого типа преобразуется в логическую КРП.

Очевидно, что логическая КРП первого типа представляет собой двухзначную функцию $X_k = X(k)$ целочисленного аргумента k. Чтобы написать аналитическое выражение этой функции, обратим внимание на следующее обстоятельство.

Если на оси времени двум следующим друг за другом целочисленным значениям ϑ_k и ϑ_{k+1} соответствует, согласно (5), один и тот же номер n, то ϑ_k не является одной из точек КРП первого типа. Напротив, если моменту времени ϑ_k соответствует номер n, а моменту времени ϑ_{k+1} – номер $n + 1$, то ϑ_k является n-й точкой рассматриваемой последовательности. Поэтому для логической КРП первого типа должна быть справедлива формула:

$$X_k = \left\lfloor \frac{(k+1)Q + R}{P} \right\rfloor - \left\lfloor \frac{kQ + R}{P} \right\rfloor. \qquad (14)$$

Выражение (14) является конечной разностью первого порядка функции (13), в которой ϑ_n заменена своим номером k, т. е. выражение (14) является дискретным аналогом первой производной функции непрерывного аргумента. Оно позволяет предсказать мгновенную частоту X_k на выходе прямочастотного автомата, выраженную через мгновенный период, в любой наперед заданный момент времени. Эта формула полезна для описания работы прямочастотного КА, но неудобна тем, что в нее, кроме одного аргумента k, входит и второй аргумент $k + 1$. Чтобы разрешить эту коллизию, введем в рассмотрение функцию:

$$Y_k = kQ + R - P\left\lfloor \frac{kQ + R}{P} \right\rfloor,$$

которую удобнее записать в следующем виде:

$$\frac{Y_k}{P} = \frac{kQ + R}{P} - \left\lfloor \frac{kQ + R}{P} \right\rfloor. \qquad (15)$$

Назовем эту функцию фазой X_k на периоде неравномерности P.

Из (15) следует:

$$kQ + R = Y_k + P\left\lfloor \frac{kQ + R}{P} \right\rfloor.$$

Теорема 5. Фаза Y_k логической КРП первого типа может принимать любое из целочисленных значений от 0 до $P - 1$ и на главном периоде частоты следования однозначно определяется выражением:

$$Y_k = P\left\{\frac{kQ + R}{P}\right\}. \quad (16)$$

Для доказательства этого утверждения напишем очевидное равенство:

$$(k + 1)Q + R = kQ + R + Q. \quad (17)$$

Из (16) и (17) следует, что:

$$(k + 1)Q + R = Y_k + P\left\lfloor\frac{kQ + R}{P}\right\rfloor + Q. \quad (18)$$

Поделим обе части (18) на P и возьмем из полученного выражения функцию $\lfloor * \rfloor$, т. е. выделим целую часть:

$$\left\lfloor\frac{(k + 1)Q + R}{P}\right\rfloor = \left\lfloor\frac{Y_k + Q}{P} + \left\lfloor\frac{kQ + R}{P}\right\rfloor\right\rfloor. \quad (19)$$

Но $\lfloor(kQ+R)/P\rfloor$ в (19) – целое число, поэтому его можно вынести за знак $\lfloor * \rfloor$, что приводит к выражению:

$$\left\lfloor\frac{(k + 1)Q + R}{P}\right\rfloor = \left\lfloor\frac{kQ + R}{P}\right\rfloor + \left\lfloor\frac{Y_k + Q}{P}\right\rfloor. \quad (20)$$

Сопоставив формулы (20) и (13), можно сделать вывод, что:

$$X_k = \left\lfloor\frac{Y_k + Q}{P}\right\rfloor. \quad (21)$$

Перепишем теперь (14) в виде:

$$Y_k = P\left(\frac{kQ + R}{P} - \left\lfloor\frac{kQ + R}{P}\right\rfloor\right). \quad (22)$$

По определению функции $x = \lfloor x \rfloor + \{x\}$, если $(kQ + R)/P$ – не целое число, то Y_k в (22) определяется выражением (16), если же $(kQ + R)/P$ – целое число, то $Y_k = 0$.

Рассмотрим подробнее выражение (16). Поскольку $kQ + R$ – число целое, то можно утверждать, что дробь $\{(kQ + R)/P\}$ может иметь лишь одно из P значений i/P, где $i \in (0, 1, 2, \ldots, P - 1)$. Соответственно, функция Y_k может принимать любое из целочисленных значений от 0 до $P - 1$. Теорема 5 доказана.

Таким образом, выражение (16) однозначно определяет функцию мгновенной (текущей) фазы $Y(k)$ на периоде P, выражение (14) однозначно определяет функцию мгновенной (текущей) частоты $X(k)$, выражение (7) позволяет определить состояние функции ϑ_n в любой наперед заданный момент времени, а выражение (13) позволяет найти номер точки n, соответствующий заданному состоянию функции ϑ_n.

Теорема 6. Временна́я ошибка КРП точек на выходе оптимального КА относительно ИРП точек той же частоты инвариантна начальному сдвигу, по модулю не превышает половины периода тактового интервала и является минимально возможной величиной для класса цифровых структур.

Перепишем формулу (7):

$$\vartheta_n = \left\lfloor\left\lfloor\frac{nP - R}{Q}\right\rfloor - \left\lfloor\left\lfloor\frac{(nP - \lfloor Q(-\varepsilon)\rfloor)}{Q}\right\rfloor\right\rfloor,$$

$$\vartheta_n = \left\lfloor\left\lfloor\frac{nP + \lfloor Q\varepsilon\rfloor}{Q}\right\rfloor\right\rfloor = \left\lfloor\left\lfloor\frac{nP}{Q}\right\rfloor + \left\lfloor\left\lfloor\frac{\lfloor Q\varepsilon\rfloor}{Q}\right\rfloor\right\rfloor = \left\lfloor\left\lfloor\frac{nP}{Q}\right\rfloor + \lfloor\varepsilon\rfloor\right\rfloor,$$

$$\vartheta_n = \left\lfloor\frac{nP}{Q}\right\rfloor + \varepsilon - 1,$$

$$\vartheta = \frac{nP}{Q} + \varepsilon - 1.$$

Тогда временна́я разность ИРП и КРП точек может быть представлена в виде выражения:

$$\vartheta - \vartheta_n \equiv \Delta = \frac{nP}{Q} + \varepsilon - 1 - \left\lfloor\frac{nP}{Q}\right\rfloor - \varepsilon + 1 = \\ = \left\{\frac{nP}{Q}\right\} < 1. \quad (23)$$

При этом:

$$0 \le \left\{\frac{nP}{Q}\right\} < 1, \quad (24)$$

и модуль разности ИРП и КРП:

$$\left|\left\{\frac{nP}{Q}\right\}\right| < \frac{1}{2}.$$

Таким образом, теорема 6 доказана.

В таблицах 2 и 3 приведены примеры формирования КРП с параметрами $P = 8$, $Q = 3$, $\varepsilon = 0$, в соответствии с формулами (16) и (14) – таблица 2, и в соответствии с формулами (7) и (24) – таблица 3. Желтым цветом выделен главный период повторения функций переходов Y_k и Δ; красным цветом выделены импульсы функции выхода X_k.

ТАБЛИЦА 2. КРП в соответствии с формулами (16) и (14)

TABLE 2. QUS in Accordance with Formulas (16) and (14)

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13
Y_k	0	3	6	1	4	7	2	5	8 = 0	3	6	1	4	7
X_k	1	0	0	1	0	0	1	0	1	0	0	1	0	0

ТАБЛИЦА 3. КРП в соответствии с формулами (7) и (24)

TABLE 3. QUS in Accordance with Formulas (7) and (24)

n	0	1	2	3	4	5	6	7	8	9
ϑ_n	0	2	5	8	10	13	16	18	21	24
Δ	0	2	1	0	2	1	0	2	1	0

Фазовая окружность первого типа

Построим окружность произвольного радиуса (рисунок 4) и расположим на ней равномерно P точек. Пронумеруем их последовательно против часовой стрелки от 0 до P – 1. Полученный график целесообразно назвать фазовой окружностью логической КРП, т. к. с его помощью нетрудно вычислить значения мгновенной фазы (а по ней и значения X) для точки логической КРП с любым номером m, если известна фаза точки с номером n.

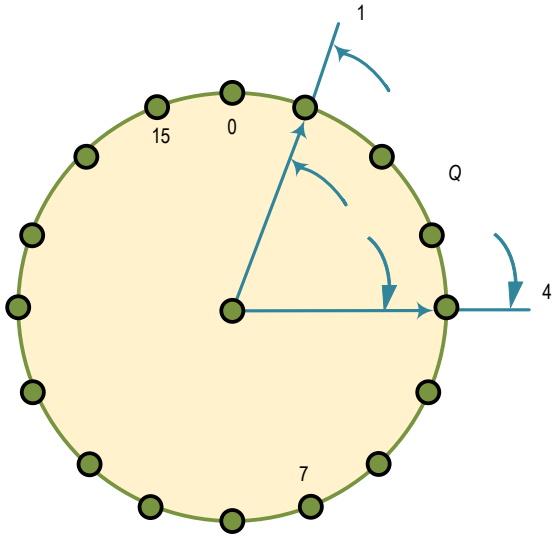


Рис. 4. Фазовая окружность для P = 16, Q = 3, R = 1

Fig. 4. Phase Circle for P = 16, Q = 3, R = 1

Действительно, пусть, например, Y_k = 4 (см. рисунок 4). Согласно (19), для получения Y_{k+1} следует пройти по окружности по часовой стрелке Q интервалов, поскольку при переходе от Y_k к Y_{k+1} первый член правой части (19) должен вырасти на Q единиц. Далее возможны три случая.

В первом случае мы не дойдем до точки с номером P – 1, во втором случае попадем в эту точку, а в третьем – перейдем через точку с номером P – 1.

В первых двух случаях третий член правой части (15) сохраняет свое значение неизменным. Следовательно, номер точки, в которую мы пришли, есть искомое значение Y_{k+1}. В третьем случае третий член правой части (15) вырастет на P единиц, и мы будем должны вычесть число P из полученной суммы. Поэтому в номерах, превышающих P – 1, нет надобности и для нахождения любого значения Y_{k+1} достаточно фазовой окружности, поделенной на P интервалов и формулы (16).

Выводы

Получена аналитическая запись КРП точек на выходе математической модели КА, что позволяет осознанно подходить к проектированию автоматов, используемых в пассивных цифровых синтезаторах частоты.

Показано, что КРП точек на выходе КА инвариантны моменту времени начала отсчета, идентичны по структуре и отличаются лишь сдвигом во времени на целое число тактов КА.

Предложены 4 функции выделения целой части рационального числа N и показано, что каждая из них может быть выражена через любую из трех других. Использование таких функций позволяет эффективно анализировать работу автоматов разной структуры.

С помощью логических КРП первого типа можно анализировать поведение прямочастотных КА (например, построенных на основе накапливающих сумматоров), используемых для синтеза частот и получать аналитические выражения для функций переходов (функций текущей фазы) и функций выходов (функций текущей частоты), подобных КА [6]. Компактная запись таких функций помогает в дальнейшем перейти к спектральному анализу КРП импульсов и получить выражения для спектра на выходе автомата в свернутом виде, т. е. без обращения к рядам.

Список источников

1. Апериодические автоматы / под ред. В. И. Варшавского. М.: Наука, 1976. 424 с.
2. Карцев М.А., Брик В.А. Вычислительные системы и синхронная арифметика. М.: Радио и связь, 1981. 360 с.
3. Филиппов А.Г., Белкин О.С. Проектирование логических узлов ЭВМ. М.: Советское Радио, 1974. 344 с.
4. Захаров Н.Г., Рогов Н.Г. Синтез цифровых автоматов. Ульяновск: УлГТУ, 2003. 135 с.
5. Поспелов Д.А. Арифметические основы вычислительных машин дискретного действия. М.: Высшая школа, 1970. 308 с.
6. Никитин Ю.А. Теория цифроаналогового синтеза частот с помощью конечных автоматов. СПб.: СПбГУТ, 2024. 342 с.
7. Виноградов И.М. Основы теории чисел. М. – Л.: ГИТТЛ, 1940. 112 с.
8. Хинчин А.Я. Цепные дроби. М.: Наука, 1978. 112 с.
9. Гельфонд А.О. Решение уравнений в целых числах. М.: Наука, 1978. 63 с.
10. Фомин С.В. Системы счисления. М.: Наука. ГИФМЛ, 1975. 48 с.
11. Иванов В.А. Прямой синтез частот на основе цифровых структур // Радиотехника и электроника. 1983. № 9. С. 1765–1771.
12. Vankka J. Direct Digital Synthesizers: Theory, Design and Applications. D.Sc Thesis. Helsinki: Helsinki University of Technology, 2000. 193 p.

13. Никитин Ю.А. Анализ конечного автомата для синтеза частот с помощью функций целочисленного аргумента // Известия высших учебных заведений. Приборостроение. 2010. Т. 53. № 5. С. 25–29. EDN:LSOURJ
14. Никитин Ю.А. Математическая модель формирования колебаний с использованием методов пассивного цифрового синтеза // Известия высших учебных заведений. Приборостроение. 2011. Т. 54. № 9. С. 52–57. EDN:OCFXEB

References

1. Varshavsky V.I. (ed.) *Aperiodic Automata*. Moscow. Nauka Publ.; 1976. 424 p. (in Russ.)
2. Kartsev M.A., Brik V.A. *Computing Systems and Synchronous Arithmetic.* Moscow: Radio i svyaz Publ.; 1981. 360 p. (in Russ.)
3. Filippov A.G., Belkin O.S. *Design of Logical Units of Computers*. Moscow: Sovetskoe Radio Publ.; 1974. 344 p. (in Russ.)
4. Zakharov N.G., Rogov V.N. *Synthesis of Digital Automata*. Ulyanovsk: UlSTU Publ.; 2003. 135 p. (in Russ.)
5. Pospelov D.A. *Arithmetic Foundations of Discrete-Action Computers*. Moscow: Vysshaya shkola Publ.; 1970. 308 p. (in Russ.)
6. Nikitin Yu.A. *Theory of Digital-to-Analog Frequency Synthesis Using Finite Automata*. St. Petersburg: SPbSUT Publ.; 2024. 342 p. (in Russ.)
7. Vinogradov I.M. *Fundamentals of Number Theory*. Moscow – Leningrad: GITTL Publ.; 1940. 112 p. (in Russ.)
8. Khinchin A.Ya. *Continued Fractions*. Moscow: Nauka Publ.; 1978. 112 p. (in Russ.)
9. Gelfond A.O. *Solution of Equations in Integers*. Moscow: Nauka Publ.; 1978. 63 p. (in Russ.)
10. Fomin S.V. *Number Systems*. Moscow: Nauka. GIFML Publ.; 1975. 48 p. (in Russ.)
11. Ivanov V.A. Direct frequency synthesis based on digital structures. *Radio engineering and electronics*. 1983;9:1765–1771. (in Russ.)
12. Vankka J. *Direct Digital Synthesizers: Theory, Design and Applications*. D.Sc Thesis. Helsinki: Helsinki University of Technology Publ.; 2000. 193 p.
13. Nikitin Yu.A. Analysis of Finite Automaton for Frequency Synthesis with the Use of Functions of Integer-Valued Argument. *Journal of Instrument Engineering*. 2010;53(5):25–29. (in Russ.) EDN:LSOURJ
14. Nikitin Yu.A. Mathematical Model of Oscillation Formation with the Use of Passive Digital Synthesis. *Journal of Instrument Engineering*. 2011;54(9):52–57. (in Russ.) EDN:OCFXEB

Статья поступила в редакцию 11.09.2024; одобрена после рецензирования 17.12.2024; принята к публикации 07.02.2025.
The article was submitted 11.09.2024; approved after reviewing 17.12.2024; accepted for publication 07.02.2025.

Информация об авторе:

НИКИТИН Юрий Александрович
кандидат технических наук, старший научный сотрудник, доцент кафедры электроники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
https://orcid.org/0000-0002-0749-9751

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-2025-11-1-44-52
EDN:ADOHFC

Метод координатометрии земной станции, основанный на использовании двух космических аппаратов

Владимир Витальевич Севидов, v-v-sevidov@mail.ru

Военная академия связи им. С.М. Буденного,
Санкт-Петербург, 194064, Российская Федерация

Аннотация

Актуальность. *Существующие методы координатометрии, такие как угломерные, угломерно-дальномерные, разностно-дальномерные, суммарно-дальномерные, достаточно хорошо изучены и оптимизированы. Однако применение указанных методов не всегда возможно или целесообразно, что стимулирует разработку и изучение новых методов и их комплексирование с существующими. В статье представлен разработанный метод координатометрии земной станции, основанный на использовании двух космических аппаратов. Показан вывод аналитических соотношений для расчета координат земных станций на основе значений взаимных временны́х задержек и частотных сдвигов. Указанные временны́е задержки и частотные сдвиги обусловлены разными расстояниями и доплеровскими сдвигами частот одних и тех же реализаций радиосигналов на различных радиотрассах.*

Представлены основные выражения для временны́х задержек и частотных сдвигов радиосигналов земных станций, ретранслированных космическими аппаратами. Составлена система из трех независимых уравнений. При этом в качестве первого уравнения выступает разностно-дальномерное уравнение, в качестве второго – разностно-радиально-скоростное уравнение, в качестве третьего – уравнение референц-эллипсоида Земли. ***Результатом*** *решения системы уравнений являются координаты земной станции.*

В ходе исследования ***использовались методы*** *моделирования и математического анализа. При решении уравнения второго порядка применялся итерационный метод Ньютона – Рафсона с разложением функций в ряды Тейлора с точностью до первых производных.*

В качестве иллюстрации разработанного метода приведен частный пример расчета. Предлагаемый метод координатометрии инвариантен к типу орбит космических аппаратов, задействованных для определения координат земных станций. В качестве примера представлены два космических аппарата: первый – на геостационарной орбите, второй – на низкой орбите.

Научной новизной *разработанного технического решения является однозначное одномоментное определение координат земных станций, находящихся на поверхности референц-эллипсоида Земли, основанного на использовании всего двух космических аппаратов. При этом нет необходимости синхронизации с излучением радиосигналов земных станций, что является необходимым условием большинства существующих методов координатометрии.*

Практическая значимость *предложенного комбинированного (разностно-дальномерного и разностно-доплеровского) метода координатометрии земных станций заключается в возможности его применения в существующих и перспективных комплексах радиомониторинга для оценки координат земных станций, нелегитимно использующих частотно-временно́й ресурс космического аппарата, а также являющихся источниками преднамеренных или непреднамеренных радиопомех.*

Ключевые слова: *модель, координатометрия, земная станция, комплекс радиомониторинга, космический аппарат, эффект Доплера*

Ссылка для цитирования: Севидов В.В. Метод координатометрии земной станции, основанный на использовании двух космических аппаратов // Труды учебных заведений связи. 2025. Т. 11. № 1. С. 44–52. DOI:10.31854/1813-324X-2025-11-1-44-52. EDN:ADOHFC

Original research
https://doi.org/10.31854/1813-324X-2025-11-1-44-52
EDN:ADOHFC

Coordinate Measurement Method of the Earth Station Based on the Two Spacecraft Use

Vladimir V. Sevidov, v-v-sevidov@mail.ru

Military Academy of Communications,
St. Petersburg, 194064, Russian Federation

Annotation

Relevance. *The existing methods of coordinate measurement, such as goniometric, goniometric-range-measuring, difference-range-measuring, total-range-measuring are well studied and optimized. However, the application of these methods is not always possible or advisable, which stimulates the development and study of new methods and their integration with the existing ones. The article presents the developed method of coordinate measurement of the earth station, based on the use of two spacecraft. The derivation of analytical relationships for calculating the coordinates of earth stations based on the values of mutual time delays and frequency shifts is shown. The specified time delays and frequency shifts are due to different distances and Doppler frequency shifts of the same implementations of radio signals on different radio paths.*

The main expressions for time delays and frequency shifts of radio signals of earth stations retransmitted by spacecraft are presented. A system of three independent equations is composed. The first equation is the difference-range equation, the second is the difference-radial-velocity equation, and the third is the equation of the Earth's reference ellipsoid. ***The result*** *of solving the system of equations is the coordinates of the earth station.*

The study ***used the methods*** *of modeling and mathematical analysis. When solving the second-order equation, the iterative Newton-Raphson method was used with the expansion of functions in Taylor series with an accuracy of up to the first derivatives.*

A particular example of calculation is given as an illustration of the developed method. The developed method of coordinate measurement is invariant to the type of orbits of spacecraft used to determine the coordinates of earth stations. Two spacecraft are given as an example: the first is in geostationary orbit, the second is in low orbit.

The scientific novelty *of the developed technical solution is the unambiguous one-time determination of the coordinates of earth stations located on the surface of the Earth's reference ellipsoid, based on the use of only two spacecraft. In this case, there is no need for synchronization with the radiation of radio signals of earth stations, which is a necessary condition for most existing methods of coordinate measurement.*

The practical significance *of the proposed combined (difference-range and difference-Doppler) method of coordinate measurement of earth stations lies in the possibility of its application in existing and prospective radio monitoring complexes for assessing the coordinates of earth stations that illegally use the frequency-time resource of a spacecraft, as well as being sources of intentional or unintentional radio interference.*

Keywords: *model, coordinate measurement, earth station, radio monitoring complex, spacecraft, Doppler effect*

For citation: Sevidov V.V. Coordinate Measurement Method of the Earth Station Based on the Two Spacecraft Use. *Proceedings of Telecommunication Universities.* 2025;11(1):44–52. (in Russ.) DOI:10.31854/1813-324X-2025-11-1-44-52. EDN:ADOHFC

Введение

Мировое развитие характеризуется лавинообразным увеличением радиоэлектронных средств и систем различного назначения, а ограниченность частотно-временно́го и пространственного радиоресурса заставляет многократно дублировать его. При штатной работе правильно спроектированной земной станции (ЗС) системы спутниковой связи (ССС), с учетом выполнения ограничений на частоту, мощность и коэффициент усиления антенны, излучаемые ей радиосигналы в направлении своего космического аппарата (КА) не оказывают деструктивного воздействия на работу других связных КА. Однако из-за внезапно возникающих неисправностей аппаратуры ЗС радиосигналы на некоторых частотах выступают в качестве не-

преднамеренных радиопомех, причем эксплуатирующий ЗС персонал может даже не знать о таких неисправностях, если отсутствуют системы контроля. Такое положение дел зачастую приводит к коллизиям, необходимость разрешения которых, в свою очередь, стимулирует развитие систем радиомониторинга.

Важнейшей задачей радиомониторинга является оценка координат источников радиоизлучения позиционными методами координатометрии (КМ), в которых синхронно измеряют один или несколько координатно-информативных параметров (временны́е задержки, частотные сдвиги и т. д.) радиосигнала разнесенными в пространстве измерителями в один или несколько моментов времени. Классические методы КМ, такие как угломерные [1, 2], угломерно-дальномерные [3], разностно-дальномерные [4…6], суммарно-дальномерные достаточно хорошо изучены и оптимизированы. Однако применение указанных методов не всегда возможно или целесообразно, что это стимулирует разработку и изучение новых методов КМ [7…10] и их комплексирование с существующими, что обуславливает актуальность настоящего исследования.

В настоящей статье представлен комбинированный (разностно-дальномерный и разностно-доплеровский) метод КМ ЗС, основанный на одномоментном приеме ретранслированного радиосигнала указанной ЗС комплексом радиомониторинга (КРМ) через два КА.

Разработка комбинированного (разностно-дальномерного и разностно-доплеровского) метода координатометрии земной станции

Геометрическая основа определения координат ЗС с использованием двух КА, включающая ЗС *I*, 1-й *S* и 2-й *D* КА и КРМ *K*, представлена на рисунке 1, где введены следующие обозначения:

R_{SI} – дистанция между *S* и *I*;

R_{SK} – дистанция между *S* и *K*;

R_{DI} – дистанция между 2-м КА и ЗС;

R_{DK} – дистанция между *D* и *K*;

$\bar{V}_S$ – вектор скорости *S* в трехмерном пространстве;

$\bar{V}_D$ – вектор скорости *D* в трехмерном пространстве;

Θ_{SI} – угол между вектором $\bar{V}_S$ и лучем *SI*;

Θ_{SK} – угол между вектором $\bar{V}_S$ и лучем *SK*;

Θ_{DI} – угол между вектором $\bar{V}_D$ и лучем *DI*;

Θ_{DK} – угол между вектором $\bar{V}_D$ и лучем *DK*;

$\dot{R}_{SI}$ – радиальная скорость *S* относительно *I*;

$\dot{R}_{SK}$ – радиальная скорость *S* относительно *K*;

$\dot{R}_{DI}$ – радиальная скорость *D* относительно *I*;

$\dot{R}_{DK}$ – радиальная скорость *D* относительно *K*.

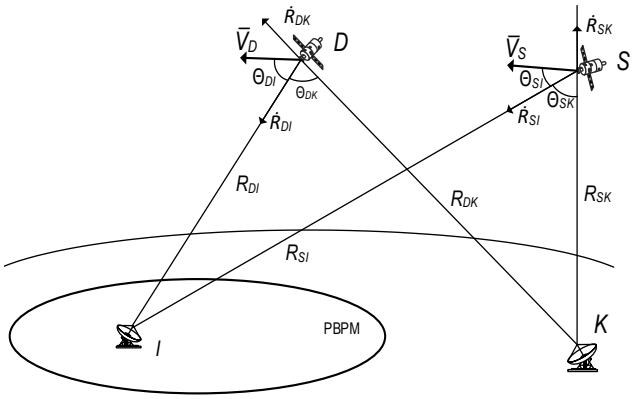


Рис. 1. Геометрическая основа метода КМ ЗС с использованием двух КА

Fig. 1. Geometrical Basis of the Coordinate Measurement Method of the Earth Station Using Two Spacecraft

На рисунке 1 схематически отображен район ведения радиомониторинга (РВРМ), который задается предварительно.

Используя неизвестные координаты *I* x_I, y_I, z_I, составляют уравнение:

$$\sqrt{(x_S-x_I)^2+(y_S-y_I)^2+(z_S-z_I)^2}-\\-\sqrt{(x_D-x_I)^2+(y_D-y_I)^2+(z_D-z_I)^2}=R_{SD}, \quad (1)$$

где $R_{SD}=ct'_{ЗД}$ – разность дистанций от *S* и *D* до *I*; $t'_{ЗД}=t_{ЗД}-\frac{R_{SK}-R_{DK}}{c}-t_S+t_D$ – рассчитанная задержка по времени, обусловленная разницей трасс *IS* и *ID*; $t_{ЗД}$ – задержка по времени, измеряемая в *K* и обусловленная разницей сумм трасс *IS*, *SK* и *ID*, *DK*, соответственно; $c\approx 300000$ км/с – скорость распространения радиосигналов в свободном пространстве; t_S, t_D – временны́е задержки в КА *S* и *D* соответственно.

Задержки t_S и t_D определяют с помощью тестовых сигналов, излученных *K* и принятых от *S* и *D*.

Известные координаты *S*, *D* и *K* позволяют рассчитать расстояния R_{SK} и R_{DK} в момент измерения временно́й задержки $t_{ЗД}$, используя выражения:

$$R_{SK}=\sqrt{(x_S-x_K)^2+(y_S-y_K)^2+(z_S-z_K)^2},$$
$$R_{DK}=\sqrt{(x_D-x_K)^2+(y_D-y_K)^2+(z_D-z_K)^2},$$

где x_K, y_K, z_K – координаты *K*; x_S, y_S, z_S – координаты *S*; x_D, y_D, z_D – координаты *D*.

Измеряемая в *K* разница частот $f_{СД}$ представляется через номиналы средних частот (НСЧ) f_{ISK} и f_{IDK} реализаций радиосигнала, излученного *I*, пройденного трассы *IS*, *SK* и *ID*, *DK*, соответственно, и принятых КРМ:

$$f_{СД}=f_{ISK}-f_{IDK}. \quad (2)$$

В свою очередь f_{ISK} и f_{IDK} могут быть представлены выражениями:

$$f_{ISK} = f_I + f_{ДSI} + f_S + f_{ДSK}, \quad (3)$$

$$f_{IDK} = f_I + f_{ДDI} + f_D + f_{ДDK}, \quad (4)$$

где f_I – НСЧ радиосигнала излучаемого I; $f_{ДSI}$ – доплеровский сдвиг частоты, обусловленный удалением (сближением) S от (c) I; $f_{ДSK}$ – доплеровский сдвиг частоты, обусловленный удалением (сближением) S от (c) K; $f_{ДDI}$ – доплеровский сдвиг частоты, обусловленный удалением (сближением) D от (c) I; $f_{ДDK}$ – доплеровский сдвиг частоты, обусловленный удалением (сближением) D от (c) K; f_S и f_D – номиналы частот переноса спектра S и D, соответственно.

Номиналы частот f_S и f_D являются известными справочными данными.

Доплеровские сдвиги частот $f_{ДSI}$, $f_{ДSK}$, $f_{ДDI}$ и $f_{ДDK}$ вычисляют по формулам:

$$f_{ДSI} = f_I \frac{\dot{R}_{SI}}{c},\ f_{ДSK} = (f_I + f_{ДSI} + f_S)\frac{\dot{R}_{SK}}{c}, \quad (5)$$

$$f_{ДDI} = f_I \frac{\dot{R}_{DI}}{c},\ f_{ДDK} = (f_I + f_{ДDI} + f_D)\frac{\dot{R}_{DK}}{c}. \quad (6)$$

Используя в качестве допущений неравенства $f_I >> f_{ДSI}$ и $f_I >> f_{ДSK}$, упрощают выражения (5) и (6) и с учетом (3) и (4) представляют их следующим образом:

$$f_{ДSI} = (f_{ISK} - f_S)\frac{\dot{R}_{SI}}{c},\ f_{ДSK} = f_{ISK}\frac{\dot{R}_{SK}}{c}, \quad (7)$$

$$f_{ДDI} = (f_{ISK} - f_S)\frac{\dot{R}_{DI}}{c},\ f_{ДDK} = f_{IDK}\frac{\dot{R}_{DK}}{c}. \quad (8)$$

Радиальная скорость S относительно I равна:

$$\dot{R}_{SI} = |\bar{V}_S|\cos\Theta_{SI}. \quad (9)$$

Используя теорему о скалярном произведении векторов, получают:

$$\cos\Theta_{SI} = \frac{(x_I - x_S)\dot{x}_S + (y_I - y_S)\dot{y}_S + (z_I - z_S)\dot{z}_S}{\sqrt{(x_I - x_S)^2 + (y_I - y_S)^2 + (z_I - z_S)^2}|\bar{V}_I|}, \quad (10)$$

где $\dot{x}_S, \dot{y}_S, \dot{z}_S$ – ортогональные составляющие вектора скорости 1-го КА $\bar{V}_S$.

Подставляя (10) в (9), получают:

$$\dot{R}_{SI} = \frac{(x_I - x_S)\dot{x}_S + (y_I - y_S)\dot{y}_S + (z_I - z_S)\dot{z}_S}{\sqrt{(x_I - x_S)^2 + (y_I - y_S)^2 + (z_I - z_S)^2}}. \quad (11)$$

Для радиальных скоростей $\dot{R}_{SK}$, $\dot{R}_{DI}$ и $\dot{R}_{DK}$ справедливы аналитические выражения:

$$\dot{R}_{SK} = \frac{(x_K - x_S)\dot{x}_S + (y_K - y_S)\dot{y}_S + (z_K - z_S)\dot{z}_S}{\sqrt{(x_K - x_S)^2 + (y_K - y_S)^2 + (z_K - z_S)^2}}, \quad (12)$$

$$\dot{R}_{DI} = \frac{(x_I - x_D)\dot{x}_D + (y_I - y_D)\dot{y}_D + (z_I - z_D)\dot{z}_D}{\sqrt{(x_I - x_D)^2 + (y_I - y_D)^2 + (z_I - z_D)^2}}, \quad (13)$$

$$\dot{R}_{DK} = \frac{(x_K - x_D)\dot{x}_D + (y_K - y_D)\dot{y}_D + (z_K - z_D)\dot{z}_D}{\sqrt{(x_K - x_D)^2 + (y_K - y_D)^2 + (z_K - z_D)^2}}, \quad (14)$$

где $\dot{x}_D, \dot{y}_D, \dot{z}_D$ – ортогональные составляющие вектора скорости 2-го КА $\bar{V}_D$.

Представленные аналитические соотношения позволяют составить систему трех квадратных уравнений, содержащую три переменные – искомые координаты ЗС x_I, y_I, z_I:

$$\begin{cases} \sqrt{(x_S - x_I)^2 + (y_S - y_I)^2 + (z_S - z_I)^2} - \\ \sqrt{(x_D - x_I)^2 + (y_D - y_I)^2 + (z_D - z_I)^2} = R_{SD}; \\ \dfrac{(x_I - x_S)\dot{x}_S + (y_I - y_S)\dot{y}_S + (z_I - z_S)\dot{z}_S}{\sqrt{(x_I - x_S)^2 + (y_I - y_S)^2 + (z_I - z_S)^2}} - \\ -\dfrac{(x_I - x_D)\dot{x}_D + (y_I - y_D)\dot{y}_D + (z_I - z_D)\dot{z}_D}{\sqrt{(x_I - x_D)^2 + (y_I - y_D)^2 + (z_I - z_D)^2}} = V, \\ \sqrt{b^2x_I^2 + b^2y_I^2 + a^2z_I^2} = R_3\ , \end{cases} \quad (15)$$

где a и b – большая и малая полуоси референц-эллипсоида Земли;

$$R_3 = ab;\ V = \frac{(f_{СД} - f_S - f_{ДSK} + f_D + f_{ДDK})c}{(f_{ISK} - f_S - f_{ДSK})}.$$

Первое квадратное уравнение системы (15) – это тождество (1), второе – получают путем последовательных математических преобразований (2…4, 7, 8, 11…14), третье – уравнение референц-эллипсоида Земли.

Поиск корней системы квадратных уравнений (15) возможен одним из численных методов, например, методом Ньютона – Рафсона, представляющим собой итерационный алгоритм, этапы которого детализированы ниже.

<u>*Этап 1*</u>. Выбирают произвольные опорные координаты $I(x_{I_1}, y_{I_1}, z_{I_1})$. Очевидно, что выбранные координаты должны принадлежать предварительно выбранному РВРМ. Так, например в качестве таких координат могут выступать координаты K или координаты подспутниковой точки (ПСТ) одного из двух КА.

<u>*Этап 2*</u>. Вычисляют значения функций R_{SD_1}, V_1, R_{3_1} в точке с опорными координатами ЗС x_{I_1}, y_{I_1}, z_{I_1}, выбранными на этапе 1:

$$R_{SD_1} = \sqrt{\left(x_S - x_{I_1}\right)^2 + \left(y_S - y_{I_1}\right)^2 + \left(z_S - z_{I_1}\right)^2} - \\ -\sqrt{\left(x_D - x_{I_1}\right)^2 + \left(y_D - y_{I_1}\right)^2 + \left(z_D - z_{I_1}\right)^2},$$

$$V_1 = \frac{(x_{I_1} - x_S)\dot{x}_S + (y_{I_1} - y_S)\dot{y}_S + (z_{I_1} - z_S)\dot{z}_S}{\sqrt{(x_{I_1} - x_S)^2 + (y_{I_1} - y_S)^2 + (z_{I_1} - z_S)^2}} - \\ -\frac{(x_{I_1} - x_D)\dot{x}_D + (y_{I_1} - y_D)\dot{y}_D + (z_{I_1} - z_D)\dot{z}_D}{\sqrt{(x_{I_1} - x_D)^2 + (y_{I_1} - y_D)^2 + (z_{I_1} - z_D)^2}},$$

$$R_{3_1} = \sqrt{b^2x_{I_1}^2 + b^2y_{I_1}^2 + a^2z_{I_1}^2}.$$

<u>*Этап 3*</u>. Определяют значения w_1, w_2 и w_3:

$$w_1 = R_{SD} - R_{SD_1},$$
$$w_2 = V - V_1,$$
$$w_3 = R_3 - R_{3_1}.$$

Этап 4. Формируют систему линейных уравнений, заменяя функции квадратного уравнения (15) рядами Тейлора, ограниченными членами, содержащими первые производные указанных функций и искомые смещения Δx, Δy и Δz по соответствующим координатам:

$$\begin{cases} \frac{\partial R_{SD_1}}{\partial x_{I_1}}\Delta x + \frac{\partial R_{SD_1}}{\partial y_{I_1}}\Delta y + \frac{\partial R_{SD_1}}{\partial z_{I_1}}\Delta z = w_1, \\ \frac{\partial V_1}{\partial x_{I_1}}\Delta x + \frac{\partial V_1}{\partial y_{I_1}}\Delta y + \frac{\partial V_1}{\partial z_{I_1}}\Delta z = w_2, \\ \frac{\partial R_{3_1}}{\partial x_{I_1}}\Delta x + \frac{\partial R_{3_1}}{\partial y_{I_1}}\Delta y + \frac{\partial R_{3_1}}{\partial z_{I_1}}\Delta z = w_3. \end{cases} \quad (16)$$

Значения частных производных в текущей опорной точке рассчитывают в соответствии с тождествами:

$$\frac{\partial R_{SD_1}}{\partial x_{I_1}} = \frac{x_{I_1}}{R_{DI_1}} - \frac{x_{I_1}}{R_{SI_1}}, \quad \frac{\partial R_{SD_1}}{\partial y_{I_1}} = \frac{y_{I_1}}{R_{DI_1}} - \frac{y_{I_1}}{R_{SI_1}},$$

$$\frac{\partial R_{SD_1}}{\partial z_{I_1}} = \frac{z_{I_1}}{R_{DI_1}} - \frac{z_{I_1}}{R_{SI_1}},$$

$$\frac{\partial V_1}{\partial x_{I_1}} = \frac{\dot{x}_S R_{SI_1} - (x_{I_1} - x_S)\dot{R}_{SI_1}}{R_{SI_1}^2} - \frac{\dot{x}_D R_{DI_1} - (x_{I_1} - x_D)\dot{R}_{DI_1}}{R_{DI_1}^2},$$

$$\frac{\partial V_1}{\partial y_{I_1}} = \frac{\dot{y}_S R_{SI_1} - (y_{I_1} - y_S)\dot{R}_{SI_1}}{R_{SI_1}^2} - \frac{\dot{y}_D R_{DI_1} - (y_{I_1} - y_D)\dot{R}_{DI_1}}{R_{DI_1}^2},$$

$$\frac{\partial V_1}{\partial z_{I_1}} = \frac{\dot{z}_S R_{SI_1} - (z_{I_1} - z_S)\dot{R}_{SI_1}}{R_{SI_1}^2} - \frac{\dot{z}_D R_{DI_1} - (z_{I_1} - z_D)\dot{R}_{DI_1}}{R_{DI_1}^2},$$

$$\frac{\partial R_{3_1}}{\partial x_{I_1}} = \frac{x_{I_1}}{R_{3_1}}, \quad \frac{\partial R_{3_1}}{\partial y_{I_1}} = \frac{y_{I_1}}{R_{3_1}}, \quad \frac{\partial R_{3_1}}{\partial z_{I_1}} = \frac{z_{I_1}}{R_{3_1}},$$

$$\frac{\partial R_{3_1}}{\partial x_{I_1}} = \frac{b^2 x_{I_1}}{R_{3_1}}, \quad \frac{\partial R_{3_1}}{\partial y_{I_1}} = \frac{b^2 y_{I_1}}{R_{3_1}}, \quad \frac{\partial R_{3_1}}{\partial z_{I_1}} = \frac{a^2 z_{I_1}}{R_{3_1}},$$

где R_{SI_1} и R_{DI_1} – дистанции от S и D до опорной точки, которые рассчитывают следующим образом:

$$R_{SI_1} = \sqrt{(x_S - x_{I_1})^2 + (y_S - y_{I_1})^2 + (z_S - z_{I_1})^2},$$

$$R_{DI_1} = \sqrt{(x_D - x_{I_1})^2 + (y_D - y_{I_1})^2 + (z_D - z_{I_1})^2},$$

$$\dot{R}_{SI_1} = \frac{(x_{I_1} - x_S)\dot{x}_S + (y_{I_1} - y_S)\dot{y}_S + (z_{I_1} - z_S)\dot{z}_S}{\sqrt{(x_{I_1} - x_S)^2 + (y_{I_1} - y_S)^2 + (z_{I_1} - z_S)^2}},$$

$$\dot{R}_{DI_1} = \frac{(x_{I_1} - x_D)\dot{x}_D + (y_{I_1} - y_D)\dot{y}_D + (z_{I_1} - z_D)\dot{z}_D}{\sqrt{(x_{I_1} - x_D)^2 + (y_{I_1} - y_D)^2 + (z_{I_1} - z_D)^2}}.$$

Систему линейных уравнений (16) решают одним из известных методов, например, методом Гаусса; в качестве решения выступают искомые смещения Δx, Δy и Δz по соответствующим координатам.

Этап 5. Вычисляют новые опорные координаты ЗС путем добавления к предыдущим опорным координатам ЗС, рассчитанные на этапе 4 смещения Δx, Δy и Δz по соответствующим координатам:

$$x_{I_2} = x_{I_1} + \Delta x,$$
$$y_{I_2} = y_{I_1} + \Delta y,$$
$$z_{I_2} = z_{I_1} + \Delta z.$$

Этапы 1–5 составляют одну итерацию. Для достижения требуемой точности итерации повторяют с использованием в качестве опорных координат ЗС координаты, полученные на этапе 5. Число итераций определяется заданной точностью и правильностью выбора начальных опорных координат ЗС и, как правило, не превышает пяти.

При окончании алгоритма, в качестве координат ЗС принимают значения ее опорных координат, вычисленные на пятом этапе завершающей итерации.

При избыточности измерений, как это зачастую практикуется для обеспечения повышения точности, когда количество измерений более двух, возможно составить более трех квадратных уравнений (включая уравнение референц-эллипсоида поверхности Земли). Представленный метод координатометрии останется прежним, однако система квадратных уравнений (15), и как следствие, система линейных уравнений (16) будут содержать более трех уравнений. В этом случае систему линейных уравнений (16) решают одним из известных методов, например, методом наименьших квадратов.

Имитационное моделирование разработанного метода КМ ЗС для выбранных исходных данных

Важнейшей характеристикой любого метода КМ является точность оценки координат. Для оценки точности разработанного метода КМ ЗС проведено имитационное моделирование в среде программирования *Matlab* с использованием разработанной модели [11...12].

Для иллюстрации разработанного метода КМ ЗС выбраны исходные данные, представленные ниже.

В качестве модели Земли выбран референц-эллипсоид, соответствующий системе геодезиче-

ских параметров ПЗ-90.11, большая a и малая b, оси которого равны:

$$a = 6\,378\,136 \text{ м}, \quad b \approx 6\,356\,751 \text{ м}.$$

Координаты КРМ $\varphi = 54{,}8\,°$ с. ш.; $\lambda = 32{,}1\,°$ в. д.; $h = 39$ м, соответствующие координатам г. Смоленск (отображены на рисунках 2 и 3 кружком). Номиналы частот: $f_I = 8{,}5$ ГГц; $f_G = 12{,}3$ ГГц.

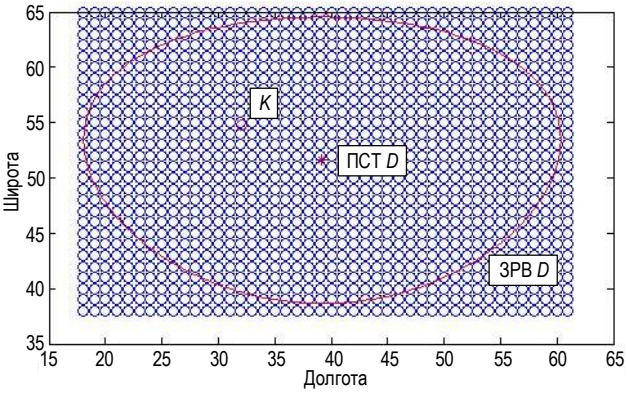


Рис. 2. Отображение координат подспутниковых точек КА *D*, КРМ *K* и исследуемых точек предполагаемого размещения ЗС

Fig. 2. Display of Sub-Satellite Points Coordinates of the Spacecraft D, Radio Monitoring Complex K and the Proposed Studied Points Placement of the Earth Station

Разработанный метод КМ ЗС инвариантен к типу орбит КА, задействованных для определения координат ЗС. В качестве примера представлены два КА с различными типами орбит:

– КА S – на геостационарной орбите с широтой 0,1 ° с. ш., долготой 50 ° в. д. и высотой 35 789 326 м;

– КА D – на низкой орбите с широтой 51,6 ° с. ш., долготой 39,2 ° в. д. и высотой 300 000 м.

Координаты и составляющие векторов скорости КА S и D в декартовой системе координат представлены в таблице 1.

Зоны радиовидимости (ЗРВ) КА S (синяя окружность рисунка 3) и КА D (красная окружность) рассчитаны, исходя из ограничения по минимальному углу места, равного $\beta_{min} = 5\,°$ (очевидно, что границы предварительно выбранного РВРМ не могут выходить за границы совместной ЗРВ КА S и D). На рисунке 3 также обозначены ПСТ КА S синей звездочкой и ПСТ КА D красной звездочкой.

ТАБЛИЦА 1. Координаты и составляющие векторов скорости КА *S* и *D* в декартовой системе координат

TABLE 1. Velocity Vectors Coordinates and Components of Spacecraft S and D in the Cartesian Coordinate System

№ п/п	КА	Координаты КА, м			Составляющие векторов скорости КА, м/с		
		x	y	z	$\dot{x}$	$\dot{y}$	$\dot{z}$
1	S	27 104 682	32 302 102	73522	–4	–1	3
2	D	3220886	2626891	5210389	6748	–928	–3680

Широты и долготы исследуемых координат предполагаемого размещения ЗС выбраны в соответствии с совместной ЗРВ КА S и D с градацией 1 ° в следующих диапазонах: по широте – от 38° с. ш. до 65 ° с. ш.; по долготе – от 18 ° в. д. до 61 ° в. д. (см. рисунок 2). Координаты ПСТ КА D отображены красной звездочкой, КРМ K – красным кружком и исследуемые точки предполагаемого размещения ЗС синими кружками.

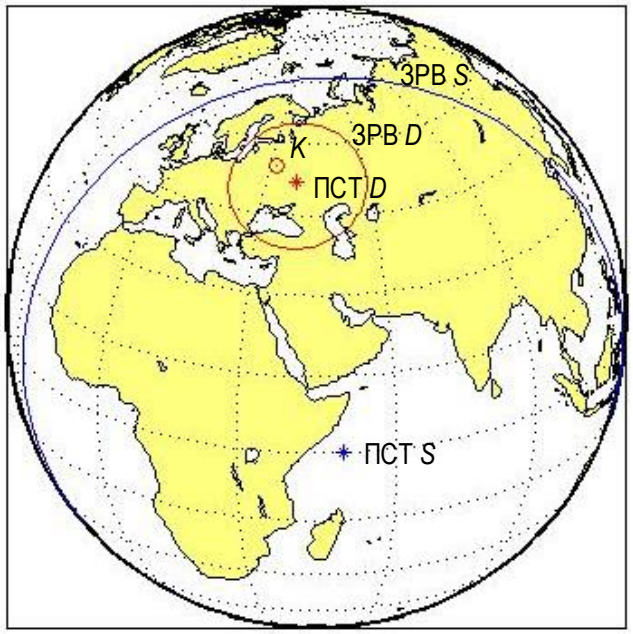


Рис. 3. Подспутниковые точки и зоны радиовидимостей космических аппаратов S и D

Fig. 3. Subsatellite Points and Radio Visibility Zones of Spacecraft S and D

Вводимые погрешности: координат КА $\sigma_S = 30$ м (для каждой их 3-х координат), вектора скорости $\sigma_V = 1$ м/с (для каждой их 3-х ортогональных составляющих), измерения частот $\sigma_f = 100$ Гц, измерения временной задержки $\sigma_t = 200$ нс. Для каждой из выбранных точек предполагаемого размещения ЗС провели следующие процедуры:

– для текущей точки размещения ЗС и каждой из двух точек размещения космических аппаратов рассчитали идеальные временну́ю задержку и НСЧ, то есть такие, какие были бы измерены при нулевых погрешностях измерений;

– ввели погрешности σ_S, σ_V, σ_f и σ_t с учетом их нормального распределения;

– по полученным значениям временно́й задержки и НСЧ, используя вышеописанный метод, рассчитали координаты ЗС для текущей исследуемой точки;

– усреднили координаты ЗС по результатам 1000 экспериментов;

– сравнили заданные и рассчитанные координаты ЗС, получили погрешность измерения σ_L;

– по результатам расчета погрешностей для всех исследуемых точек предполагаемого разме-

щения ЗС построили изолинии радиусов среднеквадратического отклонения оценки координат (изолинии для заданных условий представлены на рисунке 4).

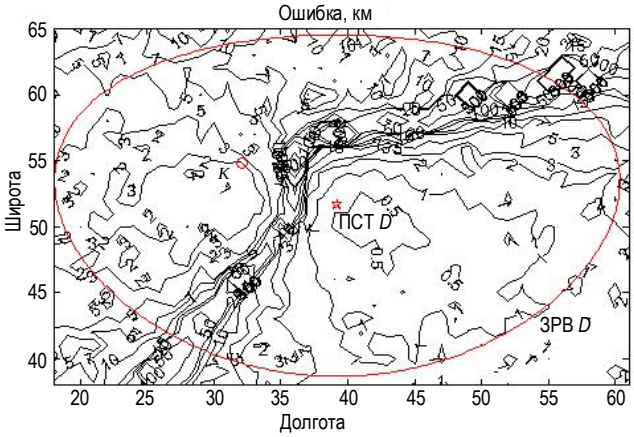


Рис. 4. Изолинии радиусов среднеквадратического отклонения оценки координат ЗС разработанного метода КМ для заданных условий

Fig. 4. Isolines of the Standard Deviation Radii of the Earth Station Coordinates of the Developed Coordinate Meas-urement Method for the Given Conditions

Координаты ПСТ КА *D* отображены красной звездочкой (см. рисунок 4), КРМ *K* – красным кружком и ЗРВ КА *D* – красной окружностью (линия несколько отличается от окружности, поскольку здесь представлено отображение проекции сферических координат в декартовой системе координат). Анализ изолиний радиусов среднеквадратического отклонения оценки координат ЗС, реализующей разработанный метод КМ для заданных условий, позволяет условно разделить ЗРВ КА *D* на рабочую и нерабочую области. В рабочей области точность оценки координат ЗС не превышает единиц километров, что вполне приемлемо для ряда задач. В нерабочей области точность оценки координат ЗС принимает недопустимые значения и может превышать сотни километров. Очевидно, что размер и границы указанных рабочей и нерабочей областей зависят прежде всего от топологии (взаимного расположения) КРМ *K*, КА *D* и КА *S*, а она не является статичной. Если движением КА *S* в рамках рассматриваемой топологии КРМ *K*, КА *D* и КА *S* возможно пренебречь, то КА *D* движется со скоростью более 7 км/с. Так, если орбита КА *D* является квазиполярной и движение КА *D* на витке осуществляется с юга на север, то уже через 3 мин. ЗРВ КА *D* нерабочая и рабочая зоны (с некоторыми изменениями) сместятся на север более чем на 10 °. Тогда, там, где просматривается нерабочая зона (см. рисунок 4), зона станет рабочей.

Еще одной особенностью представленной топологии КРМ *K*, КА *D* и КА *S*, является ее видоизменение на каждом витке КА *D*. Так, на следующем витке, период которого для выбранной высоты КА *D* составит чуть более полутора часов, поверхность Земли «сместится» более чем на 22 ° с запада на восток в ходе ее суточного вращения (при грубом приближении поверхность Земли смещается относительно «неподвижных» звезд за сутки – на 360 °, а за один час – на 15 °). Соответственно, и ЗРВ КА *D*, нерабочая и рабочая зоны (с некоторыми изменениями) сместятся на запад более чем на 22 °.

Границу РВРМ выбранного варианта предложенного метода КМ земной станции возможно описать, как окружность на поверхности референц-эллипсоида Земли, имеющую центр в районе размещения КРМ *K* и радиус не менее 1500 км. Определение координат ЗС, находящейся в указанном РВРМ будет возможно с некоторой периодичностью, обусловленной меняющейся с течением времени топологией КРМ *K*, КА *D* и КА *S*.

Заключение

В статье представлен комбинированный (разностно-дальномерный и разностно-доплеровский) метод КМ ЗС, основанный на одномоментном приеме ретранслированного радиосигнала указанной станции КРМ через два КА.

Показан вывод аналитических соотношений для расчета координат ЗС на основе значений взаимных временны́х задержек и частотных сдвигов одной и той же реализации радиосигнала ЗС, обусловленные различными радиотрассами через КА *D* и КА *S*. Составлена система из трех независимых уравнений. При этом в качестве первого выступает разностно-дальномерное уравнение, в качестве второго – разностно-радиально-скоростное, а в качестве третьего – уравнение референц-эллипсоида Земли. Результатом решения системы уравнений второго порядка является координаты ЗС. Для решения указанной системы уравнений предложен итерационный метод Ньютона – Рафсона с разложением функций в ряды Тейлора с точностью до первых производных.

В качестве иллюстрации разработанного метода приведен частный пример расчета. Разработанный метод КМ инвариантен к типу орбит КА, задействованных для определения координат ЗС. В качестве примера представлены два космических аппарата: первый – на геостационарной орбите, второй – на низкой орбите.

В ходе имитационного моделирования получены изолинии радиусов среднеквадратического отклонения оценки координат ЗС, реализующей разработанный метод КМ для заданных условий.

Выявлено наличие рабочей и нерабочей областей в совместной ЗРВ двух космических аппаратов, характерные и для альтернативных методов

КМ, обусловленные топологией (взаимным расположением) КРМ, КА *D* и КА *S*.

В рабочей области точность оценки координат ЗС не превышает единиц километров, что вполне приемлемо для решения ряда практических задач. В нерабочей области точность оценки координат принимает недопустимые значения и может превышать сотни километров.

Практическая значимость предложенного метода заключается в возможности его применения в существующих и перспективных КРМ для оценки координат ЗС, нелегитимно использующих частотно-временно́й ресурс КА, а также являющихся источниками преднамеренных или непреднамеренных радиопомех.

Представленный метод КМ может быть использован в образовательном процессе для подготовки соответствующих специалистов, а также при проектировании, эксплуатации и модернизации КРМ. Дальнейшие исследования могут затрагивать альтернативные методы КМ ЗС, а также их комплексирование с известными методами.

Список источников

1. Симонов А.Н., Волков Р.В., Дворников С.В. Основы построения и функционирования угломерных систем координатометрии источников радиоизлучений: учеб. пособие. СПб.: ВАС, 2017. 248 с. EDN:XRBXML
2. Dvornikov S.V., Sevidov V.V. Optimal points of a two-position goniometric coordinateometry system // H&ES Research. 2024. Vol. 16. Iss. 5. PP. 59–65. DOI:10.36724/2409-5419-2024-16-5-59-65. EDN:WZHCUI
3. Дворников С.В., Волков Р.В., Желнин С.Р., Саяпин В.Н., Симонов А.Н. Основы построения и функционирования угломерно-дальномерных систем координатометрии источников радиоизлучений: учеб. пособие. СПб.: ВАС, 2008. 104 с. EDN:WWJMJF
4. Волков Р.В., Дворников С.В., Саяпин В.Н., Симонов А.Н. Основы построения и функционирования разностно-дальномерных систем координатометрии источников радиоизлучений: учеб. пособие. СПб.: ВАС, 2013. 116 с. EDN:WMPHZX
5. Севидов В.В., Фокин Г.А. Разностно-дальномерный способ определения местоположения источника радиоизлучения в условиях многолучевого распространения радиоволн. Патент на изобретение RU 2805566 C1 от 03.04.2023. Опубл. 19.10.2023. EDN:KFBCOT
6. Фокин Г.А., Лазарев В.О. Оценка точности позиционирования источника радиоизлучения разностно-дальномерным и угломерным методами. Часть 3. 3D-моделирование // Труды учебных заведений связи. 2020. Т. 6. № 2. С. 87–102. DOI:10.31854/1813-324X-2020-6-2-87-102. EDN:FKSYIZ
7. Булычев Ю.Г., Мозоль А.А., Кондрашов А.Г., Жук А.С. Энергетический метод квазиоптимальной однопозиционной локации и навигации движущегося источника излучения с учетом априорной информации // Журнал радиоэлектроники. 2018. № 12. С. 4. DOI:10.30898/1684-1719.2018.12.15. EDN:YSTVKP
8. Ковалев Ф.Н. Точность местоопределения цели в бистатической радиолокационной системе // Успехи современной радиоэлектроники. 2022. Т. 76. № 4. С. 4–7. EDN:ZAOPDP
9. Ячменев А.В. Оценка эффективности гибридного метода пассивной локации // Вопросы радиоэлектроники. Серия: Техника телевидения. 2022. № 2. С. 79–83. EDN:HZOEZD
10. Агиевич С.Н., Дворников С.В., Севидов В.В., Эконом В.П. Определение координат морских объектов, терпящих бедствие, с использованием беспилотного летательного аппарата // VI Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017, Санкт-Петербург, Российская Федерация, 01–02 марта 2017 г.). СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2017. С. 14–20. EDN:YRPZGC
11. Богдановский С.В., Симонов А.Н., Медведев М.В., Теслевич С.Ф. Программа исследования ошибок определения координат в разностно-дальномерной системе. Свидетельство о государственной регистрации программы для ЭВМ. 2015. EDN:WFZZNJ
12. Полянский И.С., Полянская И.В., Фам Т.З. Математическая модель фильтрации канонических параметров спутника-ретранслятора при орбитальном движении // Физика волновых процессов и радиотехнические системы. 2019. Т. 22. № 4-1. С. 50–57. DOI:10.18469/1810-3189.2019.22.4.50-57. EDN:FHEZRK

References

1. Simonov A.N., Volkov R.V., Dvornikov S.V. *Fundamentals of Construction and Operation of Goniometric Systems for Coordinate Measurement of Radio Emission Sources*. St. Petersburg: VAS Publ.; 2017. 248 p. (in Russ.) EDN:XRBXML
2. Dvornikov S.V., Sevidov V.V. Optimal points of a two-position goniometric coordinateometry system. *H&ES Research*. 2024;16(5):59–65. DOI:10.36724/2409-5419-2024-16-5-59-65. EDN:WZHCUI
3. Dvornikov S.V., Volkov R.V., Zhelnin S.R., Sayapin V.N., Simonov A.N. *Fundamentals of Construction and Operation of Angle-Range Measuring Systems for Coordinate Measurement of Radio Emission Sources*. St. Petersburg: VAS Publ.; 2008. 104 p. (in Russ.) EDN:WWJMJF
4. Volkov R.V., Dvornikov S.V., Sayapin V.N., Simonov A.N. *Fundamentals of Construction and Operation of Difference-Range Measuring Systems for Coordinate Measurement of Radio Emission Sources*. St. Petersburg: VAS Publ.; 2013. 116 p. (in Russ.) EDN:WMPHZX

5. Sevidov V.V., Fokin G.A. *Difference-Range Measurement Method for Determining the Location of a Radio Emission Source under Conditions of Multipath Propagation of Radio Waves*. Patent RF, no. 2805566 C1, 03.04.2023. (in Russ.) EDN:KFBCOT

6. Fokin G., Lazarev V. Positioning Accuracy Evaluation of Radio Emission Sources Using Time Difference of Arrival and Angle of Arrival Methods. Part 3. 3D-Simulation. *Proceedings of Telecommunication Universities*. 2020;6(2):87–102. (in Russ.) DOI:10.31854/1813-324X-2020-6-2-87-102. EDN:FKSYIZ.

7. Bulychev Yu.G., Mozol A.A., Kondrashov A.G., Yachmenev A.V., Zhuk A.S. Energy method of quasi-optimal single-position location and navigation of a moving radiation source with allowance for a priori information. *Journal of Radio Electronics*. 2018;12:4. (in Russ.) DOI:10.30898/1684-1719.2018.12.15. EDN:YSTVKP

8. Kovalev F.N. Accuracy of Target Location in a Bistatic Radar System. *Achievements of Modern Radioelectronics*. 2022; 76(4):4–7. (in Russ.) EDN:ZAOPDP

9. Yachmenev A.V. Evaluation of the Efficiency of the Hybrid Method of Passive Location. *Voprosy radioelektroniki Seriia Tekhnika televideniia*. 2022;2:79–83. (in Russ.) EDN:HZOEZD

10. Agievich S., Dvornikov S., Sevidov V., Econom V. The Determination of the Coordinates of Sea Objects in Distress with the Use of Unmanned Aircraft Systems. *Proceedings of the VIth International Conference on Infotelecommunications in Science and Education, 1–2 March 2017, St. Petersburg, Russian Federation*. St. Petersburg: Saint-Petersburg State University of Telecommunications Publ.; 2017. p.14–20. (in Russ). EDN:YRPZGC

11. Bogdanovsky S.V., Simonov A.N., Medvedev M.V., Teslevich S.F. *The Program of the Study of Errors of Determination of Coordinates in Differential-Distance Measuring System*. Patent RF, 2015. (in Russ.) EDN:WFZZNJ

12. Polyanskii I.S., Polyanskaya I.V., Pham T.Z. Mathematical Model Filtering Canonical Parameters of Satellite-Repeater in Orbital Motion. *Physics of Wave Processes and Radio Systems.* 2019;22(4-1):50–57. (in Russ.) DOI:10.18469/1810-3189.2019.22.4.50-57. EDN:FHEZRK

Статья поступила в редакцию 28.11.2024; одобрена после рецензирования 22.01.2025; принята к публикации 23.01.2025.
The article was submitted 28.11.2024; approved after reviewing 22.01.2025; accepted for publication 23.01.2025.

Информация об авторе:

СЕВИДОВ Владимир Витальевич | докторант кафедры радиоэлектронной борьбы Военной академии связи имени Маршала Советского Союза С.М. Буденного
https://orcid.org/0009-0009-2413-1615

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

Научная статья
УДК 621.391
https://doi.org/10.31854/1813-324X-2025-11-1-53-61
EDN:DHIQLJ

Разнесенный прием сигналов Wi-Fi с использованием коммутируемой антенной решетки

Иван Сергеевич Фаустов[1, 2] ✉, faustov.97@bk.ru
Владимир Борисович Манелис[2], vbm@ircoc.vrn.ru
Владимир Алексеевич Козьмин[2], kozminva@ircos.ru
Антон Борисович Токарев[1, 2], tokarevab@ircoc.vrn.ru

[1]Воронежский государственный технический университет,
Воронеж, 394006, Российская Федерация
[2]АО «ИРКОС»,
Москва, 129626, Российская Федерация

Аннотация

Актуальность. *Активное использование беспроводных технологий требует развития средств контроля беспроводных сетей передачи данных, в частности сетей Wi-Fi. Службами радиоконтроля решаются задачи обнаружения, идентификации и локализации не санкционированно работающих точек доступа и абонентских устройств. Эффективным инструментом пеленгования радиосигналов являются корреляционно-интерферометрические пеленгаторы на базе двухканальной приемной аппаратуры и многоэлементной антенной системы. Развитие методов совместной идентификации и пеленгования позволяет разделять пеленги большого количества источников сигналов, ведущих работу в одном частотном диапазоне с разделением по времени. В настоящей работе акцент сделан на обнаружении целевых сигналов и выделении из них идентификационных признаков источника. От успешности реализации этих операций будут существенно зависеть и показатели качества пеленгования.*

Целью работы *является исследование возможностей повышения помехоустойчивости обнаружения и идентификации сигналов Wi-Fi за счет совместного использования двух каналов приема корреляционно-интерферометрического пеленгатора. В работе использованы* ***методы*** *статистического компьютерного моделирования, которые учитывают наличие замираний, возникающих из-за многолучевости канала распространения, и корреляцию радиосигналов, вызванную близким расположением приемных антенн.*

Решение. *Рассмотрены алгоритмы обнаружения частотно-временно́й синхронизации и демодуляции сигналов Wi-Fi. Предложены способы объединения каналов приема при обработке сигналов. Исследована помехоустойчивость предложенных двухканальных алгоритмов обработки сигнала при наличии квазистационарных релеевских замираний и корреляции каналов приема.*

Новизна. *Разработаны алгоритмы двухканального обнаружения, частотно-временно́й синхронизации и демодуляции сигналов Wi-Fi.*

Практическая значимость. *Совместное использование двух каналов приема при обнаружении и идентификации сигналов Wi-Fi позволяет увеличить помехоустойчивость систем радиоконтроля на 4–7 дБ даже при наличии корреляции между каналами.*

Ключевые слова: *разнесенный прием, Wi-Fi, коммутируемая антенная решетка, радиомониторинг, релеевский канал*

Ссылка для цитирования: Фаустов И.С., Манелис В.Б., Козьмин В.А., Токарев А.Б. Разнесенный прием сигналов Wi-Fi с использованием коммутируемой антенной решетки // Труды учебных заведений связи. 2025. Т. 11. № 1. С. 53–61. DOI:10.31854/1813-324X-2025-11-1-53-61. EDN: DHIQLJ

Original research
https://doi.org/10.31854/1813-324X-2025-11-1-53-61
EDN:DHIQLJ

Antenna Diversity of Wi-Fi Signals Using a Switched Antenna Array

Ivan S. Faustov[1, 2] ✉, faustov.97@bk.ru
Vladimir B. Manelis[2], vbm@ircoc.vrn.ru
Vladimir A. Kozmin[2], kozminva@ircos.ru
Anton B. Tokarev[1, 2], tokarevab@ircoc.vrn.ru

[1]Voronezh State Technical University,
Voronezh, 394006, Russian Federation
[2]IRCOS JSC
Moscow, 129626, Russian Federation

Annotation

Relevance. *The active use of wireless technologies requires the development of controls for wireless networks, in particular Wi-Fi networks. Radio monitoring services solve the tasks of detecting, identifying and localizing unauthorized access points and clients. An effective tool for bearing radio signals is correlation interferometric direction finders based on two-channel receiving equipment and a multi-element antenna system. The development of methods of joint identification and bearing makes it possible to separate the bearings of a large number of signal sources operating in the same frequency range with time division. In this work, the emphasis is placed on the detection of target signals and the identification of source features from them. The indicators of the quality of bearing will also significantly depend on the success of these operations.*

The aim *of the work is to investigate the possibilities of increasing the interference resistance of detecting and identifying Wi-Fi signals through the combined use of two channels of a correlation interferometric detector.*

Methods. *The paper uses statistical computer modeling methods that take into account the presence of fading due to multipath propagation channel and the correlation of radio signals caused by the proximity of receiving antennas.*

Decision. *Algorithms of detection, time-frequency synchronization and demodulation of Wi-Fi signals are considered. Methods of combining receiving channels in signal processing are proposed. The noise immunity of the proposed two-channel signal processing algorithms in the presence of quasi-stationary Relay fades and correlation of receiving channels is investigated.*

Novelty. *Algorithms for two-channel detection, time-frequency synchronization and demodulation of Wi-Fi signals have been developed.*

Practical significance. *The combined use of two reception channels for the detection and identification of Wi-Fi signals allows you to increase the reliability of radio monitoring systems by 4–7 dB, even if there is a correlation between the channels.*

Keywords: *antenna diversity, Wi-Fi, switched antenna array, radio monitoring, Rayleigh channel*

For citation: Faustov I.S., Manelis V.B., Kozmin V.A., Tokarev A.B. Antenna Diversity of Wi-Fi Signals Using a Switched Antenna Array. *Proceedings of Telecommunication Universities.* 2024;10(6):53–61. (in Russ.) DOI:10.31854/1813-324X-2024-10-6-53-61. EDN:DHIQLJ

Введение

Современное поколение беспроводных систем связи (БСС) ближнего действия, в частности Wi-Fi, обеспечивает передачу различных видов информации на высоких скоростях в широкой полосе частот. Необходимость радиоконтроля таких систем, включая обнаружение, идентификацию и локализацию, является актуальной задачей служб радиоконтроля [1–4]. Эффективным инструментом пеленгования радиосигналов является корреляционно-интерферометрический пеленгатор на

базе двухканальной приемной аппаратуры, использующей многоэлементную антенную решетку (АР) [5]. Некоммутируемый канал приема постоянно подключен к нулевому элементу АР, а другой – коммутируемый, последовательно подключается к элементам АР с номерами $\overline{1, M-1}$, где M – количество элементов АР. Коммутируемость антенных элементов позволяет при пеленговании использовать двухканальное радиоприемное устройство вместо M-канального.

Пеленгование источников БСС часто осложняется тем, что они выходят в эфир с разделением по времени, используя общую полосу частот. Это может порождать аномальные ошибки, если в расчете пеленга источника задействованы смежные по времени пакеты, создаваемые другими источниками. Известен ряд методов многосигнальной классификации (MUSIC, ESPRIT и др.), предназначенных для пеленгования подобных сигналов. Однако эти методы, как правило, вычислительно затратные и требуют предварительной оценки количества работающих устройств. Применительно к пеленгованию источников БСС можно существенным образом снизить вероятность возникновения аномальных ошибок, если для классификации пакетов данных использовать идентификационную информацию, передаваемую в этих пакетах. Вышеизложенное привело к развитию методов совместной идентификации и пеленгования (адресного пеленгования) источников различных систем связи [3, 4].

Совмещение процессов обнаружения, идентификации и оценивания угловых координат источника радиоизлучений (ИРИ) позволяет:

– осуществлять идентификацию и пеленгование источников сигналов различной длительности, в том числе кратковременных;

– разделять пеленги большого количества ИРИ, ведущих работу в одном частотном диапазоне с разделением по времени, благодаря привязке уникальных идентификационных признаков к направлению на источник.

В настоящей работе акцент сделан на обнаружении целевых сигналов и выделении из них идентификационных признаков источника. От успешности реализации этих операций будут существенно зависеть и частота возникновения аномальных ошибок при пеленговании. В городских условиях и внутри помещений обнаружение и прием сигналов могут существенно осложняться в случае низкого отношения сигнал / шум и при наличии замираний, обусловленных многолучевостью канала распространения. Одним из методов повышения качества приема в таких условиях является разнесенный прием, который может быть реализован на базе двух каналов корреляционного интерферометра. При этом следует учитывать, что для реализации разнесенного приема желательно, чтобы принимаемые сигналы были не коррелированы, а значит, приемные антенны расположены на существенном удалении друг от друга [6]. С другой стороны, для пеленгования элементы АР расположены достаточно близко друг к другу (обычно на расстоянии менее длины волны).

В этой связи, целью настоящей работы является исследование возможности повышения помехоустойчивости обнаружения и идентификации сигналов стандарта 802.11a/n/ac/ax на основе совместного использования двух каналов приема с учетом корреляции радиосигналов, обусловленной близким расположением приемных антенн.

Модель канала связи и пространственной корреляции

В данной работе использовалась модель канала связи, включающая N_{TX} передающих и N_{RX} приемных антенн из [6–8]. В рамках этой модели вектор $\boldsymbol{y}$ принимаемых сигналов размерности $N_{RX} \times 1$ связан с вектором $\boldsymbol{s}$ передаваемых сигналов размерности $N_{TX} \times 1$ соотношением:

$$\boldsymbol{y} = \boldsymbol{s}\boldsymbol{H}_{\boldsymbol{CORR}} + \boldsymbol{n}, \quad (1)$$

где $\boldsymbol{H}_{\boldsymbol{CORR}}$ – комплексная матрица радиоканала размерности $N_{RX} \times N_{TX}$, которая является квазистационарной (т. е., стационарной на периоде передачи пакета); $\boldsymbol{n}$ – вектор размерности $N_{RX} \times 1$, представляющий собой комплексный белый гауссовский шум с нулевым средним и ковариационной матрицей:

$$E[\boldsymbol{n}\boldsymbol{n}^T] = \sigma_n^2 \boldsymbol{I},$$

где $(\cdot)^T$ – комплексное транспонирование матрицы; $E[]$ – математическое ожидание; $\boldsymbol{I}$ – единичная матрица размерности $N_{RX} \times N_{RX}$; σ_n^2 – дисперсия шума.

Отношение сигнал / шум для одной приемной антенны составляет:

$$\rho = \frac{\sigma_s^2 N_{TX}}{\sigma_n^2},$$

где $E[\boldsymbol{s}\boldsymbol{s}^T] = \sigma_s^2 N_{TX}$ – мощность сигналов, излучаемая с помощью всех передающих антенн; σ_s^2 – дисперсия сигнала, излучаемого с помощью одной передающей антенны.

Согласно [6–8], зависимость между составляющими коэффициентов передачи каналов разнесенного приема для релеевских каналов характеризуется коэффициентами взаимной корреляции. Эти коэффициенты являются составляющими эрмитовой матрицы корреляционных коэффициентов:

$$\boldsymbol{R} = \begin{bmatrix} 1 & \cdots & r_{1,N} \\ \vdots & \ddots & \vdots \\ r_{N,1} & \cdots & 1 \end{bmatrix}, \quad (2)$$

где $r_{i,j}$, $i,j = 1,2,..,N$ – коэффициент пространственной корреляции между соответствующими антеннами; N – количество антенн.

Матрица радиоканала с учетом пространственной корреляции имеет вид [7]:

$$\boldsymbol{H}_{CORR} = \boldsymbol{\Gamma}\boldsymbol{H}, \quad (3)$$

где $\boldsymbol{H}$ – матрица радиоканала без пространственной корреляции; матрица $\boldsymbol{\Gamma}$ может быть найдена с помощью разложения Холецкого (метода квадратного корня) из условия:

$$\boldsymbol{\Gamma}\boldsymbol{\Gamma}^T = \boldsymbol{R}_{TX} \otimes \boldsymbol{R}_{RX}, \quad (4)$$

где $\boldsymbol{R}_{TX}$ – корреляционная матрица размерности $N_{TX} \times N_{TX}$ на передающей стороне; $\boldsymbol{R}_{RX}$ – корреляционная матрица размерности $N_{RX} \times N_{RX}$ на приемной стороне; $\otimes$ – оператор Кронекера.

Реализация разнесенного приема при пеленговании

На рисунке 1 представлена общая схема совместной идентификации и пеленгования сигналов стандарта 802.11a/n/ac/ax с использованием коммутируемой M-элементной АР. Индекс некоммутируемого канала положим равным $m = 0$, а коммутируемого – $m = 1$. При этом количество одновременно доступных каналов приема $N_{RX} = 2$.

Декодирование пакетов сигнала позволяет выделять идентификационные признаки ИРИ и объединять разрозненные фрагменты выборок при пеленговании конкретного ИРИ. В качестве идентификационного признака служит MAC-адрес устройства – уникальный идентификатор, присваиваемый каждой единице сетевого устройства Wi-Fi. Направление прихода сигнала вычисляется с использованием стандартного фазоразностного метода, при этом расчет производится по отсчетам пакетов с совпадающими MAC-адресами [3, 4].

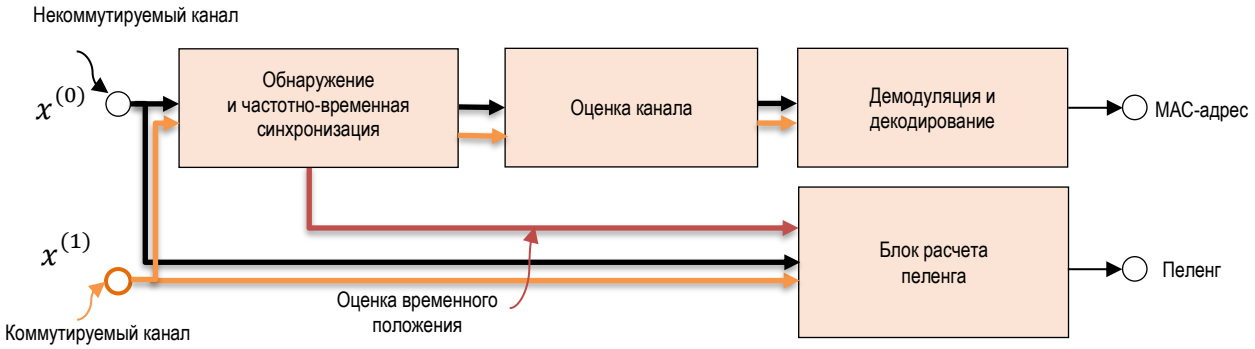


Рис. 1. Процедура адресного пеленгования сигналов 802.11a/n/ac/ax

Fig. 1. The Procedure of Address Bearing for 802.11a/n/ac/ax Signals

Обнаружение и частотно-временна́я синхронизация

Предложенный алгоритм обнаружения и синхронизации использует преамбулу Wi-Fi сигнала, которая состоит из двух частей (см. рисунок 2). Первая часть преамбулы L-STF (*аббр. от англ.* Legacy Short Training Field) представляет собой $J = 10$ коротких кодовых последовательностей длительностью τ_1. Вторая часть преамбулы L-LTF (*аббр. от англ.* Legacy Long Training Field) содержит две длинные кодовые последовательности длительностью τ_2 и защитный интервал (GI, *аббр. от англ.* Guard Interval) длительностью $\tau_2/2$ [9–12].

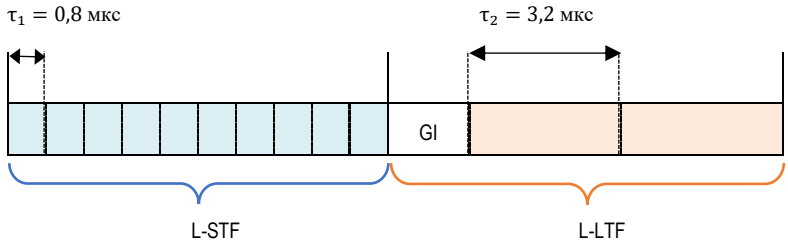


Рис. 2. Структура преамбулы сигналов 802.11a/n/ac/ax

Fig. 2. The Preamble Structure of 802.11a/n/ac/ax Signals

Обнаружение и частотно-временна́я синхронизация осуществляется в два этапа. На первом этапе выполняется обнаружение первой части преамбулы и оценка ее временно́го положения. Для этого формируется решающая функция:

$$\Lambda_n = \sum_{m=0}^{1} U_n^{(m)}, \tag{5}$$

где $U_n^{(m)} = \sum_{r=0}^{L_1-1} x_{n+r}^{(m)} \cdot s_r^*$ – результат корреляции входного сигнала и одного символа L-STF; $\boldsymbol{s} = (s_0, s_1, \dots, s_{L_1-1})$ – комплексные отсчеты одного элементарного символа; L_1 – длина короткого символа в отсчетах; $m = 0,1$ – номер канала; $(\cdot)^*$ – комплексное сопряжение.

Определяется максимум функции (5) $\Lambda_{(\max)}$ и его положение $n1 = \arg\max_n \Lambda_n$.

Решение об обнаружении первой части преамбулы выносится в случае выполнения условия:

$$\Lambda_{(\max)} > h_1 \sum_{r=0}^{J\cdot L_1-1} \sum_{m=0}^{1} \left|x_{n1}^{(m)}\right|^2, \tag{6}$$

где $h_1 = 2,5$ – пороговое значение первого этапа, выбранное эмпирически. В этом случае $n1$ является приближенной оценкой начала преамбулы.

Найдем на первом этапе предварительную оценку частотной расстройки Δf_1 между несущими входного и опорного сигналов. Для этой оценки используется фазоразностный метод, в соответствии с которым:

$$\Delta f_1 = \frac{1}{2\pi\tau_1} \times \\ \times \arg\left(\sum_{m=0}^{1} \sum_{j=1}^{J-1} U_{n1+j\cdot L_1}^{(m)} \cdot \left[U_{n1+(j-1)\cdot L_1}^{(m)}\right]^*\right). \tag{7}$$

На втором этапе поиск L-LTF производится на априорном интервале $[n_A; n_B]$, $n_A = n1 + (J-2)\cdot L_1$, $n_B = n1 + (J+2)\cdot L_1$ с учетом предварительной оценки частотной расстройки (7). Решающая статистика второго этапа имеет вид:

$$\Upsilon_n = \sum_{m=0}^{1} \left| \sum_{i=0}^{L_2-1} a_i^* \cdot x_{n+i}^{(m)} \cdot \exp\left(-j \cdot 2\pi\Delta f_1 \cdot \frac{n+i}{f_s}\right) \right|^2, \tag{8}$$

$$n \in [n_A; n_B],$$

где $\boldsymbol{a} = (a_0, a_1, \dots, a_{L_2-1})$ – комплексные отсчеты L-LTF; L_2 – длина L-LTF в отсчетах; f_s – частота дискретизации сигнала.

Определяется максимум функции (8) $\Upsilon_{(\max)}$ и его положение $n2 = \arg\max_n \Upsilon_n$.

Преамбула считается окончательно обнаруженной в случае выполнения условия:

$$\Upsilon_{(\max)} > h_2 \sum_{m=0}^{1} \sum_{i=0}^{L_2-1} \left|x_{n2+i}^{(m)}\right|^2, \tag{9}$$

где $h_2 = 25$ – пороговое значение второго этапа, выбранное эмпирически. Величина $n2$ в этом случае является оценкой временного положения второй части преамбулы L-LTF, по которой легко находится начало символов данных.

Окончательная оценка частотной расстройки для обоих каналов приема находится, как:

$$\Delta f = \Delta f_1 + \frac{1}{2\pi\tau_2} \cdot \arg\left(\sum_{m=0}^{1} R_{n2+\frac{L_2}{2.5}}^{(m)} \cdot \left[R_{n2+\frac{2\cdot L_2}{2.5}}^{(m)}\right]^*\right), \\ R_n^{(m)} = \sum_{i=0}^{\frac{L_2}{2.5}-1} x_{i+n}^{(m)} \cdot a_{i+\frac{L_2}{2.5}}^*. \tag{10}$$

Оценка канала и демодуляция

После установления частотно-временно́й синхронизации производятся процедуры приема пакета. Они показаны на рисунке 3. Для обоих каналов приема оценка частотного отклика канала выполняется независимо.

Начальная оценка канала может быть рассчитана по известным длинным символам L-LTF [13, 14]:

$$H_k^{(m)} = \frac{Y_{1,k}^{(m)} + Y_{2,k}^{(m)}}{2 \cdot B_k}, \tag{11}$$

где $H_k^{(m)}$ – канальный множитель k-й поднесущей; $Y_{1,k}^{(m)}, Y_{2,k}^{(m)}$ – быстрое преобразование Фурье (БПФ) первого и второго символов L-LTF; B_k – известные данные символов L-LTF; $m = 0,1$.

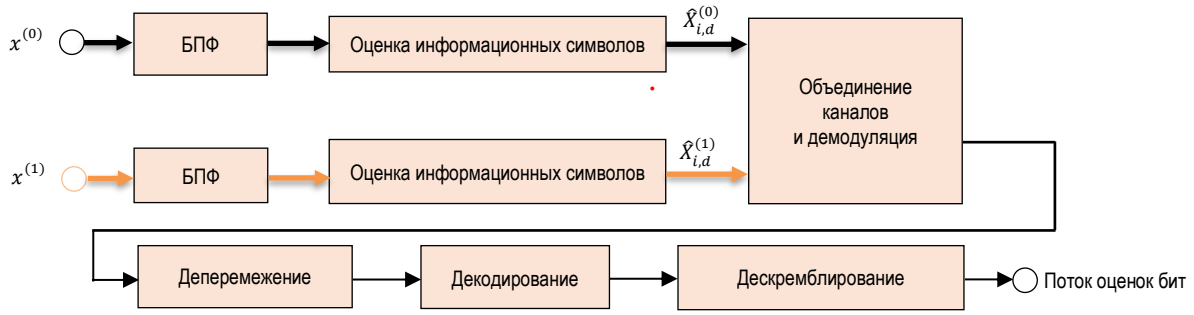


Рис. 3. Схема разнесенного приема сигналов стандарта IEEE 802.11a/n/ac/ax

Fig. 3. The Scheme of Diversity Antenna for IEEE 802.11a/n/ac/ax Signals

Частотный отклик канала в общем случае меняется со временем. Эти изменения оцениваются с помощью известных пилотных поднесущих сигнала. Будем следовать алгоритму из [15, 16]. По пилотным поднесущим оценивается разность фаз между текущим OFDM-символом пакета и второй частью преамбулы (11):

$$\varphi_i^{(m)} = \arg\left(\sum_{n\in \boldsymbol{v_P}} \frac{Y_{i,n}^{(m)}}{H_n^{(m)}} \cdot p_{i,n}\right), \qquad (12)$$

где i – индекс текущего OFDM-символа; $\boldsymbol{v_P}$ – вектор, содержащий индексы пилотных поднесущих; $p_{i,n}$ – известный элемент i-го пилот-символа n-й поднесущей.

Далее производится коррекция информационных поднесущих текущего i-го OFDM-символа:

$$\hat{Y}_{i,d}^{(m)} = Y_{i,d}^{(m)} \cdot \exp\left(-j\varphi_i^{(m)}\right), \qquad (13)$$

где $d\in\boldsymbol{v_d}$, $\boldsymbol{v_d}$ – вектор, содержащий индексы информационных поднесущих.

Окончательно двухканальная оценка символов модуляции поднесущих i-го OFDM-символа равна:

$$\hat{X}_{i,d} = \frac{1}{2}\sum_{m=0}^{1} \frac{\hat{Y}_{i,d}^{(m)}}{H_d^{(m)}}. \qquad (14)$$

В случае кодирования LDPC выполняется деперемежение оценок символов модуляции поднесущих в соответствии со стандартом [9–12].

Из массива оценок информационных символов (14) для каждой d-й информационной поднесущей i-го OFDM-символа получаем мягкие решения кодированных бит [17]:

$$\theta_{i,d}^{(k)} = \min_{X\in\Omega_k^{(1)}} \left|\hat{X}_{i,d} - K_{MOD}X\right|^2 - \min_{X\in\Omega_k^{(0)}} \left|\hat{X}_{i,d} - K_{MOD}X\right|^2, \quad k = \overline{1, \log_2 Q}. \qquad (15)$$

где X – комплексная точка созвездия модуляции; Q – число точек созвездия; $\Omega^{(1)}$ – множество точек созвездия, для которых k-й бит равен 1; $\Omega^{(0)}$ – множество точек созвездия, для которых k-й бит равен 0; K_{MOD} – известный калибровочный коэффициент [8–11].

В случае сверточного кодирования производится деперемежение полученных мягких решений бит в соответствии с правилом стандарта [9–12].

Далее выполняется декодирование (Витерби или LDPC) и дескремблирование полученных оценок бит. По принятым битам данных рассчитываются 32 проверочных бита. Принимается решение о безошибочном приеме пакета при условии, что все расчетные биты совпадают с принятыми проверочными битами пакета. В этом случае из принятого заголовка MAC-уровня определяются идентификаторы отправителя и получателя.

Результаты моделирования

Анализ разработанных алгоритмов одно- и двухканального обнаружения, частотно-временно́й синхронизации и декодирования пакетов сигнала Wi-Fi был выполнен методом статистического компьютерного моделирования. Моделировались пакеты сигнала длиной 1000 байт с BPSK-модуляцией и скоростью сверточного кодирования ½. В качестве канала связи использовалась модель релеевских замираний. Пространственная корреляция задавалась в соответствии с моделью [6–8], приведенной выше. Частотный сдвиг сигнала задавался случайным равномерно распределенным в интервале [−235,2; 235,2] кГц.

На рисунке 4 приведены результаты моделирования алгоритмов обнаружения и частотно-временно́й синхронизации для одно- и для двухканального приема при различных значениях коэффициента корреляции r между каналами.

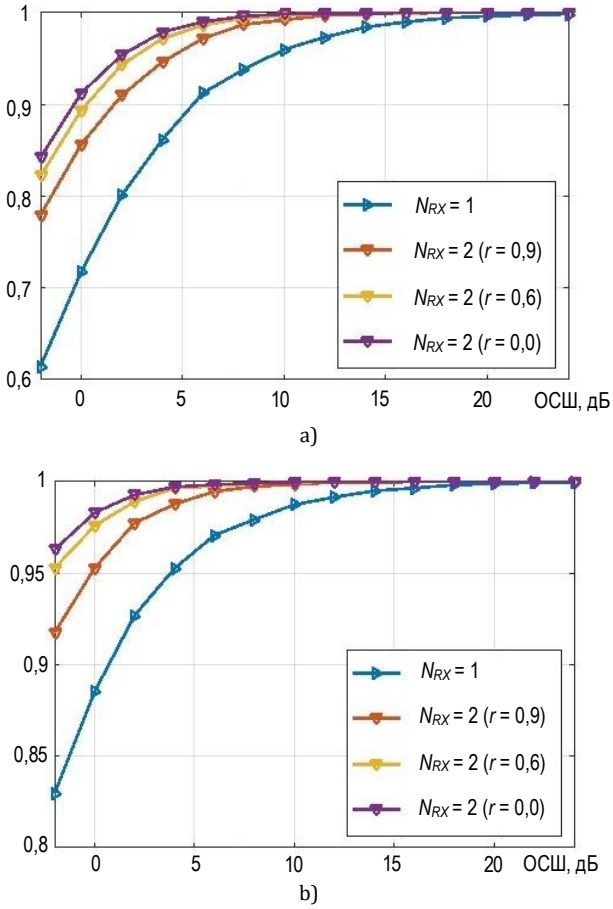


Рис. 4. Зависимость вероятности успешной временно́й (a) и частотной (b) синхронизации от отношения сигнал / шум

Fig. 4. The Probability of Successful Time Synchronization (a) and Frequency (b) vs SNR:

Под успешной временно́й синхронизацией понималось обнаружение преамбулы с погрешностью оценки ее временно́го положения не более половины префикса OFDM-символов. Такая ошибка является некритичной при приеме пакета. Качество выполнения частотной синхронизации характеризуется вероятностью $P(|\sigma| < \eta)$, где $\sigma = \Delta f / f_s$. Величина максимально допустимой ошибки оценки относительной частотной расстройки выбиралась $\eta = 0{,}0006$, что соответствует ± 12 кГц. На рисунках 4–5 значение $N_{RX} = 1$ соответствует одноканальной обработке.

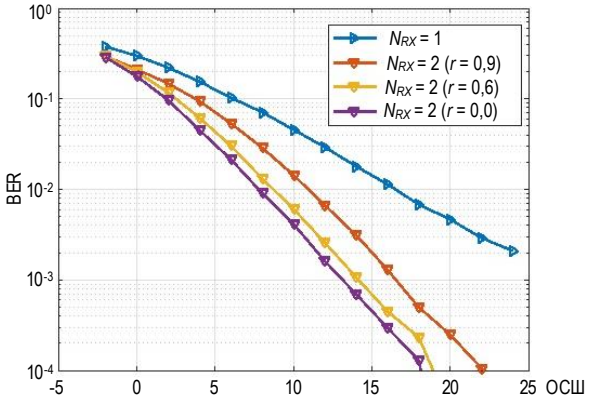


Рис. 5. Зависимость BER от отношения сигнал / шум

Fig. 5. BER vs SNR

В качестве вероятности битовой ошибки (BER, *аббр. от англ.* Bit Error Rate) использовалось среднее значение битовой ошибки, полученное по $5 \cdot 10^3$ испытаниям. При этом в расчете не учитывались пакеты, для которых не была выполнена временна́я синхронизация. Полученная зависимость BER от отношения сигнал / шум представлена на рисунке 5 и иллюстрирует эффективность использования второго канала приема при различной корреляции между каналами.

Выводы

Выполненное исследование приема сигнала Wi-Fi (802.11a/n/ac/ax) в релеевском канале распространения показало, что наличие второго канала приема обеспечивает существенный выигрыш в помехоустойчивости, который увеличивается с уменьшением корреляции сигналов разных каналов.

Использование предложенного алгоритма двухканального обнаружения и синхронизации позволило увеличить помехоустойчивость приблизительно на 4–7 дБ в зависимости от корреляции. Использование второго канала при демодуляции позволяет минимизировать вероятность битовых ошибок. Важно, что при двухканальной обработке даже при близком расположении антенн каналов имеет место существенный выигрыш по сравнению с одноканальной обработкой. Это делает эффективным использование второго канала корреляционно-интерферометрического пеленгатора не только при расчете пеленга, но и при обнаружении и идентификации источников сигнала Wi-Fi.

Предложенные в работе алгоритмы могут быть адаптированы для радиоконтроля сетей новых поколений стандарта Wi-Fi – 802.11be и др. Выполненное исследование разнесенного приема с использованием коммутируемой антенной решетки может быть обобщено и на другие беспроводные технологии, такие как ZigBee, LoRa и др.

Полученные результаты могут быть рекомендованы для повышения помехоустойчивости аппаратуры радиоконтроля беспроводных сетей передачи данных.

Список источников

1. Ашихмин А.В., Козьмин В.А., Мякинин И.С., Радченко Д.С. Спажакин М.И. Адресное пеленгование и определение местоположения источников радиоизлучения ручным пеленгатором // Спецтехника и связь. 2016. № 4. С. 101–105.
2. Алексеев П.А., Козьмин В.А., Крыжко И.Б., Сладких В.А. Определение параметров сетей и точек доступа Wi-Fi // Спецтехника и связь. 2016. № 4. С. 29–36.
3. Фаустов И.С., Сладких В.А., Токарев А.Б., Кощеев Е.В. Обнаружение и анализ сигналов Wi-Fi при адресном пеленговании // Радиотехника. 2023. Т. 87. № 7. С. 89–100. DOI:10.18127/j00338486-202307-10. EDN:HCSNXO
4. Фаустов И.С., Ашихмин А.В., Токарев А.Б. Адресное пеленгование сигналов Wi-Fi // XXIX Международная научно-техническая конференция, посвященная 70-летию кафедры радиофизики ВГУ «Радиолокация, навигация, связь» (Воронеж, Российская Федерация, 18–20 апреля 2023 г.). Воронеж: Воронежский государственный университет, 2023. С. 56–64. EDN:MGRBOI
5. Rembovsky A.M., Ashikhmin A.V., Kozmin V.A., Smolskiy S.M. Radio Monitoring. Automated Systems and Their Components. Springer, 2018. 467 p. DOI:10.1007/978-3-319-74277-9
6. Носов В.И. Методы повышения помехоустойчивости систем радиосвязи с использованием технологии MIMO и пространственно-временной обработки сигнала. Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2014. 316 с. EDN:VRTAXT
7. Панкратов Д.Ю. Анализ влияния пространственно коррелированных замираний на передающей стороне и приемной стороне на пропускную способность радиоканала системы MIMO // T-Comm: Телекоммуникации и транспорт. 2014. Т. 8. № 10. С. 72–74. EDN:SZZOVL
8. Cho Y.S., Yang W.Y., Kim J., Kang C.G. MIMO-OFDM Wireless Communications with MATLAB. John Wiley & Sons, 2010. 439 p. DOI:10.1002/9780470825631. EDN:SRQIDH

9. IEEE Std 802.11a. IEEE Standard for Information technology. Telecommunications and information exchange between systems. Local and metropolitan area networks. Specific requirements. Part 11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High speed Physical Layer in the 5 GHz band. 1999. 82 p. DOI:10.1109/IEEESTD.1999.90606

10. IEEE Std 802.11n. 2009. IEEE Standard for Information technology. Local and metropolitan area networks. Specific requirements. Part 11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput. 502 p. DOI:10.1109/IEEESTD.2009.5307322

11. IEEE Std 802.11ac. IEEE Standard for Information technology. Telecommunications and information exchange between systems. Local and metropolitan area networks. Specific requirements. Part 11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz. 2013. 395 p. DOI:10.1109/IEEESTD.2013.7797535

12. IEEE Std 802.11ax. IEEE Standard for Information Technology. Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks. Specific Requirements. Part 11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN. 2021. 766 p. DOI:10.1109/IEEESTD.2021.9442429

13. Awad M.M., Seddik K.G., Elezabi A. Channel Estimation and Tracking Algorithms for Vehicle to Vehicle Communications // Proceedings of the 82nd Vehicular Technology Conference (VTC2015-Fall, Boston, USA, 06–09 September 2015). IEEE, 2015. DOI:10.1109/VTCFall.2015.7390864

14. Mahmoud H.M., Mousa A.S., Saleem R. Channel Estimation Based in Comb-Type Pilots Arrangement for OFDM System over Time Varying Channel // Journal of Networks. 2010. Vol. 5. Iss. 7. PP. 772–776. DOI:10.4304/jnw.5.7.766-772

15. Kuang L., Ni Z., Lu J., Zheng J. A time-frequency decision-feedback loop for carrier frequency offset tracking in OFDM Systems // IEEE Transactions on Wireless Communications. 2005. Vol. 4. Iss. 2. PP. 367–373. DOI:10.1109/TWC.2004.842955

16. Jimenez V.P.G., Garcia M.J.F.-G., Serrano F.J.G., Armada A.G. Design and implementation of synchronization and AGC for OFDM-based WLAN receivers // IEEE Transactions on Consumer Electronics. 2004. Vol. 50. Iss. 4. PP. 1016–1025. DOI:10.1109/TCE.2004.1362493

17. Wang Q., Xie Q., Wang Z., Chen S., Hanzo L. A Universal Low-Complexity Symbol-to-Bit Soft Demapper // IEEE Transactions on Vehicular Technology. 2014. Vol. 63. Iss. 1. PP. 119–130. DOI:10.1109/TVT.2013.2272640

References

1. Ashihmin A.V., Koz'min V.A., Myakinin I.S., Radchenko D.S. Spazhakin M.I. Address bearing and location determination of radio sources with a manual direction finder. *Spectekhnika i svyaz'*. 2016;(4):101–105. (in Russ.)

2. Alekseev P.A., Kozmin V.A., Kryzhko I.B., Sladkih V.A. Determining the parameters of Wi-Fi networks and access points. *Spectekhnika i svyaz'*. 2016;(4):29–36. (in Russ.)

3. Faustov I.S., Sladkikh V.A., Tokarev A.B., Koshcheev E.V. Detection and analysis of Wi-Fi signals for address direction finding. *Radiotekhnika*. 2023;87(7):89–100. (in Russ.) DOI:10.18127/j00338486-202307-10. EDN:HCSNXO

4. Faustov I.S., Ashihmin A.V., Tokarev A.B. Address direction finding of Wi-Fi signals. *Proceedings of the XXIXth International Scientific and Technical Conference on the 70th Anniversary of the Department of Radiophysics of the Voronezh State University on Raradiolocation, Navigation, Communication, 18–20 April 2023, Voronezh, Russian Federation*. Voronezh: Voronezh State University Publ.; 2023. p.56–64 (in Russ.) EDN:MGRBOI

5. Rembovsky A.M., Ashikhmin A.V., Kozmin V.A., Smolskiy S.M. *Radio Monitoring. Automated Systems and Their Components.* Springer; 2018. 467 p. DOI:10.1007/978-3-319-74277-9

6. Nosov V.I. Methods for increasing the noise immunity of radio communication systems using MIMO technology and spatio-temporal signal processing. Siberian State University of Telecommunications and Informatics Publ.; 2014. 316 p. (in Russ.). EDN:VRTAXT

7. Pankratov D.Yu. Analysis of the capacity of MIMO system radio channel in conditions of spatially correlated fading. *T-Comm*. 2014;8(10):72–74. (in Russ.) EDN:SZZOVL

8. 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

9. IEEE Std 802.11a. *IEEE Standard for Information technology. Telecommunications and information exchange between systems. Local and metropolitan area networks. Specific requirements. Part 11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High speed Physical Layer in the 5 GHz band*. 1999. 82 p. DOI:10.1109/IEEESTD.1999.90606

10. IEEE Std 802.11n. 2009. *IEEE Standard for Information technology. Local and metropolitan area networks. Specific requirements. Part 11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput*. 502 p. DOI:10.1109/IEEESTD.2009.5307322

11. IEEE Std 802.11ac. *IEEE Standard for Information technology. Telecommunications and information exchange between systems. Local and metropolitan area networks. Specific requirements. Part 11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz*. 2013. 395 p. DOI:10.1109/IEEESTD.2013.7797535

12. IEEE Std 802.11ax. *IEEE Standard for Information Technology. Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks. Specific Requirements. Part 11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN*. 2021. 766 p. DOI:10.1109/IEEESTD.

2021.9442429

13. Awad M.M., Seddik K.G., Elezabi A. Channel Estimation and Tracking Algorithms for Vehicle to Vehicle Communications. *Proceedings of the 82nd Vehicular Technology Conference, VTC2015-Fall, 06–09 September 2015, Boston, USA*. IEEE; 2015. DOI:10.1109/VTCFall.2015.7390864

14. Mahmoud H.M., Mousa A.S., Saleem R. Channel Estimation Based in Comb-Type Pilots Arrangement for OFDM System over Time Varying Channel. *Journal of Networks*. 2010;5(7):772–776. DOI:10.4304/jnw.5.7.766-772

15. Kuang L., Ni Z., Lu J., Zheng J. A time-frequency decision-feedback loop for carrier frequency offset tracking in OFDM Systems. *IEEE Transactions on Wireless Communications.* 2005;4(2):367–373. DOI:10.1109/TWC.2004.842955

16. Jimenez V.P.G., Garcia M.J.F.-G., Serrano F.J.G., Armada A.G. Design and implementation of synchronization and AGC for OFDM-based WLAN receivers. *IEEE Transactions on Consumer Electronics*. 2004;50(4):1016–1025. DOI:10.1109/TCE.2004.1362493

17. Wang Q., Xie Q., Wang Z., Chen S., Hanzo L. A Universal Low-Complexity Symbol-to-Bit Soft Demapper. *IEEE Transactions on Vehicular Technology*. 2014;63(1):119–130. DOI:10.1109/TVT.2013.2272640

Статья поступила в редакцию 16.07.2024; одобрена после рецензирования 12.12.2024; принята к публикации 09.01.2025.
The article was submitted 16.07.2024; approved after reviewing 12.12.2024; accepted for publication 09.01.2025.

Информация об авторах:

ФАУСТОВ Иван Сергеевич
аспирант кафедры радиотехники Воронежского государственного технического университета, научный сотрудник научно-исследовательского сектора АО «ИРКОС»
https://orcid.org/0009-0005-3054-5540

МАНЕЛИС Владимир Борисович
доктор технических наук, доцент, ведущий научный сотрудник научно-исследовательского сектора АО «ИРКОС»
https://orcid.org/0009-0008-7077-3611

КОЗЬМИН Владимир Алексеевич
кандидат технических наук, доцент, директор по научной работе АО «ИРКОС»
https://orcid.org/0000-0002-5268-1114

ТОКАРЕВ Антон Борисович
доктор технических наук, доцент, профессор кафедры радиотехники Воронежского государственного технического университета, старший научный сотрудник научно-исследовательского сектора АО «ИРКОС»
https://orcid.org/0000-0002-2621-4336

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-2025-11-1-62-68
EDN:RVENVC

Оптимизация использования ресурсов воздушных базовых станций на основе методов искусственного интеллекта

Тунг Зыонг Чан✉, chan.tz@sut.ru
Андрей Евгеньевич Кучерявый, akouch@sut.ru

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

Аннотация

В отдаленных областях и районах стихийных бедствий беспилотные летательные аппараты (БПЛА) могут выступать в качестве базовых станций, обеспечивающих беспроводную связь с наземными пользователями. Благодаря своей высокой мобильности, низкой стоимости, а также быстрому развертыванию и поиску, БПЛА могут изменять свое местоположение в трехмерном пространстве, улучшая беспроводное соединение и повышая скорость передачи данных. В этой статье исследуются проблемы развертывания воздушных базовых станций (ABS, аббр. от англ. Aerial Base Station) в трехмерном пространстве и распределения мощности в целях максимизации скорости передачи данных в системе. Для решения этих проблем предложено использовать алгоритм Q-learning, относящийся к методам обучения с подкреплением. Используя БПЛА в качестве агента, алгоритм позволяет ABS исследовать пространство состояний на основе политики ϵ-greedy (эпсилон жадный алгоритм) для определения местоположения в трехмерном пространстве и распределения мощности. Результаты моделирования показывают, что предложенный алгоритм превосходит известные методы размещения ABS в трехмерном пространстве и распределения мощности. ***Целью*** *настоящей статьи является исследование эффективности применения современных методов искусственного интеллекта для оптимизации использования ресурсов воздушных базовых станций сетей связи общего пользования.*

Сущность *предлагаемого решения состоит в применении современных методов искусственного интеллекта, а именно: метода обучения Q-learning и эпсилон-жадного алгоритма ϵ-greedy для обеспечения совместной оптимизации размещения ABS и распределения мощности для максимизации скорости передачи данных. Система* ***имеет реализацию*** *в виде программы моделирования.* ***Эксперименты*** *при моделировании показали, что использование метода обучения с подкреплением Q-learning и эпсилон-жадного алгоритма e-greedy для совместной оптимизации обеспечивает более высокую общую скорость передачи данных в системе по сравнению с оптимизацией только местоположения или распределения мощности.*

Научная новизна *предложенного решения состоит в том, что совместная оптимизация размещения ABS и распределения мощности позволила, в отличие от известных результатов, выявить, что высота полета БПЛА с установленной на нем базовой станцией при оптимизации только местоположения будет выше, чем высота полета БПЛА при совместной оптимизации местоположения и распределения мощности.*

Практическая значимость *заключается в возможности разработки методики планирования сетей связи общего пользования при использовании ABS для получения более высокой общей скорости передачи данных на соответствующем фрагменте сети.*

Ключевые слова: *воздушная базовая станция, трехмерное местоположение, распределение мощности, скорость передачи данных, Q-learning*

Ссылка для цитирования: Чан Т.З., Кучерявый А.Е. Оптимизация использования ресурсов воздушных базовых станций на основе методов искусственного интеллекта // Труды учебных заведений связи. 2025. Т. 11. № 1. С. 62–68. DOI:10.31854/1813-324X-2025-11-1-62-68. EDN:RVENVC

Original research
https://doi.org/10.31854/1813-324X-2025-11-1-62-68
EDN:RVENVC

Resource Optimization of Airborne Base Stations Using Artificial Intelligence Methods

Tung D. Tran ✉, chan.tz@sut.ru
Andrey E. Koucheryavy, akouch@sut.ru

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

Annotation

In remote areas and disaster-stricken regions, unmanned aerial vehicles (UAVs) can serve as base stations, providing wireless communication to ground users. Due to their high mobility, low cost, and rapid deployment and retrieval capabilities, UAVs can continuously adjust their position in three-dimensional (3D) space, improving wireless connectivity and enhancing data transmission rates. In this paper, we investigate the problem of ABS (Aerial Base Station) deployment in 3D space and power allocation with the aim of maximizing the data transmission rate in the system. To address this non-convex problem, we propose Q-learning, a reinforcement learning algorithm. By using the ABS as an agent, the algorithm enables the ABS to explore the state space and take actions based on an ϵ-greedy policy (optimal epsilon value) to determine its 3D position and power allocation. Simulation results demonstrate that the proposed algorithm outperforms individual position optimization and power allocation optimization.

The purpose *of this article is to study the efficiency of using modern artificial intelligence methods to optimize the use of resources of airborne base stations of public communication networks.*

The essence of the proposed solution *is to use modern artificial intelligence methods, namely: the Q-learning method and the epsilon-greedy ϵ-greedy algorithm to ensure joint optimization of the placement of airborne base stations and power distribution to maximize the data transfer rate.* ***The system has an implementation*** *in the form of a simulation program.* ***Simulation experiments*** *have shown that the use of the Q-learning reinforcement learning method and the epsilon-greedy e-greedy algorithm for joint optimization provides a higher overall data transfer rate in the system compared to optimizing only the location or power distribution.*

The scientific novelty *of the proposed solution is that joint optimization of the placement of an airborne base station and power distribution made it possible, in contrast to known results, to establish that the flight altitude of a UAV with a base station installed on it when optimizing only the location will be higher than the flight altitude of a UAV when jointly optimizing the location and power distribution.*

The practical significance *is the possibility of developing a methodology for planning public communication networks using airborne base stations to obtain a higher overall data transfer rate on the corresponding network fragment.*

Keywords: *ABS, 3D positioning, power allocation, data transmission rate, Q-learning*

For citation: Tran T.D., Koucheryavy A.E. Resource Optimization of Airborne Base Stations Using Artificial Intelligence Methods. *Proceedings of Telecommunication Universities.* 2025;11(1):62–68. (in Russ.) DOI:10.31854/1813-324X-2025-11-1-62-68. EDN:RVENVC

1. Введение

Интернет вещей, являясь одной из определяющих концепций для сетей связи пятого поколения, позволяет осуществлять взаимодействие между устройствами Интернета вещей, такими как сенсоры, носимые устройства и смартфоны [1]. Однако появление большого числа услуг Интернета вещей создает серьезные проблемы для существующих наземных сетей. Если говорить более конкретно, число устройств Интернета вещей может достичь 100 миллиардов к 2025 г. [2], тем самым создается огромное количество источников данных, которые еще больше усложняют работу текущей наземной сети. Из-за жесткой структуры наземной сети, в основе которой, как правило, используются стационарные базовые станции и которые могут с большой вероятностью быть повреждены в случае природных катастроф, системе Интернета вещей до-

статочно сложно обеспечить покрытие и сбор данных в реальном времени от устройств в зонах бедствий и отдаленных районах. Летающие базовые станции являются одним из перспективных решений для преодоления перегрузки сетевого трафика, обеспечивающих быстрый и экономически эффективный способ поддержки потребностей в беспроводных соединениях в таких условиях [3].

Беспилотные летательные аппараты (БПЛА) играют незаменимую роль в сетях связи пятого и последующих поколений. Благодаря простоте развертывания, беспроводные сети с поддержкой БПЛА могут быть достаточно легко построены, переконфигурированы и повторно использованы по назначению в зависимости от их предназначения. Применение БПЛА возможно во многих областях, например, в таких как мониторинг, наблюдение и доставка грузов [4]. По сравнению с традиционными наземными сетями БПЛА развертываются в воздухе, что обеспечивает более высокую вероятность соединений в зоне прямой видимости (LoS, *от англ.* Line of Sight) для канала «воздух – земля». Кроме того, мобильность позволяет БПЛА легко перемещаться с места на место во время сбора данных в удаленных районах, где нет наземной сетевой системы. Они также могут выступать в качестве трехмерных (3D) базовых станций для поддержки наземного пользовательского оборудования, а также для расширения зоны действия связи в труднодоступных районах или зонах стихийных бедствий.

Использование вышеупомянутых преимуществ сетей с поддержкой БПЛА требует решения многих технических проблем с точки зрения проектирования распределения ресурсов, а также – проблем, связанных с полезной нагрузкой, временем полета и зарядкой аккумулятора. В этой статье исследуется нисходящий канал связи пользователей, обслуживаемых воздушной базовой станцией (ABS, *аббр от англ.* Aerial Base Station). Цель исследования состоит в том, чтобы максимизировать общую пропускную способность системы за счет оптимизации местоположения ABS в 3D-пространстве, а также – управления мощностью передачи для каждого пользователя. Для решения этой задачи в статье предложено использование обучения с подкреплением на основе метода *Q*-learning. Поскольку оказание услуг абонентам сетей связи общего пользования осуществляется базовой станцией, расположенной на борту БПЛА во время его нахождения в стационарном состоянии, исследование характеристик собственно БПЛА в статье не требуется.

2. Модель системы и постановка задачи

Будем рассматривать нисходящую линию связи единой беспроводной сети с поддержкой ABS, состоящей из N наземных пользователей. Все наземные пользователи являются стационарными, что обозначается множеством $TV = (1, 2, \bullet\bullet\bullet, \ldots, N)$. БПЛА развернут для зависания в определенном месте в этой области, чтобы предоставлять пользователям услуги беспроводной связи по нисходящей линии связи. Местоположение ABS в 3D-пространстве обозначается через (x_a, y_a, h_a), где (x_a, y_a) – горизонтальная координата местоположения ABS, а h_a – высота ABS. Местоположение пользователя n обозначается через $(x_n, y_n, 0)$. Предполагается, что ABS обладает полной информацией о местоположении пользователя перед развертыванием. Кроме того, для предотвращения беспроводных помех применяется множественный доступ с частотным разделением, а полоса пропускания системы, обозначаемая как B, равномерно распределяется среди всех пользователей.

Канал связи ABS с землей можно описать как вероятностную модель, которая состоит из соединений в условиях LoS и непрямой видимости (NLoS, *от англ.* Non-Line of Sight).

Вероятность потери связи между ABS и пользователем k определяется следующим образом:

$$P_n^{LoS} = \frac{1}{1 + a\exp(-b[\frac{180}{\pi}\arcsin(\frac{h_a}{d_{a,n}}) - a])}, \qquad (1)$$

где a и b – параметры среды распространения; $\arcsin(\frac{h_a}{d_{a,n}})$ – угол между ABS и пользователем n; $d_{a,n}$ – 3D-расстояние от ABS до пользователя n.

Тогда вероятность соединения в условиях NLoS будет равна $P^{LoS} = 1 - P^{NLoS}$. Без потери общности, обозначим путь ABS между собой и пользователем n как $\eta_{a,n}^{LoS} = \beta_0 d_{a,n}^{-\hat{\alpha}}$ и $\eta_{a,n}^{NLoS} = \chi\beta_0 d_{a,n}^{-\hat{\alpha}}$ для LoS- и NLoS-подключения, соответственно, где β_0 – потери распространения на эталонном расстоянии 1 м для соединений в условиях LoS; $0 < \chi < 1$ – дополнительно необходимая средняя дальность распространения для соединений в условиях NLoS; $\hat{\alpha}$ – показатель потерь распространения.

Предположим, что коэффициент усиления канала между ABS и пользователем n составляет h_n, где h – случайная величина с двумя разными уровнями случайности, т. е. случайным возникновением связи в условиях LoS и NLoS и случайным замиранием.

Чтобы упростить задачу, среднее усиление мощности канала можно определить, как:

$$h_n = P_n^{LoS}\beta_0 d_{a,n}^{-\hat{\alpha}} + P_n^{NLoS}\chi\beta_0 d_{a,n}^{-\hat{\alpha}} = \overline{P_n^{LoS}}\beta_0 d_{a,n}^{-\hat{\alpha}}, \qquad (2)$$

где $\overline{P_n^{LoS}} = P_n^{LoS} + (1 - P_n^{LoS})\chi$.

Будем предполагать, что общая мощность передачи ABS равна P_a. Пусть p_n представляет собой коэффициент распределения мощности для пользователя n, σ^2 – мощность аддитивного белого гауссовского шума.

Тогда отношение сигнал / шум у пользователя n определяется как:

$$\gamma_n = \frac{P_a p_n h_n}{\sigma^2}. \quad (3)$$

Предполагая, что B обозначает общую полосу пропускания канала, доступную для ABS, достижимая скорость нисходящей линии связи от ABS к пользователю n может быть рассчитана на основе формулы Шеннона [5]:

$$R_n = \frac{B}{N}\log_2(1+\gamma_n) = \frac{B}{N}\log_2(1+\frac{P_a p_n h_n}{\sigma^2}). \quad (4)$$

Как уже отмечалось выше, цель данной работы состоит в максимизации суммарной скорости передачи данных при ограничениях на местоположение ABS в 3D-пространстве и распределения мощности для каждого пользователя. Задача может быть сформулирована следующим образом:

$$(P) \quad \max_{\{x_a, y_a, h_a, p_n\}} D = \sum_{n=1}^{N} R_n,$$
$$C1: \sum_{n=1}^{N} p_n = 1, \quad (5)$$
$$C2: p_n > 0,\ \forall n \in N,$$
$$C3: \gamma_n \geq \gamma_0,\ \forall n \in N,$$
$$C4: x_a, y_a, h_a \in S.$$

Ограничение $C1$ означает, что общая сумма коэффициентов распределения мощности для всех пользователей в системе должна равняться 1; ограничение $C2$ представляет собой коэффициент распределения мощности для каждого пользователя; ограничение $C3$ указывает, что отношение сигнал / шум у пользователя n должно быть больше или равно пороговому значению γ_0, тогда считается, что пользователь n подключен к ABS; ограничение $C4$ требует, чтобы ABS была размещена в заданном пространстве.

3. 3D-определение местоположения и распределения мощности ABS на основе *Q*-learning

В целом проблема оптимизации P является чрезвычайно сложной для решения из-за отсутствия выпуклости ограничений на переменные положения ABS и передающей мощности. Кроме того, число переменных увеличивается вместе с ростом количества пользователей. Поэтому проблема P является невыпуклой, найти оптимальное решение довольно затруднительно. Далее предложена методика решения проблемы P, основанная на методе искусственного интеллекта Q-learning. Будет рассмотрена связь Q-learning с обучением с подкреплением (RL, *аббр. от англ.* Reinforcement Learning).

В алгоритме Q-learning ABS выступает в роли агента, а сам алгоритм состоит из четырех частей: состояния, действий, вознаграждений и Q-значений. Основная цель Q-learning – получение политики, которая максимизирует наблюдаемый результат в процессе взаимодействия агентов. На каждом временно́м шаге итерации агенты наблюдают состояние из пространства состояний S. Соответственно, они выбирают действие из пространства действий A на основе политики J. Принцип политики на каждом временно́м шаге заключается в выборе действия, которое приводит модель к максимальному Q-значению. После выполнения действия состояние каждого агента переходит в новое состояние, и агент получает необходимый результат.

Состояния (S). Эти состояния представляют ситуацию среды системы ретрансляции на базе ABS, и принятие решения о действиях основывается на состоянии сети. В данной работе основными факторами, влияющими на состояние сетевой среды, являются положение ABS в 3D-пространстве и мощность передачи для разных пользователей в сети. Затем предоставляется обратная связь для корректировки основных факторов с целью улучшения производительности сети.

Обозначаем s_t как состояние ABS на временно́м слоте t, и оно может быть определено как:

$$s_t = \{x_a^t, y_a^t, h_a^t, p_1^t, p_2^t, \ldots, p_n^t\}, \quad (6)$$

где $n \in N$, (x_a^t, y_a^t, h_a^t) – местоположение ABS на временно́м шаге t; p_n^t – мощность, выделенная для пользователя n.

Действие (A). На каждом шаге обозначим a_t как действие ABS на временно́м слоте t. ABS принимает решения на основе состояния сети, что вызывает переход сети в новое состояние. Действие состоит из двух частей: одна часть – это перемещение в следующее состояние ABS, другая – распределение мощности. Перемещение ABS включает движение вперед, назад, вправо, влево, вверх и вниз. Распределение мощности для каждого пользователя может увеличиваться или уменьшаться.

Вознаграждение (R). Целью Q-learning является максимизация накопленного ожидаемого результата. Чтобы достичь цели, поставленной в уравнении (5), необходимо включить общую системную скорость передачи данных в функцию вознаграждения. На каждом временно́м шаге t общая скорость передачи данных для пользователя D_t может быть рассчитана на основе местоположения ABS. ABS будет регулировать свое местоположение и распределение мощности таким образом, чтобы поддерживать оптимальное состояние.

Таким образом, можно выразить функцию вознаграждения во временно́м интервале t как:

$$r_t = D_t - \lambda(N - N_u), \quad (7)$$

где N – общее число пользователей в рассматриваемой области; N_u – число пользователей, обслуживаемых ABS, статус пользователя может быть основан на формуле (3); λ – штрафной коэффициент.

Политика (P). Политика – это механизм выбора действий, используемый для определения тех действий, которые агент будет выполнять во время обучения. Ее главная цель – установить баланс между исследованием и эксплуатацией таким образом, чтобы агент мог подкрепить те суждения, которые он уже знает как хорошие, но также исследовать возможные новые действия [6]. В данной работе далее будем рассматривать наиболее известную политику ϵ-greedy (эпсилон-жадный алгоритм), в которой агент выбирает случайное действие с вероятностью ε и лучшее действие, соответствующее наилучшему Q-значения в данный момент, с вероятностью 1-ε.

Таким образом, вероятность выбора действия a_t в состоянии s_t на временно́м слоте t задается следующей формулой:

$$\pi_m(s_m, \theta_m) = \begin{cases} 1-\epsilon, \text{если } Q_m(\theta) \text{ наибольшее} \\ \epsilon, \text{в противном случае} \end{cases}, \quad (8)$$

где $\epsilon \in (0,1)$.

Чтобы обеспечить сходимость Q-learning, скорость обучения α_t является функцией временно́го шага [7], который задается формулой:

$$\alpha_t = \frac{1}{(t + c_\alpha)^{\phi_\alpha}}, \quad (9)$$

где $c_\alpha > 0, \phi \in (\frac{1}{2}, 1]$.

Во время обучения функция значения состояния-действия для агента может итеративно обновляться следующим образом:

$$Q_{t+1}(s_t, a_t) \leftarrow (1-\alpha_t) \cdot Q_t(s_t, a_t) + \\ + \alpha_t \cdot [r_t + \beta . \max Q_t(s_{t+1}, a_t)], \quad (10)$$

где β – коэффициент дисконтирования.

В Q-learning параметр ϵ со временем уменьшается, чтобы обеспечить баланс между исследованием и эксплуатацией. В начале обучения высокое значение ϵ помогает агенту выбирать случайные действия для исследования окружающей среды и построения точной таблицы значений Q-learning. Однако, если ϵ останется высоким, агент всегда будет выбирать случайные действия, не используя полученные знания, что приведет к отсутствию сходимости процесса обучения. Напротив, если ϵ постепенно уменьшается, агент начнет отдавать предпочтение действиям с наивысшими значениями, согласно таблице значений Q-learning, тем самым оптимизируя политику действий. Это помогает агенту освоить лучшую стратегию после достаточного изучения пространства состояний, обеспечивая высокую производительность в долгосрочной перспективе.

Таким образом, в данной работе ϵ регулируется после каждого эпизода, в соответствии с формулой:

$$\epsilon_{p+1} = \epsilon_p \epsilon_o, \quad (11)$$

где ϵ_o – постоянное значение, на которое ϵ уменьшается после каждого эпизода; ϵ_p и ϵ_{p+1} – значение ϵ в эпизоде p и (p + 1).

4. Результаты моделирования

Рассмотрим случай для N = 5 пользователей, равномерно распределенных на площади 300 м × 300 м. Горизонтальное положение ABS ограничено в пределах рассматриваемой области, а высота ABS фиксирована и составляет h_a = 50 м. Другие параметры моделирования приведены в таблице 1.

ТАБЛИЦА 1. Параметры моделирования

TABLE 1. Simulation Parameters

Параметр	Значение	Параметр	Значение
P_a	100 мВт	B	5 МГц
a	9,16	b	0,16
σ^2	–110 дБм	β_0	–40 дБ
γ_o	5 дБ	$\hat{\alpha}$	–2,3
χ	0,1	–	–

Параметры для предложенного Q-learning следующие: β = 0,99; c_α = 0,5; ϕ_α = 0,7; ϵ = 1; ϵ_o = 0,999; штрафной коэффициент λ = 20. Число эпизодов обучения составляет 250 с шагом по времени T = 500.

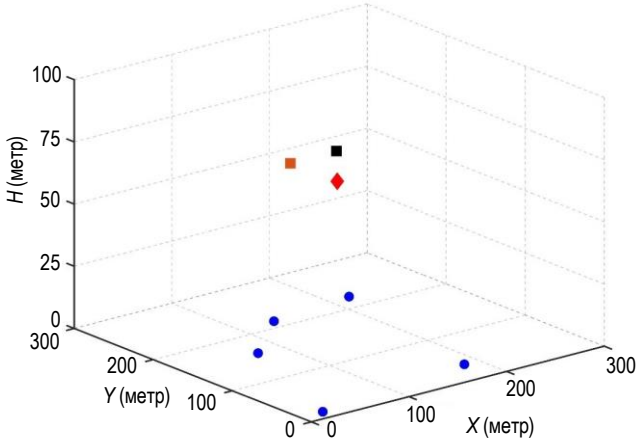


Рис. 1. 3D-положение ABS и пользователей

Fig. 1. 3D-Location of Aerial Base Station (ABS) and Users

На рисунке 1 показано 3D-расположение ABS в различных случаях. Красный ромб отображает позицию ABS при оптимизации местоположения и распределения мощности. Эта точка имеет координаты (140, 140,5, 65). Оранжевый квадрат представляет положение ABS при использовании оптимальной позиции, равномерно распределяющей мощность между пользователями. Эта точка имеет координаты (149, 151, 74). Черные квадраты представляют любое положение ABS и отображают распре-

деление мощности между пользователями. Как видим, высота ABS при оптимизации только местоположения будет выше, чем высота полета ABS при оптимизации местоположения и распределения мощности. Это связано с тем, что при одинаковом уровне распределения мощности среди пользователей ABS будет находиться выше, чтобы уменьшить связь в условиях NLoS в канале «воздух – земля» для удаленных пользователей. Между тем, в случае, когда энергия может быть распределена между пользователями, при наличии удаленных пользователей ABS могут увеличить распределение энергии по сравнению с близлежащими пользователями.

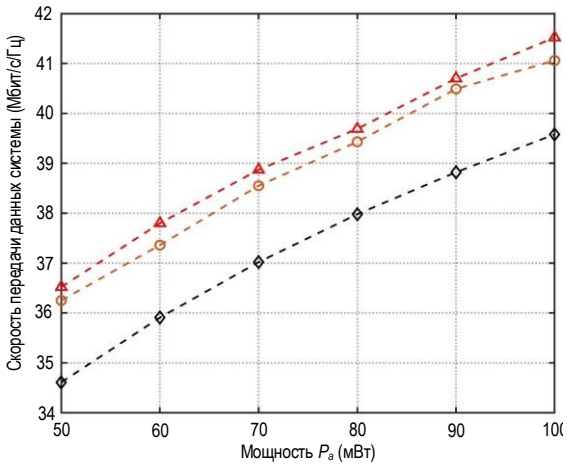


Рис. 2. Скорости передачи данных системы с различной мощностью передачи ABS

Fig. 2. Data Transmission Rate of the System with Different ABS Transmission Power

Скорость передачи данных системы при различной мощности передачи ABS показана на рисунке 2 в зависимости от положения ABS (см. рисунок 1). Как видим, что при оптимизации положения ABS производительность будет выше, чем при случайном формировании положения ABS. При этом скорость передачи данных системы при оптимизации положения ABS имеет примерно такое же значение, как скорость передачи данных системы при оптимизации положения и распределения энергии. Из этого следует, что местоположение играет важную роль в увеличении показателя скорости.

На рисунке 3 показана средняя суммарная скорость передачи данных системы при различном количестве и распределении пользователей. В целом, с ростом их количества уменьшается средняя суммарная скорость передачи данных в системе. Это можно объяснить тем, что по мере увеличения количества пользователей потери при передаче данных будут возрастать вследствие большего количества подключений пользователей к ABS.

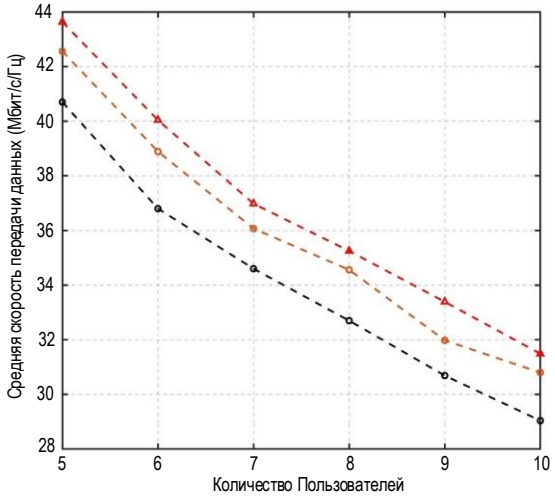


Рис. 3. Средняя суммарная скорость передачи данных системы при различном числе и местоположении наземных пользователей

Fig. 3. Average Data Transmission Rate of the System with Different Number and Locations of Ground Users

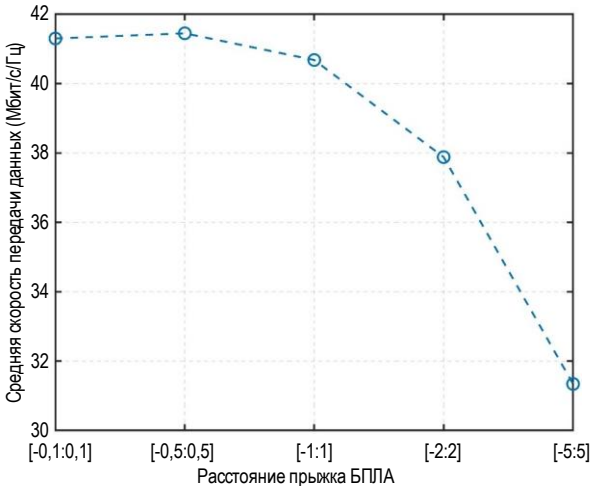


Рис. 4. Скорость передачи данных системы при различных расстояниях перелета ABS

Fig. 4. Data Transfer Rate of the System at Different ABS Flight Distances

Средняя скорость передачи данных внешней системы зависит от расстояния после каждого временно́го шага ABS. Более конкретно [–1:1] означает, что БПЛА может изменять положение максимум на 1 м в каждом направлении в 3D-пространстве. Как показано на рисунке 4, при увеличении расстояния перехода средняя скорость передачи данных системы вначале остается неизменной, а затем резко снижается. Это связано с тем, что при большом расстоянии перелета ABS может легко пропустить глобальную оптимальную точку и вернуться обратно будет очень сложно.

5. Выводы

Во-первых, в статье исследуются проблемы совместной оптимизации размещения ABS и распределения мощности для максимизации скорости передачи данных в системе. В интересах решения

этой проблемы предложено использовать метод обучения с подкреплением *Q*-learning и эпсилон-жадный алгоритм ϵ-greedy.

Во-вторых, совместная оптимизация размещения БПЛА и распределения мощности позволила, в отличие от известных результатов, установить, что высота ABS при оптимизации только местоположения будет выше, чем высота ABS при совместной оптимизации местоположения и распределения мощности.

В-третьих, результаты моделирования показали также, что использование метода обучения с подкреплением *Q*-learning и эпсилон-жадного алгоритма ϵ-greedy для совместной оптимизации обеспечивает более высокую общую скорость передачи данных в системе по сравнению с оптимизацией только местоположения или распределения мощности.

Список источников

1. Ding G., Wu Q., Zhang L., Lin Y., Tsiftsis T.A., Yao Y.D. An amateur drone surveillance system based on the cognitive Internet of Things // IEEE Communications Magazine. 2018. Vol. 56. Iss. 1. PP. 29–35. DOI:10.1109/MCOM.2017.1700452. EDN:YBEOMH
2. Rose K., Eldridge S., Chapin L. The internet of things: An overview // The internet society (ISOC). 2015. Vol. 80(15). PP. 1–53.
3. Zhao N., Lu W., Sheng M., Chen Y., Tang J., Yu F.R., et al. UAV-Assisted Emergency Networks in Disasters // IEEE Wireless Communications. 2019. Vol. 26. Iss. 1. PP. 45–51. DOI:10.1109/MWC.2018.1800160
4. Li B., Fei Z., Zhang Y. UAV communications for 5G and beyond: Recent advances and future trends // IEEE Internet of Things Journal. 2018. Vol. 6. Iss. 2. PP. 2241–2263. DOI:10.1109/JIOT.2018.2887086. EDN:UPZMGQ
5. Shannon C.E. A mathematical theory of communication // The Bell System Technical Journal. 1948. Vol. 27. Iss. 3. PP. 379–423. DOI:10.1002/j.1538-7305.1948.tb01338.x
6. Sutton R.S. Reinforcement learning: An introduction. The MIT Press, 2018.
7. Jaakkola T., Jordan M., Singh S. Convergence of Stochastic Iterative Dynamic Programming Algorithms // Advances in Neural Information Processing Systems 6 (NIPS 1993). 1993.

References

1. Ding G., Wu Q., Zhang L., Lin Y., Tsiftsis T.A., Yao Y.D. An amateur drone surveillance system based on the cognitive Internet of Things. *IEEE Communications Magazine*. 2018;56(1):29–35. DOI:10.1109/MCOM.2017.1700452. EDN:YBEOMH
2. Rose K., Eldridge S., Chapin L. The internet of things: An overview. *The internet society (ISOC)*. 2015;80(15):1–53.
3. Zhao N., Lu W., Sheng M., Chen Y., Tang J., Yu F.R., et al. UAV-Assisted Emergency Networks in Disasters. *IEEE Wireless Communications*. 2019;26(1):45–51. DOI:10.1109/MWC.2018.1800160
4. Li B., Fei Z., Zhang Y. UAV communications for 5G and beyond: Recent advances and future trends. *IEEE Internet of Things Journal*. 2018;6(2):2241–2263. DOI:10.1109/JIOT.2018.2887086. EDN:UPZMGQ
5. Shannon C.E. A mathematical theory of communication. *The Bell System Technical Journal*. 1948;27(3):379–423. DOI:10.1002/j.1538-7305.1948.tb01338.x
6. Sutton R.S. *Reinforcement learning: An introduction.* The MIT Press; 2018.
7. Jaakkola T., Jordan M., Singh S. Convergence of Stochastic Iterative Dynamic Programming Algorithms. *Advances in Neural Information Processing Systems 6 (NIPS 1993)*. 1993.

Статья поступила в редакцию 13.01.2025; одобрена после рецензирования 15.02.2025; принята к публикации 21.02.2025.
The article was submitted 13.01.2025; approved after reviewing 15.02.2025; accepted for publication 21.02.2025.

Информация об авторах:

ЧАН Тунг Зыонг
аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
https://orcid.org/0009-0006-0080-9477

КУЧЕРЯВЫЙ Андрей Евгеньевич
доктор технических наук, профессор, заведующий кафедрой сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
https://orcid.org/0000-0003-4479-2479

Кучерявый А.Е. 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.
Koucheryavy A.E. 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.


ИНФОРМАЦИОННЫЕ
ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
2.3.1 – Системный анализ, управление и обработка информации, статистика
2.3.6 – Методы и системы защиты информации, информационная безопасность

Научная статья
УДК 004.056.5
https://doi.org/10.31854/1813-324X-2025-11-1-70-83
EDN:QOBBRA

Метод моделирования коммуникационной инфраструктуры на основе средств имитационного и полунатурного моделирования

Дмитрий Александрович Васинев, vda33@academ.msk.rsnet.ru

Академия Федеральной службы охраны Российской Федерации,
Орел, 302015, Российская Федерация

Аннотация

Актуальность исследования *объясняется сложившимся противоречием предметной области, которое заключается в динамически меняющейся в процессе функционирования коммуникационной инфраструктуре объекта критической информационной инфраструктуры (КИИ), а также методах воздействия нарушителя на объект КИИ, создающих предпосылки для снижения уровня информационной безопасности, и возможностями существующих методов оценки защищенности объекта на основе сигнатур, экспертного подхода, а также методов и средств обеспечения информационной безопасности, не позволяющих учитывать такую динамику изменения уровня информационной безопасности объекта.*

Цель исследования: *обеспечение информационной безопасности коммуникационной инфраструктуры объектов КИИ за счет учета коммуникационных и конфигурационных параметров, динамики взаимодействующих субъектов.*

Методы исследования: *математические методы теории систем и системного анализа, теории вероятностей, методы теории графов, методы имитационного моделирования.*

Результаты. *В статье представлен метод моделирования коммуникационной инфраструктуры, который позволяет формировать параметрически точные имитационные модели объекта КИИ для исследования свойств защищенности и устойчивости, моделировать воздействия нарушителя на объект КИИ.*

Новизна. *Разработан метод моделирования коммуникационной инфраструктуры на основе конфигурационных и коммуникационных параметров объекта КИИ, учитывающий динамику взаимодействия коммуникационной инфраструктуры, политики его информационной безопасности и действия нарушителя.*

Теоретическая значимость. *Развитие методов информационной безопасности в области моделирования коммуникационной инфраструктуры объектов КИИ на основе гиперграфов, вложенных раскрашенных сетей Петри, позволяющих учитывать динамику взаимодействующих субъектов (коммуникационную и конфигурационную инфраструктуру, политику информационной безопасности, воздействие нарушителя).*

Практическая значимость. *Метод моделирования позволяет учитывать конфигурационные и коммуникационные особенности построения и функционирования объекта КИИ, параметры воздействия нарушителя на объект КИИ, существующую политику безопасности, моделировать свойство устойчивости, проводить исследование влияния взаимодействующих субъектов на защищенность объекта КИИ, уменьшить зависимость от экспертных оценок, получать параметрически обоснованные оценки защищенности коммуникационной инфраструктуры объекта КИИ.*

Ключевые слова: *критическая информационная инфраструктура, коммуникационная инфраструктура, конфигурационная инфраструктура, метод моделирования, метод оценки защищенности, киберустойчивость, протокольные блоки данных*

Ссылка для цитирования: Васинев Д.А. Метод моделирования коммуникационной инфраструктуры на основе средств имитационного и полунатурного моделирования // Труды учебных заведений связи. 2025. Т. 11. № 1. С. 70–83. DOI:10.31854/1813-324X-2025-11-1-70-83. EDN:QOBBRA

Original research
https://doi.org/10.31854/1813-324X-2025-11-1-70-83
EDN:QOBBRA

Method of Communication Infrastructure Modeling Based on Simulation and Semi-Natural Modeling

Dmitry A. Vasinev, vda33@academ.msk.rsnet.ru

Academy of the Russian Federal Guard Service,
Orel, 302015, Russian Federation

Annotation

The relevance *of the research is explained by the existing contradiction of the subject area, which consists in the communication infrastructure of the critical information infrastructure (CII) object dynamically changing in the process of functioning, as well as the methods of the intruder's impact on the CII object, as well as the methods of the intruder's impact on the CII object, which create preconditions for reducing the level of information security and the capabilities of the existing methods of assessing the object's security based on signatures, expert approach, as well as methods and means of ensuring information security, which do not allow taking into account such dynamics of changes in the level of information security of the object.*

Purpose of the research. *Provision of information security of communication infrastructure of CII objects by taking into account communication and configuration parameters, dynamics of interacting subjects.*

Research methods. *Mathematical methods of systems theory and system analysis of probability theory, methods of graph theory, methods of simulation modeling.*

Results. *The article presents a method of modeling of communication infrastructure that allows to form parametric accurate simulation models of the CII object to study the properties of security and stability, to simulate the impact of an intruder on the CII object.*

Novelty*. A method of modeling the communication infrastructure based on configuration and communication parameters of the CII object has been developed, taking into account the dynamics of communication infrastructure interaction, its information security policy and intruder actions.*

Theoretical significance. *Development of information security methods in the field of modeling the communication infrastructure of CII objects on the basis of hypergraphs, nested colored Petri nets, allowing to take into account the dynamics of interacting subjects (communication and configuration infrastructure, information security policy, the impact of the intruder).*

Practical significance. *The modeling method allows to take into account configuration and communication peculiarities of construction and functioning of the CII object, parameters of the intruder's impact on the CII object, the existing security policy, to model the stability property, to conduct research of the influence of interacting subjects on the security of the CII object, to reduce the dependence on expert assessments, to receive parametrically justified assessments of the security of the communication infrastructure of the CII object.*

Keywords: *critical information infrastructure, communication infrastructure, configuration infrastructure, modeling method, security assessment method, cyber resilience, protocol data blocks*

For citation: Vasinev D.A. Method of Communication Infrastructure Modeling Based on Simulation and Semi-Natural Modeling. *Proceedings of Telecommunication Universities.* 2025;11(1):70–83. (in Russ.) DOI:10.31854/1813-324X-2025-11-1-70-83. EDN:QOBBRA

Введение

Продолжающееся информационное противоборство делает актуальными вопросы обеспечения информационной безопасности (ИБ) для информационных систем (ИС), информационно-телекоммуникационных сетей (ИТС), автоматизированных систем управления (АСУТП) критических информационных инфраструктур (далее КИИ), функциони-

рующих в критически важных отраслях деятельности государства (в медицине, образовании, промышленности, энергетике поясняется отраслевой принадлежностью объектов атак). Среди прочих, целью нарушителя являются объекты КИИ. При этом уровень деструктивных действий нарушителя на коммуникационную инфраструктуру говорит о сетевых угрозах преимущественно высокого и критического уровней воздействия нарушителя, проявляющихся в атаках на КИИ[1][2][3]. В качестве составных элементов КИИ выступают распределенные фрагменты сетей, центры обработки данных (ЦОД), АСУТП, объединенные в единую распределенную ИТС организации. Пример обобщенного представления распределенной КИИ представлен на рисунке 1.

Существующие особенности построения коммуникационной инфраструктуры технологически достаточно разнообразны [1, 2]. Общими моментами являются применение технологий виртуальных частных сетей (VPN, *от англ.* Virtual Private Network), резервирования, отказоустойчивости, обеспечение киберустойчивости в условиях воздействия компьютерных атак (КА) [3–6]. Кроме того, современные условия функционирования технических систем предполагают применение отечественного коммуникационного оборудования, средств защиты для проектирования новых и импортозамещения существующих фрагментов КИИ. В этих условиях исследование в области оценки защищенности и устойчивости КИИ при воздействии на нее КА с учетом параметрических особенностей объекта, самого воздействия, является актуальной задачей [3, 7].

Воздействие нарушителя на распределенную инфраструктуру объекта КИИ обусловлено инфраструктурными, коммуникационными особенностями организации каналов связи, предлагаемых оператором, на основе которых осуществляется организация взаимодействия между распределенными филиалами телекоммуникационных объектов КИИ (см. рисунок 1). Сетевые, транспортные и управляющие протоколы (Ethernet, ICMP, IP, TCP, UDP, SNMP) применяются в коммуникационных инфраструктурах для передачи данных, управления.

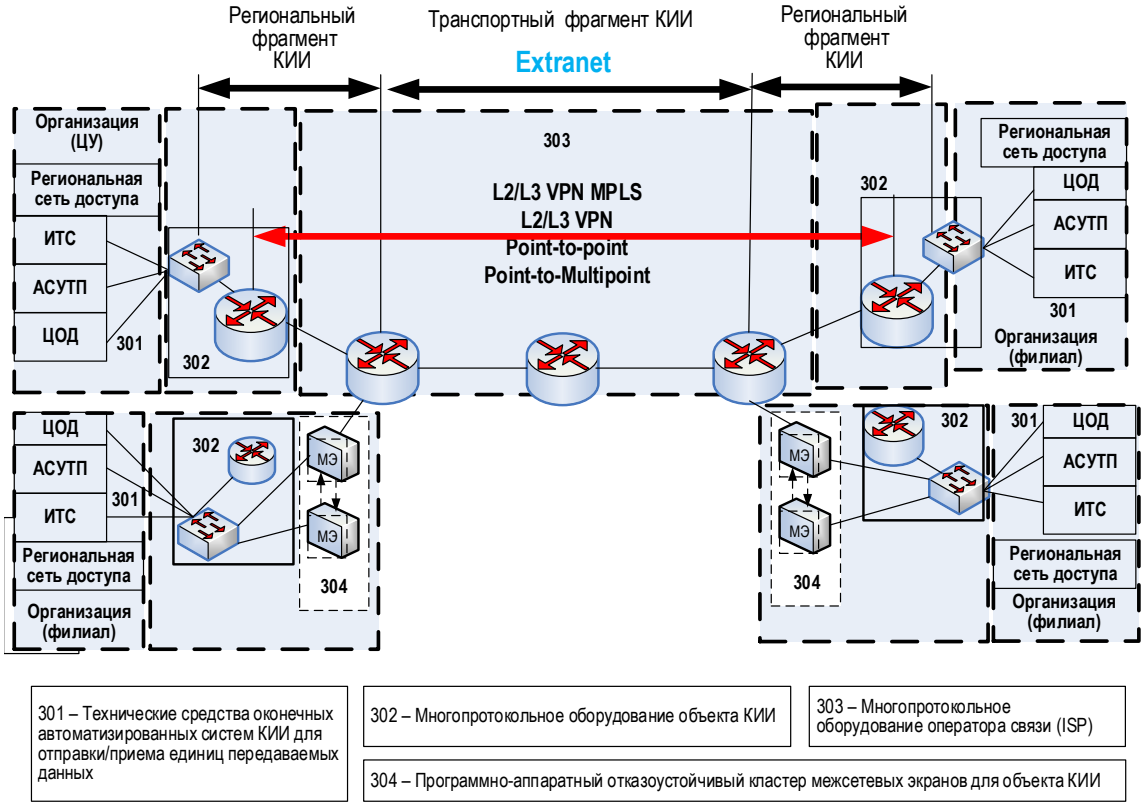


Рис. 1. Формирование распределенной инфраструктуры: для объектов ИС, АСУТП, ИТС КИИ

Fig. 1. Formation of Distributed Infrastructure: for Information System (IS), Automated Process Control Systems Information-Telecommunication System (ITS) of Critical Information Infrastructure (CII) Objects

[1] РосТелекомм. Аналитический отчет об атаках на онлайн ресурсы компании за 2022 г. URL:https:// https://rt-solar.ru/upload/iblock/34a/5w4h9o57axovdbv3ng7givrz271ykir3/Ataki-na-onlayn_resursy-rossiyskikh-kompaniy-v-2022-godu.pdf

[2] ТрансТелеКом. Аналитический отчет по сервису «Защита от DDoS-атак» 1 квартал 2023. URL: https://ttk.ru/upload/doc/business/ddos_1_2023.pdf

[3] Бюллетени НКЦКИ: новые уязвимости ПО. URL: https://safe-surf.ru/specialists/bulletins-nkcki

Для выделенных протоколов помимо иерархических – коммуникационных особенностей – можно выделить конфигурационные компоненты формирования инфраструктур, которые также могут быть причиной снижения защищенности объекта (в связи с воздействием нарушителя, или неквалифицированными действиями персонала в распределенных фрагментах ИТС).

Очевидно, что логическая структура каналов связи для объектов КИИ имеет иерархическую особенность построения, обусловленную применением коммуникационных и конфигурационных параметров в КИИ рассматриваемых подсистем (ИС, АСУТП, ИТС), функционирующих в единой распределенной сети организации. Для моделирования и оценки защищенности таких подсистем, а также исследования свойств устойчивости [6, 8, 9], с учетом иерархических особенностей формирования объектов КИИ, предлагается применять совокупность имитационных и полунатурных моделей [7]. При этом отличительным признаком данного решения на основе имитационных моделей сетей Петри является учет не только иерархии построения объектов КИИ, но и их конфигурационных и коммуникационных особенностей функционирования, а также воздействия нарушителя как на логическую (коммуникационную и конфигурационную), так и на физическую составляющую объекта КИИ [9–12, 13, 18].

В сложившихся условиях при воздействии на коммуникационную инфраструктуру объекта КИИ, сетевых воздействиях нарушителя существующие методы оценки защищенности основаны на знании сигнатур угроз и сводятся к методам оценки защищенности на основе ранее известных угроз, например, баз данных угроз (БДУ) ФСТЭК [14–17], что представлено на рисунке 2.

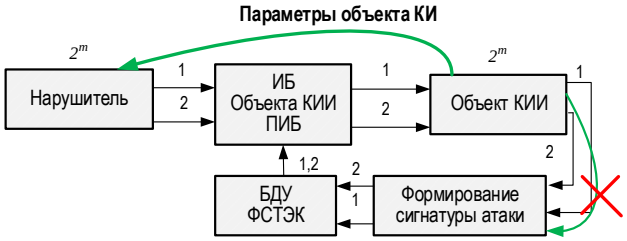


Рис. 2. Существующая подход к оценке защищенности объектов КИИ

Fig. 2. Existing Approach to Assessing the Security of Critical Information Infrastructure (CII) Facilities

В таких условиях нарушитель, работающий в известном пространстве состояний объекта КИИ, обладает сведениями о 2^m параметрах функционирования объекта КИИ. Эти же параметры являются основой для формирования воздействия нарушителя на объект КИИ. Такие возможности нарушителя позволяют изменять сигнатуры, формировать новые, ранее не известные воздействия 1 и 2 (см. рисунок 2). При этом методы обеспечения защищенности объекта КИИ на основе сигнатурных средств всегда отстают по времени от воздействия нарушителя, что создает предпосылки нахождения объекта КИИ в незащищенных состояниях 1, 2 (см. рисунок 2).

Формирование сигнатур на основе существующих БД сигнатур методами машинного обучения является перспективным направлением, требовательным к исходным данным о состоянии объекта. Причем применение для этого знаний о параметрах функционирования самого объекта КИИ является ключевым фактором, учитываемым в разрабатываемых моделях. Решением сложившегося противоречия между многообразием воздействия нарушителя и существующими возможностями методов и средств обеспечения ИБ является учет параметров объекта КИИ в формировании его политики ИБ, обозначенной на рисунке 3 как ПИБ.

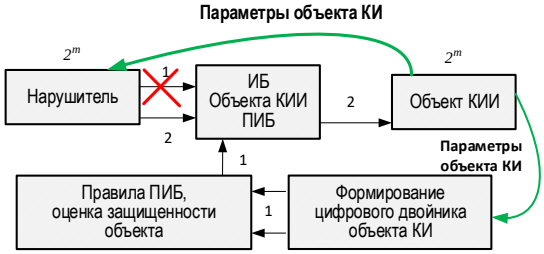


Рис. 3. Предлагаемый метод оценки защищенности объекта КИИ

Fig. 3. Proposed Method for Assessing the Security CII Facility

В основе предлагаемого метода оценки защищенности – разработанная на основе конфигурационных и коммуникационных параметров функционирования взаимосвязанная система имитационных моделей. Имитационные модели коммуникационной инфраструктуры позволяют формализовать в заданных правилах параметры коммуникационной инфраструктуры, политику ИБ, сформировать основанную на параметрах систему тестов для верификации политики ИБ. Предлагаемый метод позволяет получать параметрически точные модели коммуникационной инфраструктуры – цифрового двойника объекта КИИ, в динамике исследовать влияние на политику ИБ действий нарушителя. В основе цифрового двойника – имитационные модели на основе вложенных раскрашенных сетей Петри, верификация которых осуществляется полунатурными моделями. Комплекс моделей цифрового двойника включает в себя модель коммуникационной инфраструктуры объекта КИИ, модели каналов связи, комплекс взаимоувязанных моделей, связанных с формированием политики ИБ, анализом защищенности и действиями нарушителя [2].

Метод сквозного моделирования объектов КИИ на основе средств полунатурного и имитационного моделирования

Моделирование многоуровневых коммуникационных инфраструктур связано с особенностями их построения (рисунок 4 из [7]). На основе анализа существующих методов моделирования и оценки защищенности [8, 9, 12, 15, 17, 19–23], а также сформулированных ранее предположений о необходимости учета параметров объекта КИИ [7], разработан метод моделирования иерархически сложных телекоммуникационных объектов и метод оценки защищенности объектов КИИ на основе конфигурационных и коммуникационных параметров функционирования объекта КИИ.

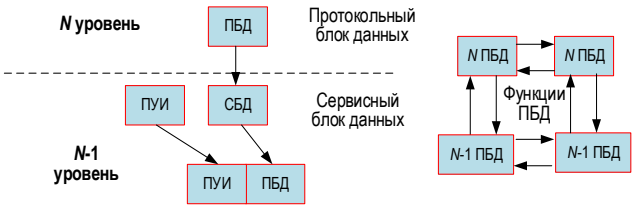


Рис. 4. Методы и способы взаимодействия протокольных блоков данных в соответствии с моделью OSI (7498), X.200 (ГОСТ Р ИСО/МЭК 7498-1-99)

Fig. 4. Methods and Ways of Interaction of PBDs in Accordance with the Following OSI Model (7498), X.200 (GOST R ISO/IEC 7498-1-99)

Основными особенностями, которые легли в основу универсальных масштабируемых модулей для имитационного и полунатурного моделирования, является внутриуровневое и межуровневое взаимодействие протокольных блоков данных, обозначенных на рисунке 4 как ПБД.

В связи с необходимостью моделировать множество протоколов, разработана концептуальная модель протокольного блока данных для реализации концепции вертикального и горизонтального взаимодействия протокольных блоков данных (рисунок 5), учитывающая наиболее важные подсистемы взаимодействия [7]. Для реализации разнотипных протокольных блоков данных, функционирующих в объектах КИИ, предлагается обобщенное концептуальное представление протокольного блока данных. В его основе – протокол с множеством параметров протокола π_l на l-м уровне функционирования в коммуникационной инфраструктуре объекта КИИ, с множеством $\Theta_{l,\pi}$ – множество функциональных связей между алгоритмами $A_{l,\pi}$ в протоколе π_l на l-м уровне функционирования в коммуникационной инфраструктуре объекта КИИ, $R_{l,\pi}$ – ресурсом на l-м уровне функционирования в коммуникационной инфраструктуре объекта КИИ, применяемым для функционирования протокола π_l коммуникационной инфраструктуры, множеством показателей качества обслуживания ($Qos_{l,\pi}$), характеризующих функциональное состояние коммуникационной инфраструктуры объекта КИИ. Для протокола π_l на l-м уровне функционирования входными / выходными параметрами являются $X_{l,\pi}$; формируется множество параметров политики информационной безопасности ($PIB_{l,\pi}$). Протокол имеет предварительно заданное множество параметров конфигураций ($CNF_{l,\pi}$). Для протокола, а также политики ИБ для протокола π_l l-го уровня предусмотрено множество параметров деструктивных воздействий ($VIB_{l,\pi}$) нарушителя на алгоритмы функционирующих в коммуникационной инфраструктуре объекта КИИ протоколов [8].

Предлагаемое обобщенное представление протокольных блоков данных позволяет объединять похожие по функциональному назначению элементы (алгоритмы работы протокола, ресурс протокола, его конфигурации, политику ИБ, воздействие нарушителя) для построения универсальных имитационных моделей на основе вложенных раскрашенных сетей Петри [7].

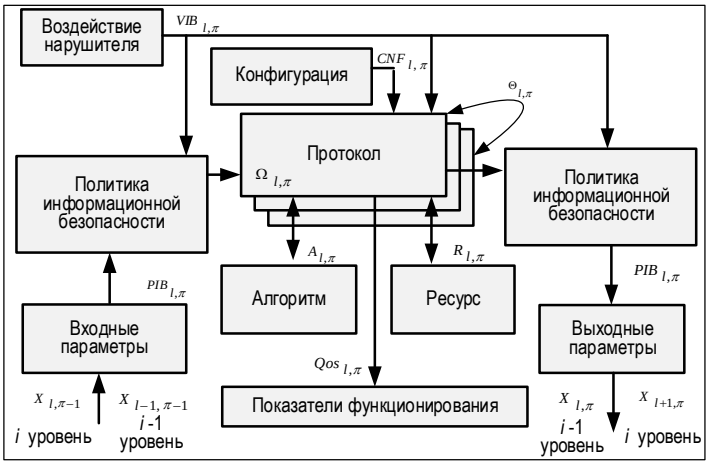


Рис. 5. Концептуальная модель протокольного блока данных

Fig. 5. Conceptual Model of the Protocol Data Unit (PDU)

Применение имитационного моделирования позволяет разработать универсальный метод построения блоков данных для различных типов протоколов, учесть коммуникационные и конфигурационные особенности их функционирования, осуществить перенос конфигурации с физического объекта в имитационные модели, являющиеся основой метода сквозного моделирования коммуникационной инфраструктуры объектов КИИ (рисунок 6).

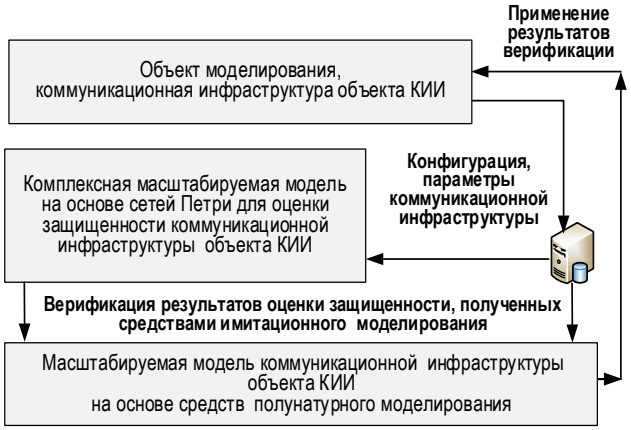


Рис. 6. Метод сквозного моделирования объектов КИИ на основе средств полунатурного и имитационного моделирования

Fig. 6. End-to-End Modeling Method of CII Objects Based on Simulation and Semi-Natural Modeling

Суть предлагаемого метода заключается во взаимосвязи конфигураций (параметров) объекта КИИ с полунатурными и имитационными моделями, а также возможностями переноса конфигурации как с физического объекта на имитационные и полунатурные модели, так и с имитационных и полунатурных моделей в физический объект. Представленная структурная взаимосвязь моделей в методе позволяет исследовать значимые свойства информационной безопасности физического объекта на имитационных и полунатурных моделях и переносить значимые результаты (оценки защищенности, результаты верификации политик ИБ), на физические объекты.

Объекты, представленные на рисунке 6, объединены единой логической составляющей – конфигурационными и коммуникационными параметрами. На физическом объекте эти параметры переносятся в полунатурные модели. Для применения в средствах имитационного моделирования необходимы дополнительные преобразования, позволяющие из разнообразных типов конфигураций получать параметры для имитационной модели. Основной задачей решаемой в методе моделирования коммуникационной инфраструктуры является получение универсальных масштабируемых имитационных и полунатурных моделей, пригодных для моделирования многоуровневых распределенных коммуникационных инфраструктур различных объектов КИИ. Структура комплекса имитационных моделей и возможные области их конфликтного взаимодействия для моделирования коммуникационной инфраструктуры объекта КИИ подсистем ИБ и действий нарушителя представлены на рисунке 7.

Пример реализации комплексной имитационной модели, учитывающей конфигурационные и коммуникационные параметры, методы обеспечения ИБ и воздействия нарушителя, представлен на рисунке 8.

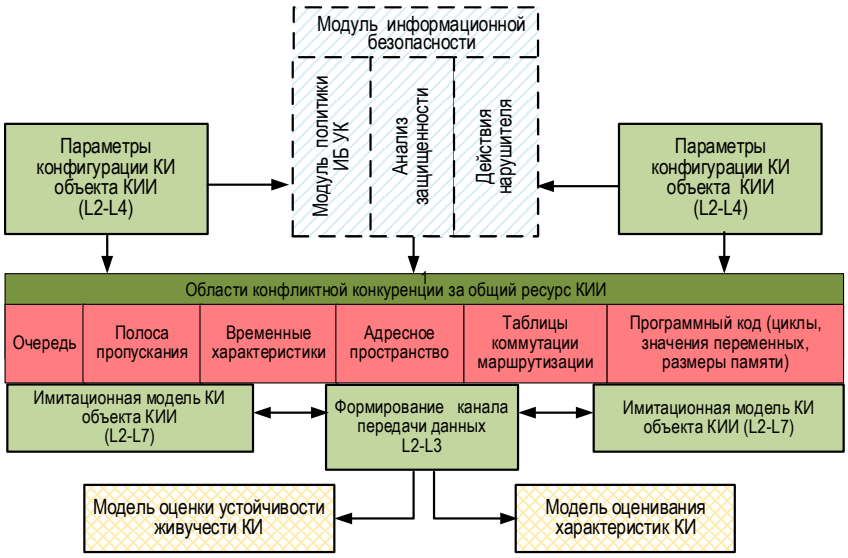


Рис. 7. Области конфликтного взаимодействия в модели оценки защищенности коммуникационной объекта КИИ

Fig. 7. Areas of Conflict Interaction in the Security Assessment Model of CII Communication Facility

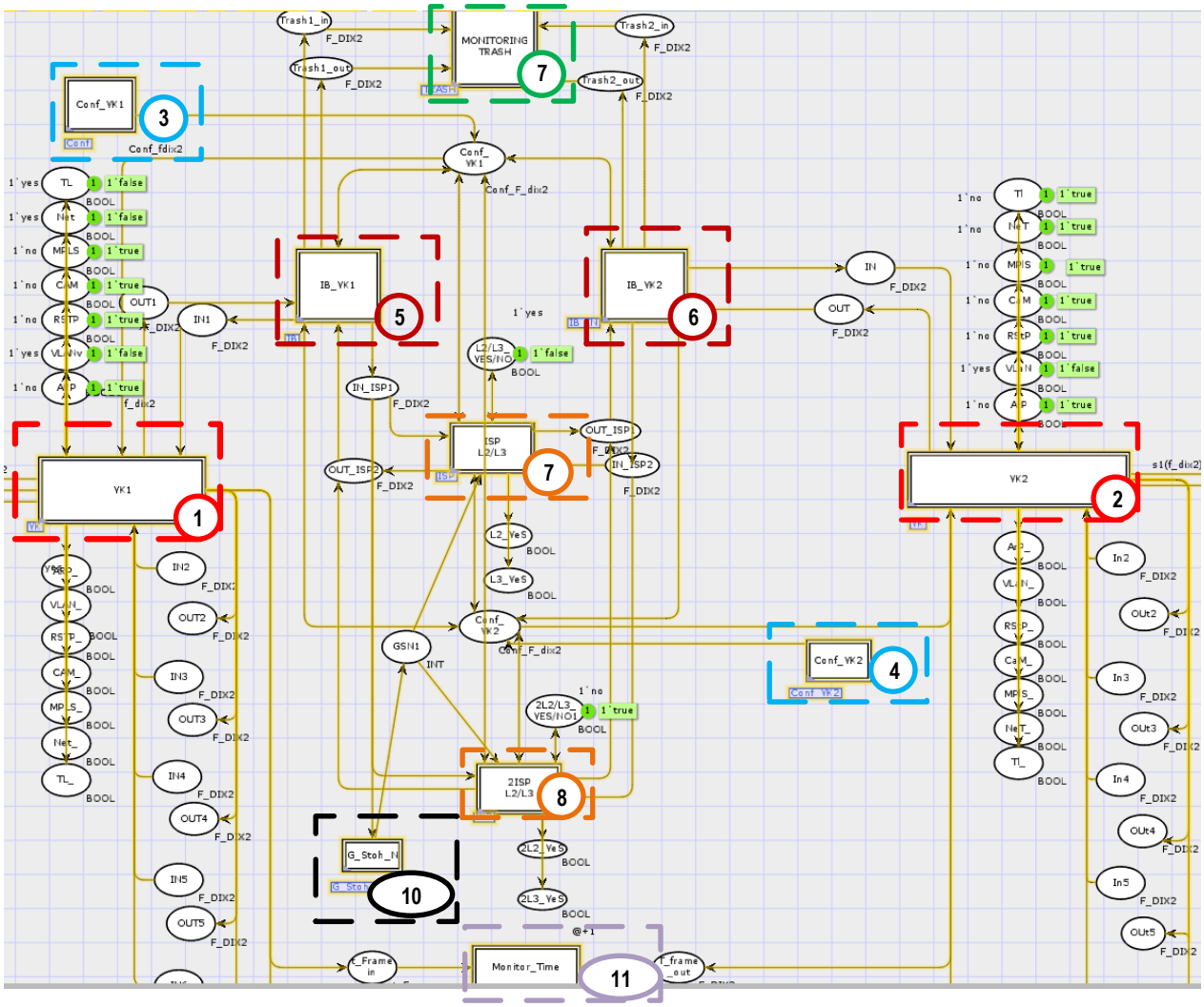


Рис. 8. Комплексная имитационная модель коммуникационной инфраструктуры с учетом функционирования методов и средств обеспечения ИБ, а также конфликтности взаимодействия

Fig. 8. Comprehensive Simulation Model of Communication Infrastructure Taking into Account the Functioning of Information Security Methods and Tools, and the Conflict of Interaction

Модель (см. рисунок 8) объединяет основные взаимодействующие субъекты, коммуникационную инфраструктуру, методы обеспечения ИБ, в том числе и воздействия нарушителя, что позволяет моделировать конфликтное поведение взаимодействующих субъектов. Имитационная модель позволяет исследовать влияние новых конфигураций, иерархических транспортных конструкций на защищенность объекта КИИ, проверять функциональность политики безопасности на потенциально возможные воздействия нарушителя, известные из БДУ ФСТЭК.

Основными составными элементами комплексной имитационной модели являются:

1, 2 – универсальные масштабируемые модели коммуникационной инфраструктуры объекта КИИ;

3, 4 – модели ввода конфигураций, коммуникационной инфраструктуры, задания сервисов;

5, 6 – универсальные масштабируемые модели ИБ для коммуникационной инфраструктуры объекта КИИ;

7 – результирующее множество регистрируемых угроз и их параметров для политики ИБ коммуникационной инфраструктуры объекта КИИ;

8, 9 – универсальные масштабируемые модели каналов оператора связи для коммуникационной инфраструктуры объекта КИИ;

10 – блок оценки устойчивости / живучести для коммуникационной инфраструктуры объекта КИИ;

11 – блок оценки характеристик устойчивости / живучести для коммуникационной инфраструктуры объекта КИИ.

Запуск имитационной модели осуществляется на основе конфигурационных данных, получаемых от физического объекта. Концепция построения функции конфигурации в имитационной модели представлен на рисунке 9.

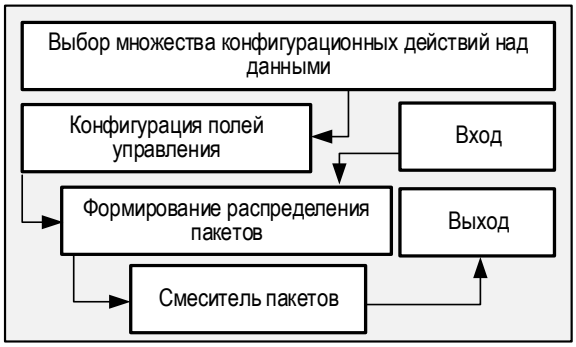


Рис. 9. Концепция построения функции конфигурации универсального протокольного блока данных коммуникационной инфраструктуры объекта КИИ

Fig. 9. Building Concept the Configuration Function of the Universal Protocol Data Block of CII Communication Facility Object

На основе поступающих на вход протокольных блоков данных различного размера формируется детерминированные или стохастические посылки протокольных блоков данных, объединяемые в смесителе, после которого поступают на выход конфигурационного блока. Блок конфигурации имитационной модели представлен на рисунке 10, является основой для работы моделей узла коммутации, а также запуска модуля ИБ и расчета тестовых конструкций для проверки политики ИБ.

Коммуникационная инфраструктура объекта КИИ обладает иерархичностью, вложенностью в соответствии с моделью взаимодействия открытых систем OSI (7498), X.200 (ГОСТ Р ИСО/МЭК 7498-1-99). Для учета иерархических и вложенных протокольных конструкций объекта КИИ разработана структура и функционал модуля коммутации в имитационной модели, обладающего свойством масштабируемости (рисунок 11).

Формируя единый универсальный модуль коммутации на основе рисунка 11, появляется возможность формировать и наращивать функциональные свойства модуля имитационной модели, моделировать функционал сервера, рабочей станции, коммутатора, маршрутизатора, других объектов коммуникационной инфраструктуры объекта КИИ. Пример реализации модуля в имитационной модели представлен на рисунке 12. Такое решение дает возможность наращивать функционал единого модуля коммутации, применять его при моделировании различных наборов протоколов, изменяя его при необходимости.

Основным элементом имитационной модели является модуль обеспечения ИБ, концепция построения которого для входящего и исходящего информационного направления представлена на рисунке 13. Для входящего и исходящего направления структура блока обеспечения ИБ содержит:

– модуль приема конфигурации протокола в форме $|m|$ параметров коммуникационной инфраструктуры;

– модель формирования политики ИБ (ее формализация в виде команд имитационной модели;

– модуль анализа защищенности для политики безопасности на основе $2 \times |m|$ тестовых параметров;

– модуль формирования действий нарушителя политики безопасности коммуникационной инфраструктуры на основе $2 \times |m \pm \Delta|$ (методом стохастического случайного поиска в заданном пространстве состояний параметров $|m|$ (Требования по безопасности информации к многофункциональным межсетевым экранам уровня сети: приказ ФСТЭК № 33 от 07.03.2024 г.).

Реализация представленной на рисунке 13 концепции построения модуля ИБ в имитационной модели на основе вложенных раскрашенных сетей Петри представлена на рисунке 14. Ключевым фактором является учет всех параметров $|m|$ коммуникационной инфраструктуры объекта КИИ, на основе которых осуществляется расчет тестовых комбинаций для анализа защищенности $2 \times |m|$, а также вторичная верификация в пространстве случайных состояний $2 \times |m \pm \Delta|$.

Предлагаемая структурно-функциональная схема построения блока обеспечения ИБ позволяет осуществлять оценку защищенности как для канала связи целиком, так и для каждого информационного направления, кроме того, – получать оценки защищенности как для входящего, так и исходящего направления. Имитационная модель позволяет формировать и детерминированные, и стохастические вектора атак, а также исследовать их влияние на политику ИБ объекта КИИ, исследовать известные угрозы из БДУ ФСТЭК и их влияние на политику ИБ.

Верификация политики ИБ множеством тестовых запросов в полунатурной модели коммуникационной инфраструктуры объекта КИИ, структура программно-аппаратного комплекса, представленного на рисунке 15, позволяет проверить работоспособность политики ИБ относительно тестов на основе параметров объекта – $|m|$.

С целью верификации политики ИБ формируется программно-аппаратный комплекс на основе полунатурных моделей, например, UNL/EVE или на основе средств виртуализации – операционных систем с открытым исходным кодом [24]. В полунатурную модель подключаются средства измерения, такие как программно-аппаратные датчики М-716, или программные средства измерения на основе программного средства iperf. Реализация тестовых протокольных конструкций осуществляется на основе программного средства Scapy, а также разработанного программно-аппаратного комплекса тестирования телекоммуникационного и оконечного оборудования объектов КИИ [25, 26].

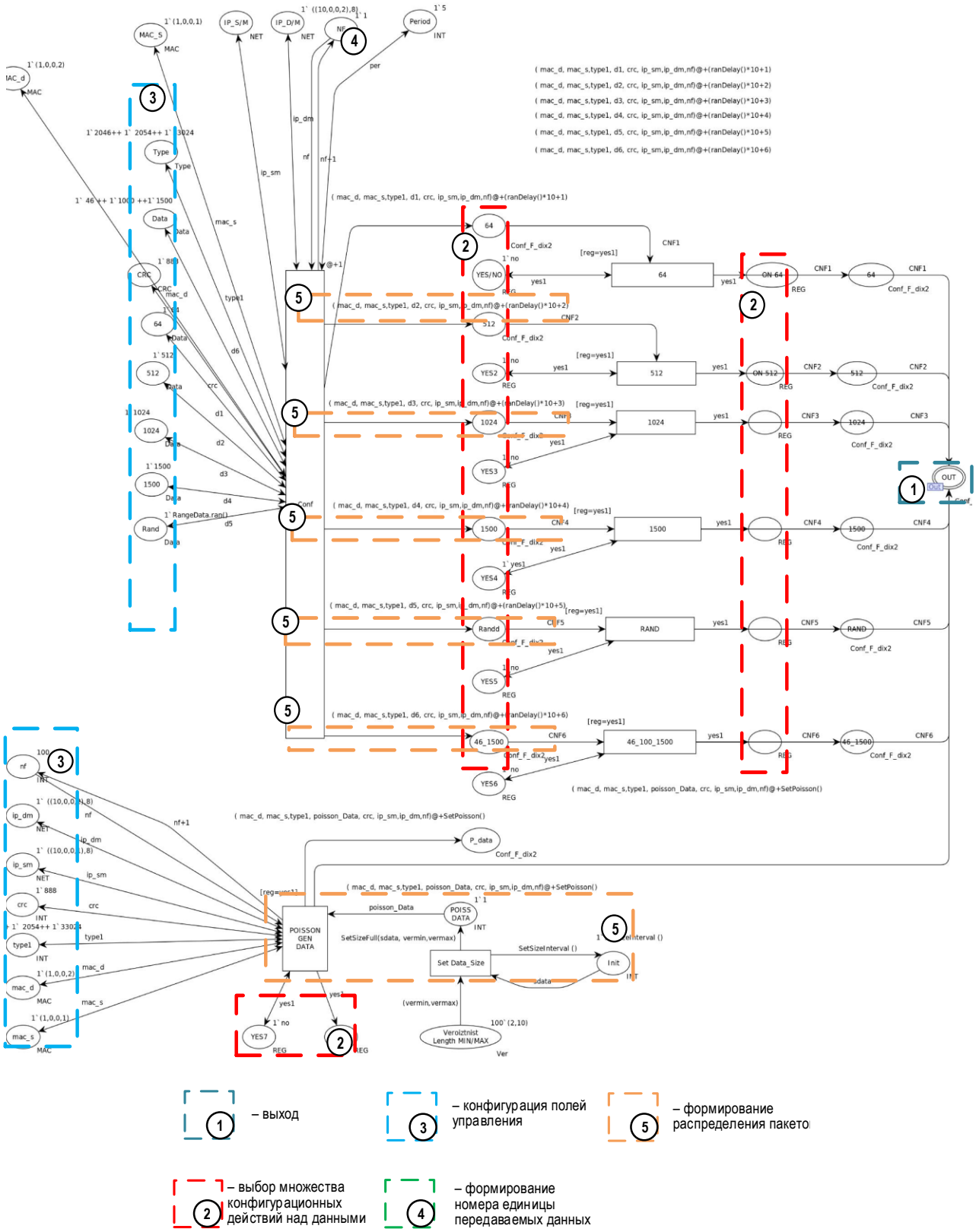


Рис. 10. Пример реализации функции конфигурации универсального протокольного блока данных коммуникационной инфраструктуры объекта КИИ

Fig. 10. Example of Implementation of the Universal Protocol Data Block of CII Communication Facility Object

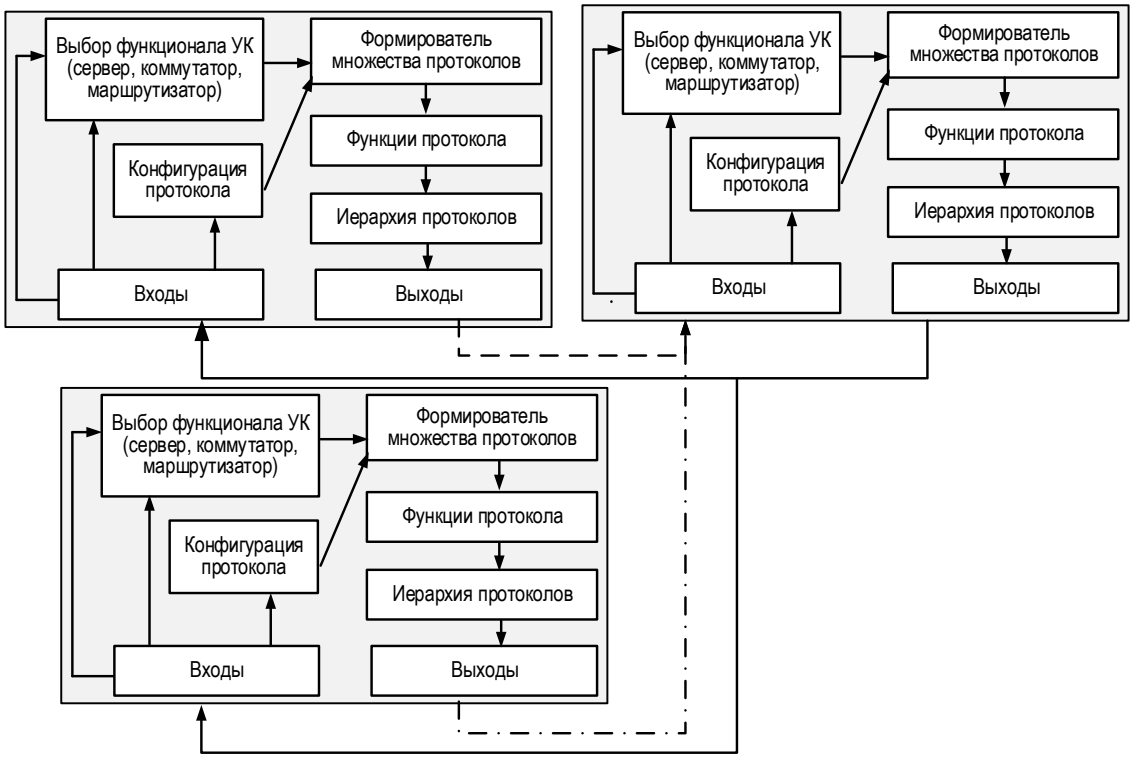


Рис. 11. Концепция иерархического построения горизонтальных и вертикальных связей протокольного блока данных коммуникационной инфраструктуры объекта КИИ

Fig. 11. Concept of Hierarchical Construction of Horizontal and Vertical Connections of Protocol Data Block of CII Communication Facility Object

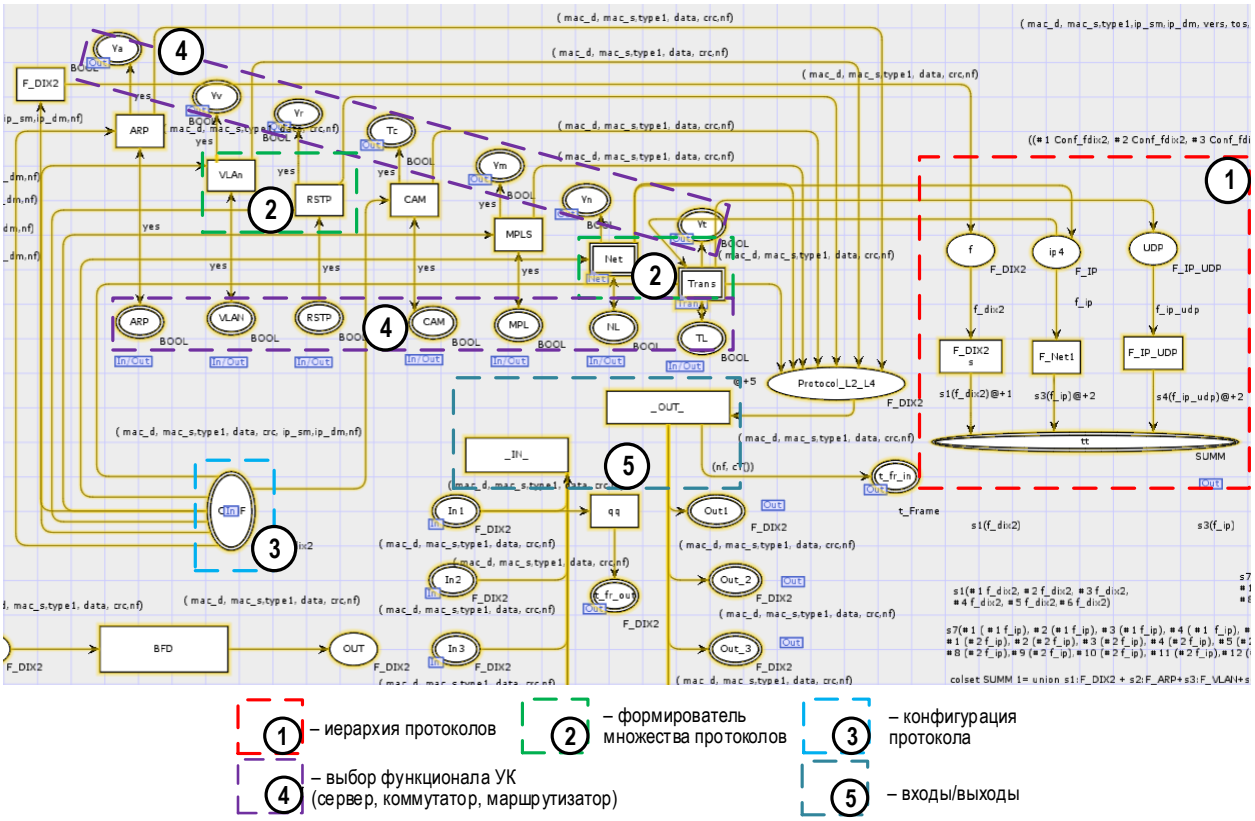


Рис. 12. Пример построения универсального протокольного блока данных для моделирования коммуникационной инфраструктуры объекта КИИ

Fig. 12. Example of Building a Universal Protocol Data Block for Modeling of CII Communication Facility Object

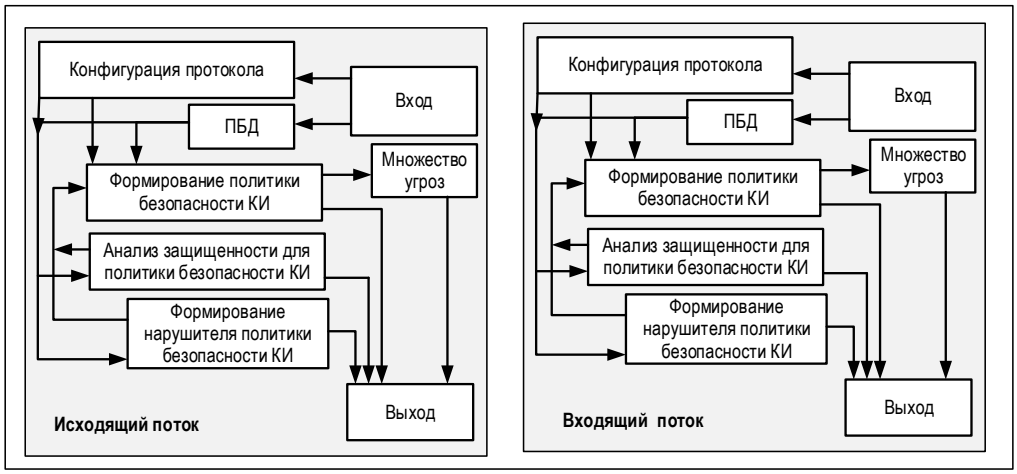


Рис. 13. Концепция построения модуля ИБ для моделирования политики ИБ, анализа защищенности, формирования модели нарушителя в коммуникационной инфраструктуре объекта КИИ

Fig. 13. Concept of Building an Information Security Module for Modeling the Information Security Policy, Security Analysis, Formation of the Intruder Model in the CII Communication Facility Object

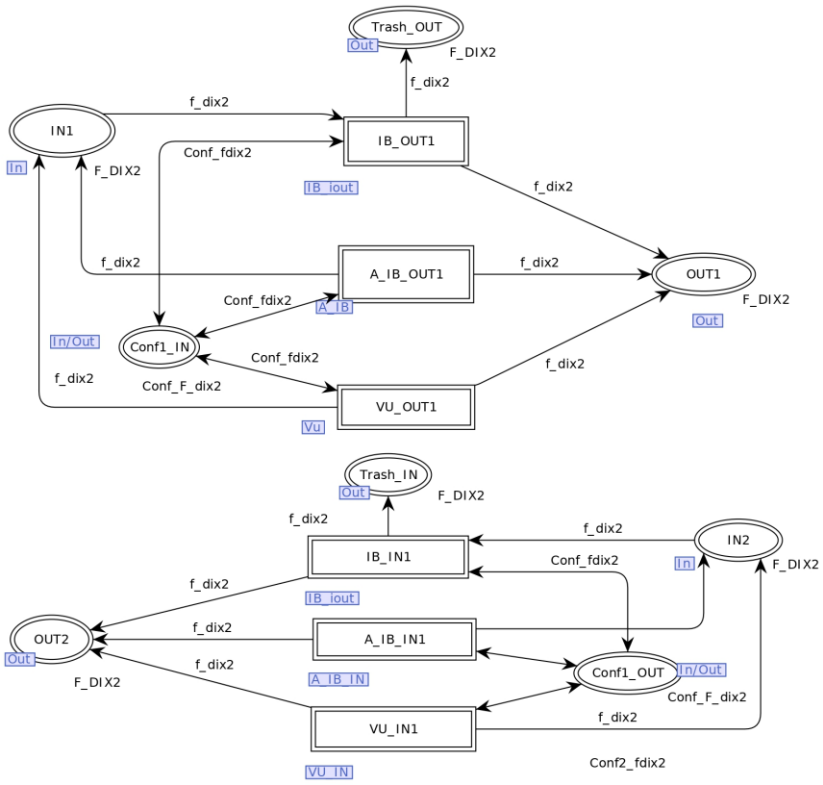


Рис. 14. Пример моделирования политики ИБ, анализа защищенности, формирования модели нарушителя в коммуникационной инфраструктуре объекта КИИ на основе вложенных, раскрашенных сетей Петри для входящего и исходящего направления

Fig. 14. Example of Modeling of Information Security Policy, Security Analysis, and Formation of Intruder Model in the CII Communication Facility Object Based on Nested, Colored Petri Nets for Incoming and Outgoing Directions

Предлагаемый метод формирования моделей коммуникационной инфраструктуры, верификация результатов имитационного моделирования позволяет формировать параметрически точные модели, учитывающие существующие конфигурации коммуникационной инфраструктуры объекта КИИ, параметры его политики ИБ, моделировать параметрическим способом действия нарушителя и исследовать влияние выделенных подсистем на защищенность объекта КИИ в динамике их взаимодействия. Верификация результатов имитационного моделирования предусмотрена полунатур-

ными моделями, аналитическими методами, сравнением функциональных характеристик (формирование и фильтрация протокольных блоков данных) с физическим объектом.

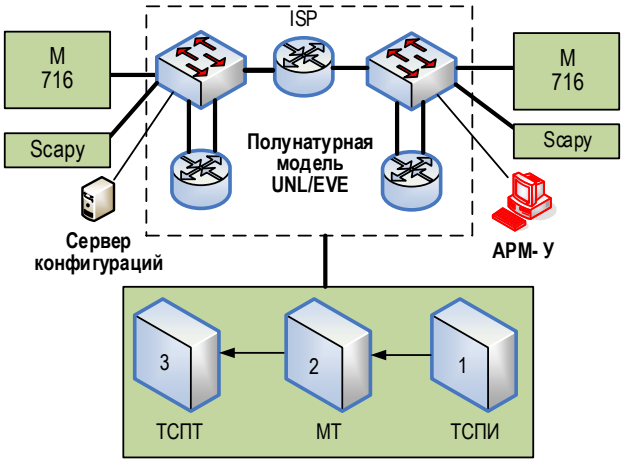


Рис. 15. Пример варианта программно-аппаратной реализации коммуникационной инфраструктуры в средствах полунатурного моделирования

Fig. 15. An Example of Variant of Software and Hardware Implementation of Communication Facility in Semi-Natural Modeling Tools

Заключение

Таким обазом, предлагаемый метод моделирования коммуникационной инфраструктуры объектов КИИ (ИС, АСУТП, ИТС) на основе иерархических, раскрашеных сетей Петри позволяет расширить прикладной аспект теории ИБ в направлении развития методов моделирования: учета иерархичности и вложенности объектов проверяемой теорией гиперграфов и реализации этих принципов вложенными, раскрашенными сетями Петри. Моделирование на основе сетей Петри позволяет исследовать влияние протокольных особенностей построения рассматриваемых объектов КИИ (ИС, АСУТП, ИТС) на свойства устойчивости и доступности, и оценивать на основе этого их защищенность. Формирование параметрически точных моделей КИИ позволяет строить цифровые двойники объектов коммуникационной инфраструктуры и в динамике исследовать функционирование такого объекта с учетом изменения конфигурации, воздействия нарушителя, формирования физических или логических резервных направлений связи. Полученные результаты позволяют разрабатывать в том числе и количественные параметрически обоснованные показатели оценки защищенности объектов КИИ.

Список источников

1. Запечников С.В., Милославская Н.Г., Толстой А.И. Основы построения виртуальных частных сетей: учебное пособие для вузов. М.: Горячая линия – Телеком, 2011. 249 с.

2. Захватов М.А. Построение виртуальных частных сетей на базе технологии MPLS. М.: Изд-во Cisco Systems, 2001.

3. Зегжда Д.П. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам. М.: Горячая линия – Телеком, 2023. 500 с.

4. Петренко С.А. Киберустойчивость цифровой индустрии 4.0. СПб.: Издательский Дом «Афина», 2020. 256 с.

5. Петренко С.А. Управление киберустойчивостью: постановка задачи // Защита информации. Инсайд. 2019. № 3(87). С. 16–24. EDN:HHVJNX

6. Штыркина А.А. Обеспечение устойчивости киберфизических систем на основе теории графов // Проблемы информационной безопасности. Компьютерные системы. 2021. № 2. С. 145–150. EDN:HACNAD

7. Бочков М.В., Васинев Д.А. Моделирование устойчивости критической информационной инфраструктуры на основе иерархических гиперсетей и сетей Петри // Вопросы кибербезопасности. 2024. № 1(59). С. 108–151. DOI:10.21681/2311-3456-2024-1-108-115. EDN:KWFIOY

8. Минаев М.В., Бондарь К.М., Дунин В.С. Моделирование киберустойчивости информационной инфраструктуры МВД России // Криминологический журнал. 2021. № 3. С. 123–128. DOI:10.24412/2687-0185-2021-3-123-128. EDN:EAKMQK

9. Осипенко А.А., Чирушкин К.А., Скоробогатов С.Ю., Жданова И.М., Корчевной П.П. Моделирование компьютерных атак на программно-конфигурируемые сети на основе преобразования стохастических сетей // Известия Тульского государственного университета. Технические науки. 2023. № 2. С. 274–281. DOI:10.24412/2071-6168-2023-2-274-281. EDN:VNGXMX

10. Ванг Л., Егорова Л.К., Мокряков А.В. Развитие теории Гиперграфов // Известия РАН. Теория и системы управления. 2018. № 1. С. 111–116. DOI:10.7868/S00023388180110. EDN:YSTDTE

11. Величко В.В., Попков В.К. Модели и методы повышения живучести современных систем связи. М.: Горячая линия – Телеком, 2017. 270 с.

12. Попков Г.В., Попков В.К. Математические основы моделирования сетей связи. М.: Горячая линия – Телеком, 2018. 182 с.

13. Колосок И.Н., Гурина Л.А. Оценка показателей киберустойчивости систем сбора и обработки информации в ЭЭС на основе полумарковских моделей // Вопросы кибербезопасности. 2021. № 6(46). С. 2–11. DOI:10.21681/2311-3456-2021-6-2-11. EDN:IJWNVI

14. Гурина Л.А. Повышение киберустойчивости SCADA и WAMS при кибератаках на информационно-коммуникационную подсистему ЭЭС // Вопросы кибербезопасности. 2022. № 2(48). С. 18–26. DOI:10.21681/2311-3456-2022-2-18-26. EDN:QITQLA

15. Гурина Л.А. Оценка киберустойчивости системы оперативно-диспетчерского управления ЭЭС // Вопросы

кибербезопасности. 2022. № 3(49). С. 23–31. DOI:10.21681/2311-3456-2022-3-23-31. EDN:SAPIYH

16. Чиркова Н.Е. Анализ существующих подходов к оценке киберустойчивости гетерогенных систем // Международная научно-практическая конференция «Техника и безопасность объектов уголовно-исполнительной системы» (Воронеж, Российская Федерация, 18–19 мая 2022 г.). Иваново: ИПК "ПресСто", Воронежский институт ФСИН России, 2022. С. 408–410. EDN:CPZRVP

17. Макаренко С.И. Динамическая модель системы связи в условиях функционально-разноуровневого информационного конфликта наблюдения и подавления // Системы управления, связи и безопасности. 2015. № 3. С. 122–185. DOI:10.24411/2410-9916-2015-10307. EDN:UKSPAV

18. Бобров В.Н., Захарченко Р.И., Бухаров Е.О., Калач А.В. Системный анализ и обоснование выбора моделей обеспечения киберустойчивого функционирования объектов критической информационной инфраструктуры // Вестник Воронежского института ФСИН России. 2019. № 4. С. 31–43. EDN:DPJJCN

19. Левшун Д.С. Иерархическая модель для проектирования систем на основе микроконтроллеров защищенными от киберфизических атак // Труды учебных заведений связи. 2023. Т. 9. № 1. С. 105–115. DOI:10.31854/1813-324X-2023-9-1-105-115. EDN:QCZRIH

20. Костогрызов А.И., Нистратов А.А., Голосов П.Е. Методические положения по вероятностному прогнозированию качества функционирования информационных систем. Часть 2. Моделирование с использованием «Черных ящиков» // Вопросы кибербезопасности. 2024. № 6(64). С. 2–27. DOI:10.21681/2311-3456-2024-6-2-27. EDN:ELOIDW

21. Язов Ю.К., Панфилов А.П. Составные сети Петри-Маркова со специальными условиями построения для моделирования угроз информационной безопасности // Вопросы кибербезопасности. 2024. № 2(60). С. 53–65. DOI:10.21681/2311-3456-2024-2-53-65. EDN:TEJAVM

22. Водопьянов А.С. Использование цифровых двойников с целью обеспечения информационной безопасности киберфизических систем // Вопросы кибербезопасности. 2024. № 4(62). С. 140–144. DOI:10.21681/2311-3456-2024-4-140-144. EDN:XTJILH

23. Скрыль С.В., Ицкова А.А., Ушаков К.Е. О возможности совершенствования процедур количественной оценки защищенности информации объектов критической информационной инфраструктуры от угроз несанкционированного доступа // Безопасность информационных технологий. 2024. Т. 31. № 3. С. 94–104. DOI:10.26583/bit.2024.204. EDN:CZFYYR

24. Васинев Д.А. Применение операционных систем с открытым исходным кодом в коммуникационном оборудовании для сетей с коммутацией пакетов // Вопросы кибербезопасности. 2016. № 4(17). С. 36–44. DOI:10.21681/2311-3456-2016-4-36-44. EDN:XCMVAV

25. Васинев Д.А., Соловьев М.В. Предложения по построению универсального фаззера протоколов // Труды учебных заведений связи. 2023. Т. 9. № 6. С. 59–67. DOI:10.31854/1813-324X-2023-9-6-59-67. EDN:AABMEE

26. Васинев Д.А., Бочков М.В., Кирьянов А.В., Андреев С.Ю., Полехин А.А., Сенотрусов И.А. и др. Способ и программно-аппаратный комплекс для оценки защищенности телекоммуникационного оконечного оборудования критической информационной инфраструктуры. Патент на изобретение № RU 2831928 C1. Опубл. 16.12.2024.

References

1. Zapechnikov S.V., Miloslavskaya N.G., Tolstoj A.I. *Basics of Building Virtual Private Networks*. Moscow: Goryachaya liniya – Telekom Publ.; 2011. 249 p. (in Russ.)

2. Zahvatov M.A. *Building Virtual Private Networks Based on MPLS Technology*. Moscow: Cisco Systems Publ.; 2001. (in Russ.)

3. Zegzhda D.P. *Cybersecurity of the Digital Industry. Theory and Practice of Functional Resistance to Cyberattacks*. Moscow: Goryachaya liniya – Telekom Publ.; 2023. 500 p. (in Russ.)

4. Petrenko S.A. *Cyber Resilience of Digital Industry 4.0*. Saint Petersburg: Afina Publ.; 2020. 256 p. (in Russ.)

5. Petrenko S.A. Cyber Resilience Management: Problem Statement. *Zaŝita informacii. Inside*. 2019;3(87):16–24. (in Russ.) EDN:HHVJNX

6. Shtyrkina A.A. Cyber-Physical Systems Sustainability Based on Graph Theory. *Information Security Problems. Computer Systems*. 2021;2:145–150. (in Russ.) EDN:HACNAD

7. Bochkov M.V., Vasinev D.A. Modeling the Stability of Critical Information Infrastructure Based on Hierarchical Hypernets and Petri Nets. *Voprosy kiberbezopasnosti*. 2024;1(59):108–151. (in Russ.) DOI:10.21681/2311-3456-2024-1-108-115. EDN:KWFIOY

8. Minaev M.V., Bondar K.M., Dunin V.S. Modeling of Cyber Resilience Information Infrastructure of the Internal Affairs Ministry of Russia. *Kriminologicheskij zhurnal.* 2021;3:123–128. (in Russ.) DOI:10.24412/2687-0185-2021-3-123-128. EDN:EAKMQK

9. Osipenko A.A., Chirushkin K.A., Skorobogatov S.Yu., Zhdanova I.M., Korchevnoj P.P. Simulation of Computer Attacks on Software-Configured Networks Based on Stochastic Networks Transformation. *Izvestiya Tula State University. Technical Sciences*. 2023;2:274–281. (in Russ.) DOI:10.24412/2071-6168-2023-2-274-281. EDN:VNGXMX

10. Vang L., Egorova L.K., Mokryakov A.V. Development of Hypergraph Theory. *Journal of Computer and Systems Sciences International*. 2018;57(1):109–114. DOI:10.1134/S1064230718010136. EDN:XXVAJV

11. Velichko V.V., Popkov V.K. *Models and Methods for Increasing the Survivability of Modern Communication Systems*. Moscow: Goryachaya liniya – Telekom Publ.; 2017. 270 p. (in Russ.)

12. Popkov G.V., Popkov V.K. *Mathematical Foundations of Communication Network Modeling*. Moscow: Goryachaya liniya – Telekom Publ.; 2018. 182 p. (in Russ.)

13. Kolosok I.N., Gurina L.A. Assessment of Cyber Resilience Indices of Information Collection and Processing Systems in Electric Power Systems Based on Semi-Markov Models. *Voprosy kiberbezopasnosti*. 2021;6(46):2–11. (in Russ.) DOI:10.21681/

2311-3456-2021-6-2-11. EDN:IJWNVI

14. Gurina L.A. Increasing Cyber Resilience of SCADA and WAMS in the Event of Cyber Attacks on the Information and Communication Subsystem of the Electric Power System. *Voprosy kiberbezopasnosti*. 2022;2(48):18–26. (in Russ.) DOI:10.21681/2311-3456-2022-2-18-26
15. Gurina L.A. Assessment of Cyber Resilience of Operational Dispatch Control System of EPS. *Voprosy kiberbezopasnosti.* 2022;3(49):23–31. (in Russ.) DOI:10.21681/2311-3456-2022-3-23-31. EDN:SAPIYH
16. Chirkova N.E. Analysis of Existing Approaches to Assessing the Cyber Resilience of Heterogeneous Systems. *Proceedings of the International Scientific and Practical Conference on Technology and Security of Penal System Facilities, 18–19 May 2022, Voronezh, Russian Federation*. Ivanovo: PressTo Publ.; Voronezh Institute of the Federal Penitentiary Service of Russia Publ.; 2022. p.408–410. (in Russ.) EDN:CPZRVP
17. Makarenko S.I. Dynamic Model of Communication System in Conditions the Functional Multilevel Information Conflict of Monitoring and Suppression. *Systems of Control, Communication and Security.* 2015;3:122–186. (in Russ.) DOI:10.24411/2410-9916-2015-10307. EDN:UKSPAV
18. Bobrov V.N., Zaharchenko R.I., Buharov E.O., Kalach A.V. System Analysis and Justification of Selection of Models for Ensuring Cyber-Stable Functioning of Critical Information Infrastructure Facilities. *Vestnik of Voronezh Institute of the Russian Federal Penitentiary Service*. 2019;4:31–43. (in Russ.) EDN:DPJJCN
19. Levshun D. Hierarchical Model for the Design of Microcontroller-Based Systems Protected from Cyber-Physical Attacks. *Proceedings of Telecommunication Universities*. 2023;9(1):105–115. (in Russ.) DOI:10.31854/1813-324X-2023-9-1-105-115. EDN:QCZRIH
20. Kostogryzov A.I., Nistratov A.A., Golosov P.E. Methodological Provisions on Probabilistic Prediction of Information Systems Operation Quality. Part 2. Modeling Using "Black Boxes". *Voprosy kiberbezopasnosti*. 2024;6(64):2–27. (in Russ.) DOI:10.21681/2311-3456-2024-6-2-27. EDN:ELOIDW
21. Yazov Yu.K., Panfilov A.P. Composite Petri-Markov Networks With Special Construction Conditions for Modeling Information Security Threats. *Voprosy kiberbezopasnosti*. 2024;2(60):53–65. (in Russ.) DOI:10.21681/2311-3456-2024-2-53-65. EDN:TEJAVM
22. Vodopyanov A.S. Using Digital Twins to Ensuring Information Security of Cyberphysical Systems. *Voprosy kiberbezopasnosti*. 2024;4(62):140–144. (in Russ.) DOI:10.21681/2311-3456-2024-4-140-144. EDN:XTJILH
23. Skryl S.V., Iczkova A.A., Ushakov K.E. On the Possibility of Improving the Procedures for Quantifying Information Protection of Critical Information Infrastructure Objects from Threats of Unauthorized Access. *IT Security*. 2024;31(3):94–104. (in Russ.) DOI:10.26583/bit.2024.204. EDN:CZFYY
24. Vasinev D.A. Application of Operating Systems with Open Source Code in of Communication Equipment for Networks with Commutation of Packages. *Voprosy kiberbezopasnosti.* 2016;4(17):36–44. (in Russ.) DOI:10.21681/2311-3456-2016-4-36-44. EDN:XCMVAV
25. Vasinev D., Solovev M. Proposals for Universal Protocol Fuzzer Construction. *Proceedings of Telecommunication Universities*. 2023;9(6):59–67. (in Russ.) DOI:10.31854/1813-324X-2023-9-6-59-67. EDN:AABMEE
26. Vasinev D.A., Bochkov M.V., Kirianov A.V., Andreev S.Iu., Polekhin A.A., Senotrusov I.A., et al. *Method and Software and Hardware System for Assessing Security of Telecommunication and Terminal Equipment of Critical Information Infrastructure*. Patent RF, no. 2831928 C1, 16.12.2024. (in Russ.)

Статья поступила в редакцию 24.12.2024; одобрена после рецензирования 12.02.2025; принята к публикации 20.02.2025.
The article was submitted 24.12.2024 approved after reviewing 12.02.2025; accepted for publication 20.02.2025.

Информация об авторе:

ВАСИНЕВ Дмитрий Александрович

кандидат технических наук, сотрудник Академии Федеральной службы охраны Российской Федерации
https://orcid.org/0009-0004-7030-5421

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

Научная статья
УДК 004.41
https://doi.org/10.31854/1813-324X-2025-11-1-84-98
EDN:URSGXI

Проблемные вопросы генетической деэволюции представлений программы для поиска уязвимостей и рекомендации по их разрешению

Константин Евгеньевич Израилов, konstantin.izrailov@mail.ru

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук,
Санкт-Петербург, 199178, Российская Федерация

Аннотация

Актуальность *темы обосновывается отсутствием методологии реверс-инжиниринга программного обеспечения, необходимой для разрешения следующего научного противоречия области (как противопоставления потребности vs возможности): с одной стороны поиск уязвимостей наиболее эффективен в тех представлениях программы, в которых они были внедрены (например, исходный код, алгоритмы или архитектура); с другой стороны, для анализа имеется, как правило, лишь машинный код, слабо подходящий для выявления высокоуровневых уязвимостей (т.е. из более ранних представлений). Созданию составляющих данной методологии (концепции, модели, метода, алгоритмов, метрики, а также их реализаций) и посвящено основное авторское исследование, заключительный этап которого приводится в статье.*

Целью *настоящей статьи является обсуждение 25 проблемных вопросов (так называемая научная дискуссия), возникших в основном исследовании, посвященном развитию направления реверс-инжиниринга программного обеспечения на базе генетических алгоритмов. Основным применением результатов исследования является как получение представления программы, подходящего для экспертного (и иного) анализа на предмет наличия в нем уязвимостей, так и их непосредственный поиск встроенным сигнатурным методом. При этом разрешение даже части вопросов позволит существенно* ***повысить эффективность*** *такого генетического реверс-инжиниринга.*

В работе использованы следующие ***методы****: анализ результатов основного исследования для выделения проблемных вопросов, синтез путей их разрешения, а также систематизация и балльное сравнение вопросов с позиции путей устранения для общей оценки завершенности научной работы.*

Детальное ***изучение*** *причин возникновения каждого из вопросов позволило определить пути их разрешения, реализуемость которых обосновывает и результаты основного исследования. В частности, проблемные вопросы* ***базируются*** *как на отсутствии одних теоретических инструментов, необходимых для генетического реверс-инжиниринга, так и на недостаточной практической эффективности других.*

Научная новизна *проблемных вопросов заключается в том, что практически каждый из них озвучен впервые.*

Теоретическая значимость*: развитие каждого проблемного вопроса может как открыть отдельное научное исследование (или даже направление), так и получить новые значимые результаты.*

Практическая значимость *заключается в возможности создания программных решений по разрешению выявленных вопросов, которые могут быть также применены и для смежных задач.*

Ключевые слова: *информационная безопасность, уязвимость, программа, реверс-инжиниринг, генетический алгоритм, деэволюция, декомпиляция, проблемные вопросы*

Источник финансирования: *Работа выполнена при частичной финансовой поддержке бюджетной темы FFZF-2025-0016.*

Ссылка для цитирования: Израилов К.Е. Проблемные вопросы генетической деэволюции представлений программы для поиска уязвимостей и рекомендации по их разрешению // Труды учебных заведений связи. 2025. Т. 11. № 1. С. 84–98. DOI:10.31854/1813-324X-2025-11-1-84-98. EDN:URSGXI

Original research
https://doi.org/10.31854/1813-324X-2025-11-1-84-98
EDN:URSGXI

Problematic Issues of a Program Representations Genetic De-Evolution for Search Vulnerabilities and Recommendations for Its Resolution

Konstantin E. Izrailov, konstantin.izrailov@mail.ru

Saint-Petersburg Federal Research Center of the Russian Academy of Sciences,
St. Petersburg, 199178, Russian Federation

Annotation

The relevance *of the topic is justified by the software reverse engineering methodology lack required to resolve the following scientific contradiction in the field (as a contrast between need and opportunity): on the one hand, vulnerability search is most effective in those program representations in which they were implemented (e.g. source code, algorithms or architecture); on the other hand, as a rule, only machine code is available for analysis, which is poorly suited for identifying high-level vulnerabilities (i.e. from earlier representations). The main author's study, the final stage of which is given in the article, is devoted to the creation of the this methodology elements (concept, model, method, algorithms, metrics, as well as their implementations).*

The purpose *of this article is to discuss 25 problematic issues (the so-called scientific discussion) that arose in the main study devoted to the software reverse engineering development based on genetic algorithms. The main application of the research results is both obtaining a program representation suitable for expert (and other) analysis for vulnerabilities, and their direct search using the built-in signature method. At the same time, resolving even a part of the issues will significantly* ***increase the efficiency*** *of such genetic reverse engineering.*

The following ***methods*** *were used in the work: the main research results analysis to identify problematic issues, ways to resolve them synthesis, as well as issues systematization and scoring from the standpoint of ways to eliminate them for an overall assessment of the scientific work completeness.*

A causes of each issue detailed ***research*** *allowed us to determine ways to resolve them, the feasibility of which also justifies the main research results. In particular, problematic issues are* ***based both on*** *some absence of theoretical tools necessary for genetic reverse engineering, and on the insufficient practical efficiency of others.*

The scientific novelty *of the issues lies in the fact that almost each of them is voiced for the first time.*

The theoretical significance *lies in the fact that the development of each problematic issue can both open a separate scientific study (or even a direction), and obtain new significant results.*

The practical significance *lies in the possibility of creating software solutions to resolve identified issues, which can also be applied to related tasks.*

Keywords: *information security, vulnerability, program, reverse engineering, genetic algorithm, de-evolution, decompilation, problematic issues*

Funding: *The work was partially funded by the budget project FFZF-2025-0016.*

For citation: Izrailov K.E. Problematic Issues of a Program Representations Genetic De-evolution for Search Vulnerabilities and Recommendations for Its Resolution. *Proceedings of Telecommunication Universities.* 2025;11(1): 84–98. (in Russ.) DOI:10.31854/1813-324X-2025-11-1-84-98. EDN:URSGXI

Введение

Наличие уязвимостей в программном обеспечении (далее – ПО) является актуальнейшей проблемой в области информационных технологий. Несмотря на наличие определенного пула качественно разных способов их поиска (например, применяя сигнатурный и эвристический анализ [1], нечеткие хэши [2] и пр.), все они обладают соб-

ственными недостатками, что не позволяет создать «идеальный» способ. Как результат, исследования в данном направлении информационной безопасности (далее – ИБ) еще далеки от завершения; притом, в условиях, когда злоумышленники, сознательно внедряющие уязвимости в программный код, непрерывно совершенствуют свои методы и инструменты. Одним из применяемых подходов является *реверс-инжиниринг ПО*, классически заключающийся в преобразовании машинного кода программы (далее – МК), слабо пригодного для ручного анализа, в более высокоуровневое представление исходного кода (далее – ИК), которое поддается анализу на предмет наличия уязвимостей эксперту по безопасности ПО (далее – Эксперт); такой подход носит название *декомпиляции* программы.

Концепция качественно нового авторского способа реверс-инжиниринга ПО (далее – Концепция), основанная на применении генетического алгоритма (далее – ГА), уже имеет определенную доказательную базу в виде большого пула публикаций, посвященных теоретическим изысканиям и практическим реализациям в виде программного прототипа (далее – Прототип), преобразующего при ряде ограничений заданный МК в соответствующий ему ИК. Тем не менее, как и для любой инновационной работы, в реализации Концепции существуют ряд проблемных вопросов, которым и посвящена данная статья.

Результаты исследования

Прежде чем кратко описать полученные результаты в рамках создания Концепции, укажем используемые в ней термины и понятия.

Терминология

Поскольку в основу Концепции положено применение ГА, то часть основных связанных с этим термином имеет слово «генетический».

По аналогии с существующей в области терминологией, для получения ИК из МК применяется *генетическая декомпиляция* (далее – ГДК), суть которой заключается в получении предыдущего представления программы из текущего, которое имеет бинарный вид инструкций процессора (естественно, с помощью ГА [3]).

Расширение Концепции на любые формы программы, используемые в рамках программной инженерии (например, алгоритмы и архитектуру), позволяют говорить о получении каждого предыдущего представления из текущего (а не только ИК из МК), т. е. о *генетической деэволюции* пары представлений (далее – ГДЭ) [4, 5]. Необходимость в ГДЭ более высокоуровневых представлений обосновывается тем, что поиск уязвимостей наиболее эффективен в том представлении, в котором они были заложены в программу (как сознательно, так и случайно).

И, наконец, весь процесс последовательности преобразований пар представлений (например, от МК до концептуальной модели программы) в рамках Концепции назван генетическим *реверс-инжинирингом* (далее – ГРИ). Данный термин и определяет предметную область авторского исследования – проведение ГРИ программы в интересах поиска в ней уязвимостей. Очевидно, что ГРИ является диаметрально противоположным процессом классической программной инженерии.

Соответствие основных «генетических» терминов предметной области отображено на рисунке 1; обозначение «Представление P_i» соответствует i-му представлению программы. При этом отличительной особенностью ГРИ от аналогичных решений является гипотетическая независимость его алгоритмов от синтаксисов представлений, а также получение программы, в точности собираемой (в случае ИК – компилируемой) в исследуемую.

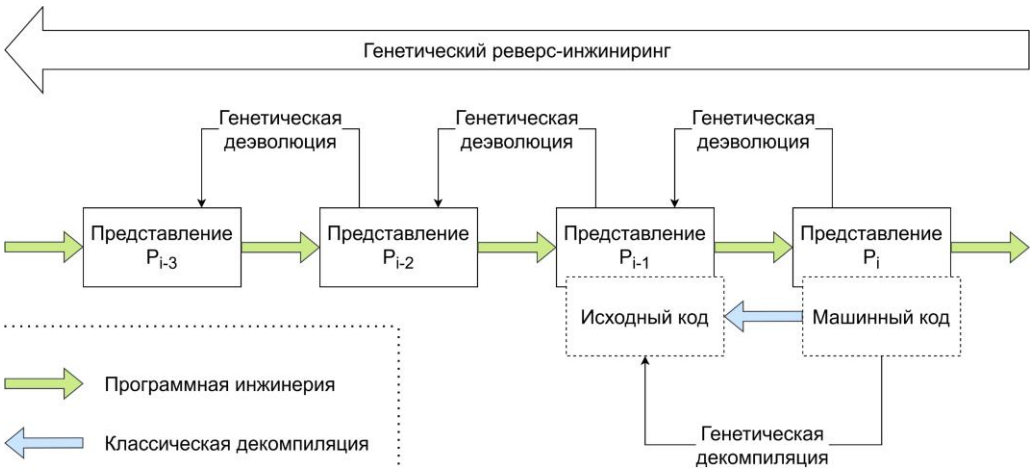


Рис. 1. Соответствие основных терминов предметной области

Fig. 1. Correspondence of the Subject Area Main Terms

Кроме того, несмотря на то, что современные декомпиляторы в ряде случаев справляются с получением ИК по МК существенно лучше (хотя и получают зачастую лишь псевдо ИК, не всегда компилируемый), однако их реализации работают с крайне ограниченным набором пар представлений. К примеру, плагин Hex-Rays, входящий в продукт IDA Pro, в максимальной комплектации позволяет декомпилировать только 6 процессорных архитектур (x86, ARM, MIPS, PowerPC, ARC и RICS) и только в С-подобный псевдокод (https://hex-rays.com/pricing), хотя общее количество как процессоров, так и языков программирования (далее – ЯП) достаточно большое, не говоря уже об их комбинации.

На текущий момент в области поиска уязвимостей путем реверс-инжиниринга основной задачей является именно получение ИК из МК, поскольку большинство ПО, используемого в критических областях (например, в киберфизических системах или встроенных устройствах) не имеет открытых текстов ИК. Поэтому, хотя далее и будут приведены основные полученные результаты и проблемные вопросы для ГДЭ (составляющих весь ГРИ), основной целью доработки Прототипа и Концепции является осуществление именно ГДК.

Генетическая деэволюция представлений

Общий принцип ГДЭ (являющейся обобщением ГДК на любые представления и составляющей весь процесс ГРИ), как было указано, основан на работе ГА, которым посвящено достаточное количество публикаций [6]. Так, суть ГА заключается в итеративном решении оптимизационной задачи по нахождению экстремума целевой функции путем генерации большого количества особей популяции, каждая из которых задает одно из возможных (вначале неверных) решений задачи. Каждая особь сопоставляется с некоторой хромосомой, гены которой в некотором смысле являются параметрами такой функции приспособленности (в англоязычной литературе называемой *Fitness*), поскольку она показывает «успешность» особи или ее близость к идеальной эталонной – т. е. той, которая и является искомым решением.

Для сопоставления особи хромосомой применяются следующие основные операции:

– генерация первоначальной популяции особей (состоящих из случайных хромосом);

– скрещивание (получение новой особи из хромосом ее родителей);

– мутация (случайное изменение ген особи);

– селекция (отбор в новую популяцию наилучших особей, т. е. имеющих максимальную приспособленность).

Естественно, в ГА присутствуют определенные вариации, такие, как получение нескольких особей при скрещивании или отбор не всегда наилучших особей. Выбор частоты скрещивания и мутации имеет принципиальное значение для скорости схождения алгоритмов [7].

Для понимания ГДЭ, опишем ее в терминах ГА, используя примеры, характерные для ГДК. Сама оптимизационная задача заключается в поиске экземпляра программы в предыдущем представлении, который бы при сборке ПО (например, компиляции) преобразовывался в некоторую эталонную программу в текущем представлении; таким образом, можно будет говорить о деэволюции этой программы в более высокоуровневое представление (например, путем получения искомого ИК из эталонного МК). Сама функция приспособленности в этом случае оценивает близость программы, полученной при сборке из текущего представления, с эталонной (например, некоторый ИК компилируется в МК и сравнивается с эталонным МК, близость к которому и определяет его приспособленность а, следовательно, и шансы на «выживание» в новой популяции). Под особями же, таким образом, понимаются экземпляры программ в требуемом представлении, а их хромосомы и гены определяют способ ее записи (например, через токены языка программирования или более сложные конструкции). В рамках ГДЭ для соответствия генов особи конкретному экземпляру программы используется граф синтаксических правил (далее – ГСП), задающий в формальном виде синтаксис ЯП или нотацию для представления, каждый ген в котором задает один из выборов возможного передвижения по графу (например, хромосома ИК с текстом «*x* – *z*» для синтаксиса с идентификаторами «*x*, *y*, *z*» и математическими операциями «+, –, *, /» может состоять из генов «1, 2, 3», которые последовательно задают выбор 1-го идентификатора «*x*», 2-й операции «–» и 3-го идентификатора «*z*») – таким образом, программа задается с помощью пути по ГСП. Тривиальный и интуитивно понятный пример записи формального синтаксиса для приравнивания двух переменных в форме Бэкуса – Наура (далее – ФБН) [8] приведен в листинге 1, где префиксами до «::=» указаны номера правил синтаксиса, а символом «…» – незаконченность строки в виде аналогичного продолжения идентификаторов.

Листинг 1. Пример синтаксиса приравнивания двух переменных (в форме Бэкуса – Наура)

Listing 1. Example of Syntax for Equating Two Variables (in Backus – Naur Form)

```
1: assign ::= identifier operation identifier ;
2: identifier ::= ‘a’ | ‘b’ | ‘c’ | ... ;
```

Согласно синтаксису в Листинге 1, первой строкой задается правило приравнивания «assign» (в левой части), соответствующее (в правой части) двум идентификаторам «identifier» с операцией «operation» между ними. Во второй строке задаются возможные значения для идентификаторов

(символы «*a*», «*b*», «*c*» и т. д.) – т. е. альтернативные раскрытия правила. Представление данного синтаксиса в графической форме ГСП (в интересах компактности, для трех идентификаторов) представлено на рисунке 2.

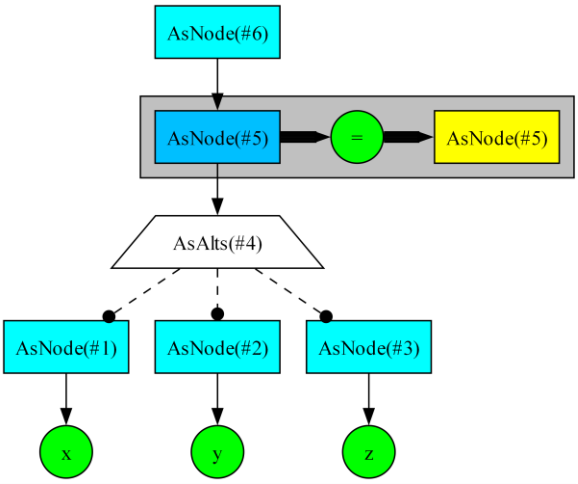


Рис. 2. Пример синтаксиса приравнивания двух переменных (в форме графа синтаксических правил)

Fig. 2. Example of Syntax for Equating Two Variables (in the Form of a Syntax Rules Graph)

Необходимо отметить, что хотя синтаксическое правило «assign» задается через 2 идентификатора, каждый из которых раскрывается тремя символами (см. листинг 1), в ГСП (см. рисунок 2) символы раскрываются только для первого идентификатора (узел «AsNode(#5)» синего цвета) с нисходящими ветками из дочернего узла «AsAlts(#4)»), а второй идентификатор представлен только одним узлом (узел «AsNode(#5)» желтого цвета), поскольку идентичен такому же узлу на 2 узла левее; такая запись существенно улучшает восприятие сложных графов, делая его визуально деревом (т. е. без циклов). Также несколько путей из узла «AsAlts(#4)» соответствуют тому, что из него продвижение по графу может пойти по нескольким путям – т. е. альтернативам.

Поскольку все передвижения по правилам в ФБН и ГСП, кроме достижения родительских узлов с альтернативами, идут по безусловному пути (например, после идентификатора «AsNode(#5)» обязательно следует символ «=» и еще один идентификатор «AsNode(#5)»), то основной вариативностью в генерации или «парсинге» ИК может быть один из выборов этих альтернатив; таким образом, именно порядковый номер альтернативы и был выбран в качестве гена соответствующей хромосомы экземпляра программы.

Важной особенностью ГДЭ, отличной от большинства решений на базе ГА, является переменность размера хромосомы, поскольку сама программа может состоять из различного количества конструкций (например, ИК может быть как тривиальным «$x = y$», так и комплексным математическим выражением с вызовом функций «$x = y * (z - \text{funct}(x, y, z))$»). При этом операции селекции и мутации в ГДЭ имеют достаточно сложную логику и состоят из качественно различных изменений формы и содержания программы (например, в ИК может как мутировать отдельный идентификатор или операция без изменения длины хромосомы, так и производиться принципиальная «перестройка» крупных конструкций условных переходов). Соответственно, задача ГДЭ считается решенной, когда получена программа, которая после преобразования в заданное представление тождественна эталонной (например, если был получен ИК, компилируемый в МК, побайтно совпадающий с эталонным, то, следовательно, этот ИК и является результатом декомпиляции). Такая идентичность результата компиляции ИК к эталонному МК заключается не только в гарантированности корректно проведенной ГДЭ, но и в том, что повторная сборка программы с устраненной в ИК уязвимостью позволит получить соответствующий МК, отличный от исследуемого лишь отсутствием этой уязвимости, не затрагивая иной функционал.

Сигнатурный поиск уязвимостей

Несмотря на то, что целевым предназначением ГРИ является отображение уязвимостей в каждом из представлений, дополнительные исследования показали [9], что поиск уязвимостей может производиться непосредственно на структурах ГДЭ путем сигнатурного анализа. Так, поскольку уязвимость в некотором представлении задается теми же конструкциями, что и основная программа, то ее сигнатура может быть задана, как часть пути по ГСП (например, деление на 0 в ГСП отражается, как последовательный переход на операцию деления, вторым операндом которой является константа с нулевым значением). А поскольку полная хромосома программы задается путем по ГСП, то ее часть (как подпоследовательность ген) может быть отожествлена с сигнатурой уязвимости.

Проблемные вопросы

Приведем далее основные проблемные вопросы (с префиксом «ПВ»), выявленные в результате исследования и развития ГРИ, а также опишем рекомендации (т. е. фактически обоснованные пути разрешения) для их устранения; для большей понятности часть вопросов будет касаться только ГДК, хотя путем обобщения они могут быть отнесены и к любым представлениям в процессе ГРИ.

ПВ_1. Формирование входного синтаксиса

Поскольку одним из входных параметром в ГДЭ является синтаксис ЯП, подходящий для обработки алгоритмами ГА, то возникает проблемный вопрос его формирования. Это может быть достигнуто

парсингом и преобразованием формальной записи синтаксиса, напрямую используемого в компиляторе (который, собственно, и применяется для получения из ИК соответствующего МК, сравниваемого с эталонным). В результате, синтаксис может быть переведен во внутренние структуры конкретной реализации ГДЭ и использоваться для построения и обхода ГСП.

ПВ_2. Восстановление неоптимального ИК

Исходя из того, что один и тот же ИК может соответствовать нескольким МК, его восстановленные вариации гипотетически имеют различную оптимальность (как по производительности, так и по лаконичности). Например, три таких ИК, как «$x = y$», «$x = y + 0$» и «$x = 2 * y - y$», идентичны с позиции результатов своей работы и теоретически могут после компиляции привести к одному МК. Впрочем, во-первых, без применения опций оптимизации 2-й и 3-й ИК скорее всего не будут упрощены компилятором и приведут к излишним инструкциям сложения и умножения, что сделает их существенно отличными от эталонного МК. А, во-вторых, добавление и учет метаинформации в синтаксисе ЯП может снизить появление излишних конструкций в ИК (например, невозможность получения после скрещивания или мутации выражений со сложением, где одним из аргументов является 0).

ПВ_3. Восстановление слабо интерпретируемого ИК

Крайне интересным с научной и практической точки зрения является абсолютно корректное получение ИК, который, хотя в точности и соответствует эталонному МК, но его понимание Экспертом является сложной задачей из-за эволюционного получения такой особи, логика работы которой (заданная ее хромосомой, отраженной в элементах ИК) строится на иных принципах, нежели человеческая логика. Данная проблема характерна для искусственных нейронных сетей, которые также имеют слабую интерпретируемость [10]. С этой позиции, одним из положительно-побочных эффектов области ГДЭ может стать развитие области искусственно-интеллектуальной логики, качественно отличной от человеческой, которая также получена эволюционным способом, но в синтетической среде (как совокупности «выживания» особей ИК, стремящихся к приспособленности в виде близости к эталонному МК, как некоторому «условному прообразу цифрового идеала»). Повышения же интерпретируемости можно добиться как модификацией ГСП, так и дополнительной алгоритмической обработкой ИК (в том числе, исходя из корректировок Эксперта).

ПВ_4. Попадание в локальный максимум

Одним из проблемных вопросов любого ГА считается возможность попадания в так называемый локальный максимум (или минимум) [11], суть которой заключается в нахождении псевдооптимального решения. В контексте ГДЭ это означает, что будет сформировано поколение подобных друг другу экземпляров ИК, которые компилируются в МК, близкий, но не тождественный эталонному. При этом операции скрещивания и мутации не позволяют выйти из данной ситуации, поскольку стенки такой локальной «ямы» слишком велики (т. е. удаленность функции приспособленности для ИК, более близкого к истинному решению, окажется критичной для ГА). Тем не менее для решения данного вопроса существует ряд техник, таких как оптимизация параметров ГА (например, увеличение «силы» мутации) или применение искусственного интеллекта для контроля качества популяции, чтобы избежать «застревания» эволюции).

ПВ_5. Рост количества итераций ГДЭ от размера ГСП

Размер ГСП (т. е. количество узлов, связей и т. п.) может критически сказаться на количестве итераций эволюции, что негативно повлияет и на оперативность работы ГДЭ. В итоге время решения оптимизационной задачи восстановления программы может оказаться выше предельно допустимого. Для качественного ускорения эволюции путем анализа МК имеет смысл использовать не весь синтаксис ЯП (на альтернативах которого определены гены особей), а выбрать его минимально необходимое подмножество – подграф синтаксических правил которого окажется существенно меньше основного графа. Например, если в МК нет инструкций условного перехода (соответствующих, например, конструкциям «if–else» в ЯП C), то нет смысла использовать соответствующие правила и при выполнении операций скрещивания и мутации.

ПВ_6. Рост количества итераций ГДЭ от вложенности синтаксиса

Наличие в синтаксисе ЯП конструкций, описывающих сложные вложенные выражения, будет иметь такое же негативное влияние на длительность эволюции, как и размер ГСП. Так, например, ИК вложенного сложения «$x + (x + (x + (x + x)))$» может быть записан с помощью синтаксических правил так, как показано в листинге 2.

Листинг 2. Пример синтаксиса выражения с вложенным сложением (в форме Бэкуса – Наура)

Listing 2. Example of Syntax for Expression with Nested Addition (in Backus – Naur Form)

```
1: expression ::= identifier ‘+’ identifier_or_expression ;
2: identifier_or_expression ::= ‘x’ | ‘(’ expression ‘)’ ;
```

ГСП для такого синтаксиса приведен на рисунке 3; во второй строке узлов указаны ссылки на соответствующие правила. Вложенность синтаксиса, соответствующая рекурсии его правил, в данном случае заключается в том, что «expression» (или узел «AsNode(#4)») выражается через правило «identifier_or_expression» (узел «AsNode(#2)»), вто-

рая альтернатива которого (узел «AsNode(#6)», дочерний к «AsAlts(#1)») содержит это же правило «expression». Соответственно, алгоритмы ГДЭ гипотетически могут тратить значительное количество эволюционных итераций на обход данной рекурсии в глубину даже для выражений без больших вложенностей. Решением этого проблемного вопроса может стать упрощение синтаксиса (и, соответственно, ГСП) с помощью ограничения рекурсивности путем ее «распаковки» в аналогичные последовательности простых выражений. Например, одна строка ИК с комплексным выражением «$w = x + (y + z)$» может быть записана, как две строки с приравниванием промежуточных значений к временны́м переменным: «$t1 = y + z$; $w = x + t1$». Значит, для записи второго варианта ИК рекурсия для указания вложенных выражений не требуется. Естественно, полностью от рекурсий отказаться не удастся, поскольку любой ИК программы представляет собой теоретически бесконечную последовательность выражений (которые зачастую соответствуют одной строке ИК); однако эволюционный подбор такой циклической по ГСП конструкции является более решаемой задачей для ГДЭ, поскольку каждое вложенное выражение ИК на этапе компиляции, как правило, разворачивается в последовательность простых, оперирующих промежуточными значениями и временны́ми переменными.

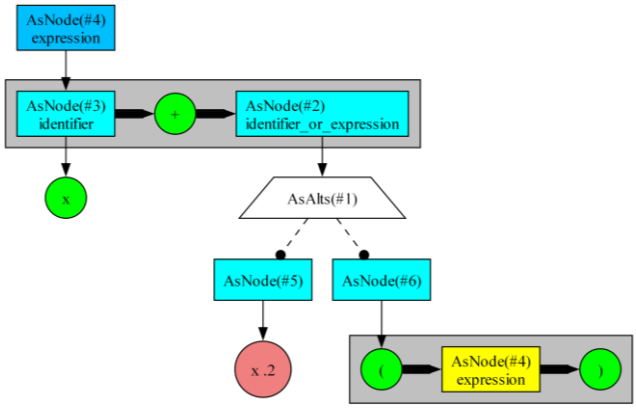


Рис. 3. Пример синтаксиса выражения с вложенным сложением (в форме графа синтаксических правил)

Fig. 3. Example of Syntax for Expression with Nested Addition (in the Form of a Syntax Rules Graph)

ПВ_7. Сложность подбора идентификаторов

Сложность подбора идентификаторов в ИК заключается в том, что они уже отсутствуют в МК и, соответственно, не могут быть из него восстановлены. Также идентификаторы, как правило, отсутствуют и в синтаксисе ЯП, поскольку процесс разбора имени переменной типовым компилятором происходит на ранней фазе парсинга кода – лексическим анализатором [12], который передает последующему синтаксическому анализатору лишь тип токена – идентификатор. Впрочем, само название не имеет принципиальной важности как для ГДК, так и для дальнейшего анализа ИК Экспертом. Также, поскольку необходимым для решения текущей оптимизационной задачи является получение ИК, в точности компилируемого в эталонный МК, то важно восстановить именно зависимость данных межу переменными, а не сами их имена. Таким образом, в синтаксис возможно введение некоторого разумного пула альтернативных имен переменных, среди которых ГА и будет выбирать необходимую.

Так, например, для небольшого размера ассемблерного кода (далее – АК) достаточным может оказаться наличие в ИК всего пяти переменных, задаваемых следующим синтаксическим правилом:

identifier ::= ‘var1’ | ‘var2’ | ‘var3’ | ‘var4’ | ‘var5’.

Также, используя синтаксис АК, в котором четко указано место имени идентификатора, возможно предварительно провести разбор его текста, определить используемые идентификаторы, модифицировать синтаксис ИК и, уже используя его, провести ГДЭ.

ПВ_8. Сложность подбора числовых константных значений

Одним из сложнейших проблемных вопросов в ГДЭ по формальному синтаксису ЯП является подбор числовых константных значений, которые для 32-х битных систем могут принимать огромные значения – от 0 до 4294967295. Естественно, даже с учетом мутаций подбор таких значений займет недопустимо большое время (а наличие дробных чисел в программе, зачастую представляемых посредством целых в специальном формате, еще существеннее усложнит данную задачу). Разрешение данной ситуации может лежать в плоскости следующих двух способов.

Первый способ связан с тем, что учет частоты используемых константных значений в типовых программах позволит изначально выбирать те, которые с наибольшей вероятностью являются верными; данная статистика уже была собрана ранее и определила Топ-10 таких констант – 0, 1, 2, 3, 4, 10, 5, 8, 16, 7 [13]. Естественно, «угадать» абсолютно любую константу вряд ли окажется возможным, что несколько ограничивает область применения ГДК.

Вторым способом является анализ АК или МК на предмет присутствия в нем константных значений, которые логичным образом должны присутствовать и в ИК (по аналогии с разрешением ПВ_7); например, если в АК присутствуют выражения, оперирующие числами 3, 7 и 11, то и в ИК константами будут именно они. Таким образом, альтернативы в используемом синтаксисе ЯП (и, соответственно, ГСП) могут состоять лишь из ведущих к узлам с этими числами: number ::= ‘3’ | ‘7’ | ‘11’.

ПВ_9. Сложность подбора строковых константных значений

Еще более сложной задачей, чем подбор идентификаторов и числовых константных значений, является восстановление текстовых строк, используемых в программе, поскольку они могут состоять из огромного количества символов, подбор которых займет практически неограниченное время. Частично данный проблемный вопрос может быть разрешен аналогичным для подбора числовых констант образом. Например, в Топ-50 наиболее часто используемых строк входят следующие: «%d», «%d\n», «\n» и «""». При этом анализ бинарной формы программы на предмет наличия в ней строк (хранящихся, допустим, в секции «.rodata» для выполняемого файла формата ELF [14]), а также соответствующая модификация ГСП, позволит качественно ускорить деэволюцию МК.

ПВ_10. Сложность восстановления группы функций вместо ИК одной

Несмотря на то, что теоретические исследования и практические эксперименты показали возможность ГДЭ отдельных участков МК, однако его полноценное применение для целой программы, состоящей из набора функций (хотя более точно говорить о подпрограммах), требует дополнительного исследования по данной ветке. Причина этого заключается в том, что отображение функций в синтаксисе ЯП, а также в МК и АК программы, является более сложным, чем подобное отображение конструкций внутри нее. Так, помимо разделения программы на функции, каждая из них имеет аргументы с разными способами передачи (через регистры, стек или глобальную память) и опционально возвращаемые значения, может вызывать другие функции, в том числе по указателю (ссылке) и т. п. Базовым решением вопроса целесообразно рассмотреть применение соответствующих методов детектирования как самих участков функций, так и информации об их входных и выходных параметрах; что, впрочем, снизит общую инвариантность ГДЭ.

Другим решением может стать введение нового (возможно, промежуточного) представления между ИК и МК, которое бы представляло собой некоторый граф вызовов функций и их декларации. Тогда сам ГДЭ вначале будет восстанавливать программу в этом представлении, оставляя без изменений МК внутри функций, а затем уже производить деэволюцию каждой отдельной функции.

ПВ_11. Генерация первоначальной популяции

Первоначальная популяция, как и ее размер, хотя и не имеет решающее значение, однако существенно влияет на скорость проведения деэволюции программы, поскольку, чем ближе ее особи окажутся к искомой эталонной, тем быстрее сойдется ГА. В этой ситуации случайная генерация особей не позволит соптимизировать ГДЭ. Возможным решением может быть распознавание шаблона программы в текущем представлении (например, с применением машинного обучения) и генерация первоначальной популяции в соответствии с ним. Также с помощью существующих методов возможно определение ее оптимального размера [15].

ПВ_12. Выбор первоначального размера хромосомы

Размер хромосомы можно считать таким же важным оптимизационным фактором, как и гены представителей первоначальной популяции, поскольку чем сильнее отличается количество ее ген от того, которое позволяет получить эталонную особь (т. е. приводит к завершению ГДЭ), тем более долгий путь придется пройти эволюции для «увеличения» или «уменьшения» длины хромосомы. Так, например, если эталонный МК получен из ИК, который задается хромосомой из 10 ген, а в первоначальной популяции были особи с 1 и 20 генами, то количество итераций ГДЭ в среднем будет больше, чем если бы хромосомы такой популяции содержали бы 9 или 11 (а в идеале, 10) ген. Для предсказания же их количества возможно использовать зависимость (очевидно, существующую) между ИК и получаемым из него МК; что уже было получено ранее [16].

ПВ_13. Выбор частот скрещивания и мутации

Выбор параметров ГА, таких, как частота скрещивания пары особей или мутации одной из них (как, впрочем, и применение той или иной разновидности этих операций) очевидно оказывает влияние на получение более «удачного» поколения и, следовательно, общее время работы ГДЭ. Как правило, такие параметры выбираются эмпирически и, гипотетически, будут иметь схожие значения для типовых синтаксисов или шаблонов программ. Следовательно, опыт предыдущих восстановлений ИК из группы может быть применен и для ГДЭ других подобных ИК. Впрочем, это требует отдельного теоретического исследования и практических экспериментов для разнородных входных данных.

ПВ_14. Влияние качества функции приспособленности на сходимость

Одним из решающих факторов успешного эволюционирования особей в ГДЭ является качество функции приспособленности, которая определяет близость программ, полученных преобразованием (в случае ИК – компиляцией) экземпляров популяции предыдущего представления к эталонной особи текущего представления. При этом точные критерии близости сложно определимы, а подобная задача принципиально не рассматривалась другими учеными. Однако для проверки Концепции, сравнение двух программ в представлении АК осуществлялось с помощью авторской метрики,

принимающей на вход список из двух строк, состоящих из последовательности символов [17]; метрика также способна учитывать отдаленность строк и символов от начала содержащих их множеств, что отражает соответствие последовательности логики функционирования в ИК и АК. Данная метрика с достаточной чувствительностью позволяет оценивать, как близость одной текстовой строки к другой, так и одного их упорядоченного списка к другому. Также, качественным развитием механизма является непосредственный учет в сравнении синтаксиса текущего представления, которым в случае АК может являться TASM, NASM, MASM, FASM, YASM, ASM-51 и др.

Так, если имеются две следующие строки АК:

```
mov eax, DWORD PTR _x$[ebp]  # занесение в
регистр EAX значения переменной _x
```

и

```
add edx, DWORD PTR _x$[ebp]  # добавление к
регистру EDX значения переменной _x
```

то посимвольное сравнение будет не совсем точным, поскольку более существенное отличие этих строк в том, что используются принципиально различные процессорные инструкции – приравнивание (MOV) и добавление (ADD). Такую разницу возможно определить путем учета синтаксиса АК, в котором строчки будут определяться различными подграфами соответствующего ГСП.

ПВ_15. Время-затратность вычисления функции приспособленности

Практически в любой реализации Концепции наиболее длительной по времени операцией является вычисление функции приспособленности [18], поскольку она требует наличие МК, соответствующего ИК, согласно генам особи. Для этого производится ресурсозатратный (не только по времени, но и по аппаратным ресурсам рабочей станции) вызов компилятора программы. Данная ситуация отличается от классической, в которой зачастую эта функция производит ряд несложных аналитических действий, хорошо распараллеливаемых. Впрочем, существенного ускорения компиляции можно достигнуть тремя способами.

Во-первых, ведение базы уже скомпилированных экземпляров ИК (например, в форме словаря, где ключом является последовательность ген ИК, а значением – приспособленность его МК) предотвратит повторное вычисление функции.

Во-вторых, компиляция группы ИК (так называемый, пакетный режим) будет несколько быстрее, поскольку ряд операций (запуск процесса, инициализация компилятора и т. п.) вызовутся 1 раз для всей группы. При этом компиляцию можно вызывать для всей популяции, т. к. приспособленность их особей требуется только перед операцией селекции – т. е. один раз за эпоху эволюции.

И, в-третьих, наличие открытого ИК утилиты компиляции позволит внедрить ее алгоритмы напрямую в ГДЭ, что еще более снизит накладные расходы.

Первые 2 способа были реализованы на практике в авторском Прототипе и показали свою эффективность.

ПВ_16. Идентификация средства преобразования особи

При проведении ГРИ программы, информация о которой отсутствует (например, уничтожена злоумышленником или иными деструктивными воздействиями), определение средства ее преобразования из предыдущего представления в текущее (для сравнения особей с эталонной) является важным проблемным вопросом. В ином случае, например, когда компилятор ИК или его опции были выбраны некорректно, ГДЭ может осуществляться критически высокое время (а в ряде случаев, и не завершиться вовсе). Однако существуют исследовательские разработки, которые позволяют идентифицировать такие средства по метаинформации в программах [19].

ПВ_17. Идентификация синтаксиса представления

Аналогично идентификации средства преобразования особей, требуется определение синтаксиса текущего представления для более корректного выбора или настройки функции приспособленности. Так, например, в случае восстановления ИК из МК необходимо понимание процессорной архитектуры. Однако современные наработки с достаточно большой эффективностью позволяют создавать «цифровые портреты» (на основании специфики распределения байтов МК) для каждой такой архитектуры, обеспечивая, тем самым, ее идентификацию (что было продемонстрировано в авторских [20, 21] и иных [22] научно-практических исследованиях).

ПВ_18. Использование АК вместо МК

Достаточно большая часть как теоретических исследований, так и практических реализаций ГДЭ проведена в интересах восстановления ИК по его АК, поскольку использование вместо этого в качестве эталонного классического МК является одним из проблемных вопросов. Хотя получение АК из МК и осуществляется в полной мере так называемыми утилитами дизассемблирования [23], получаемый ими АК все же будет отличен от такого же, сгенерированного при непосредственной компиляции ИК. Так, например, ИК функции сложения двух аргументов, представленный в листинге 3 в процессе компиляции преобразуется в АК в листинге 4, хотя дизассемблирование в продукте IDA Pro полученного МК дает АК, представленный в листинге 5.

Листинг 3. Исходный код функции сложения двух аргументов

Listing 3. Source Code for the Function Adding Two Arguments

```
int f(int x, int y) {
  return x + y;
}
```

Листинг 4. Ассемблерный код функции сложения двух аргументов (после компиляции исходного кода)

Listing 4. Assembly Code of the Two Arguments Addition Function (After Compilation the Source Code)

```
_x$ = 8
_y$ = 12
_f  PROC
; Line 1
  push ebp
  mov ebp, esp
; Line 2
  mov eax, DWORD PTR _x$[ebp]
  add eax, DWORD PTR _y$[ebp]
; Line 3
  pop ebp
  ret 0
_f  ENDP
```

Листинг 5. Ассемблерный код функции сложения двух аргументов (после дизассемблирования машинного кода)

Listing 5. Assembly Code of the Two Arguments Addition Function (After Disassembling the Machine Code)

```
_f proc near
arg_0 = dword ptr 8
arg_4 = dword ptr 0Ch

push ebp
mov ebp, esp

mov eax, [ebp + arg_0]
add eax, [ebp + arg_4]

pop ebp
retn

_f  endp
_text$mn ends
end
```

Впрочем, отличия таких АК (см. листинги 4 и 5) носят несущественный характер – формат строк с инструкциями практически идентичен за исключением метаинформации, создаваемой утилитами (пометки о границах функций, аргументах и т. п.), доступа к значению переменных (DWORD PTR вместо конструкции «[…]») и самих имен переменных (исходные «*_x*» и «*_y*» вместо автоматически сгенерированных «arg_0» и «arg_4»). Соответственно, поскольку оба АК в точности соответствуют одному МК, то и инструкции в их строках идентичны по содержанию, а отличия в формах могут быть скорректированы достаточно тривиальным образом. Потеря же имен переменных при получении АК из МК не будет критичной, поскольку конкретные их идентификаторы не имеют существенного значения для успешности ГДЭ.

ПВ_19. Отсутствие формальных синтаксисов ряда представлений

Следуя масштабности описанной Концепции, она гипотетически предназначена для получения из МК не только ИК или алгоритмов, но и архитектуры программы, ее концептуальной модели или даже самой идеи – например, в форме текстового описания сущности целой программы, ее отдельных функций и назначения. Тем не менее, наиболее распространенными и проработанными синтаксисами представлений на сегодняшний день остаются 3 следующих – МК, АК и ИК; хотя формализация алгоритмов (как более абстрактного и человекоориентированного представления ИК) в форме блок-схем или псевдокода также применяется. Тем не менее, судя по общему усложнению области программной инженерии, а также внедрению в этот процесс искусственного интеллекта, можно спрогнозировать появление формализации других представлений программы (за счет их формального синтаксиса или иных моделей), что повлечет за собой и возможность проведения соответствующей ГДЭ. С этой позиции, ГРИ представляет собой перспективное направление поиска уязвимостей программ в тех представлениях, где они были заложены.

ПВ_20. Проверка Концепции ГДЭ на ограниченном количестве представлений

Исходя из того, что формальные представления и средства преобразования на сегодняшний день наиболее развиты лишь для двух (точнее трех) представлений – ИК и МК, преобразуемого в АК, проверка Концепции на остальных носит больше теоретический характер. Однако качественная подобность всех представлений и создание алгоритмов ГДЭ, как независимых (в пределе) от специфики программ, позволяют полагаться на работоспособность Концепции и в более широких границах применения. Так, например, если будет создан полноценный синтаксис алгоритмов программы (как в форме блок-схем, так и псевдокода), позволяющий по ним генерировать ИК за счет подбора альтернатив, то ГДЭ между этими двумя представлениями будет возможна также, как и ГДК. В качестве близкого примера можно привести графический язык программирования логических контроллеров (FBD, *аббр. от англ.* Function Block Diagram) [24], программы на котором как раз и преобразуются в псевдо ИК или АК. Проведение ГДЭ таких графических блок-схем можно рассматривать в качестве одной из ближайших целей обоснования Концепции для ГРИ МК в более высокоуровневые формы.

Также стоит отметить, что на первый взгляд узкая задача по восстановлению ИК из МК или АК является крайне принципиальной с точки зрения ИБ, поскольку экспертный (а в ряде случае, и автоматический) анализ этих представлений качественно отличен с позиции эффективности – бинарная форма практически не подходит для ручного поиска уязвимостей, а соответствующие методики анализа по ИК существуют и давно используются. При этом в области программной инженерии основная работа заключается именно в создании ИК

и его преобразовании в МК, который уже непосредственно выполняется на устройствах.

ПВ_21. Зависимость сигнатур уязвимостей от синтаксиса

Существенным ограничением широкого применения предложенной сигнатурной записи уязвимостей является их зависимость от конкретного синтаксиса представления – т. к. сигнатура описывается начальным узлом и выбором альтернатив по заданному ГСП. Однако даже такую запись можно считать более расширенной, чем классическая, когда сигнатура задает строгую последовательность байт или инструкций в МК для конкретного процессора выполнения. Так, например, типовое выявление вредоносного кода в МК, собранного под N процессорных архитектур, потребовало бы наличия такого же количества сигнатур. Использование же ГДЭ позволяет восстановленный из них ИК записать с помощью одной хромосомы (соответствующей пути на выбранном ГСП), что потребует наличия лишь одной сигнатуры уязвимости. Аналогичная ситуация будет и в случае создания уязвимости на одном из N языков программирования. Таким образом, гипотетически можно предположить востребованность в создании единого (или их ограниченной группы) синтаксиса, адаптированного для отображения на нем сигнатур уязвимостей и деэволюции в них МК программы для большого количества процессорных архитектур.

ПВ_22. Отсутствие учета семантики и динамики при поиске уязвимостей

Очевидно, что сигнатура уязвимостей задает исключительно ее синтаксические особенности (например, последовательностью конструкций ЯП) и не позволяет выявлять более сложные случаи. Так, два следующих ИК потенциально приводят к делению на 0:

1) «$y = x / 0$»;
2) «if (z == 0) { $y = x / z$; }».

Первый ИК выявляется синтаксическим анализом (по факту наличия константы «0» после оператора деления), а второй – семантическим или динамическим (условие будет выполняться только при нулевом значении «z», что и приведет к делению на 0). Впрочем, сигнатуры по ГСП изначально не были предназначены для выявления более сложных «логических» уязвимостей, что следует из ограничений сигнатурного анализа (по крайне мере, его статической формы). Тем не менее, гипотетически можно развить ГДЭ и для восстановления семантики кода, например, путем введения графа семантических правил, сигнатур на нем и необходимого набора алгоритмов.

ПВ_23. Неполный охват обнаруживаемых уязвимостей

Следуя отсутствию «глубоких» алгоритмов ГДЭ анализа уязвимостей, определяемых внутренней логикой функционирования программы (а не ее внешней синтаксической формой), необходимым условием выявления можно считать их локализацию в коде. Так, например, если часть одной уязвимости расположена в начале тела функции, часть – в середине, а часть – в конце, то ее запись через сигнатуру (как последовательность узлов ГСП) вряд ли будет возможна. Однако частичным разрешением данного проблемного вопроса может быть применение более сложных форм сигнатур, построенных, например, как шаблоны, определяющие лишь необходимые части синтаксиса. Впрочем, без учета семантики или динамики выполнения кода (следуя ПВ_22), даже применение сигнатурных шаблонов будет достаточно ограниченным.

ПВ_24. Частичная инвариантность алгоритмов от синтаксисов представлений

Обеспечение полной инвариантности алгоритмов ГДЭ от синтаксических и иных особенностей программы во всех представлениях, хотя и является одной из теоретических особенностей Концепции, тем не менее имеет определенные трудности в практической реализации. Так, выбор размера хромосом особи требует предварительного определения зависимости между размерами программ в ближайших представлениях; предсказание константных значений для мутационного подбора – аналогичного составления статистики по частоте их использования или применения иных специализированных методов (например, как было указано ранее – выявление в АК констант, которые затем должны перебираться в ИК); адаптация существующих синтаксисов представлений – частичного учета соответствующих им семантических и иных правил; развитие поиска уязвимостей – отражение в их сигнатурах большего количества метаинформации о программе и т. д. Впрочем, повышение инвариантности может быть обеспечено оптимизационными и иными способами, которые имеют лишь технические сложности в реализации, однако не нарушают общую концепцию и не снижают ее обоснованность. Так, например, внедрение моделей и методов машинного обучения, которые после каждой компиляции ИК в МК будет обучаться «понимать», какая последовательность ген для каких узлов ГСП приводит к каким синтаксическим конструкциям в машинных инструкциях, гипотетически позволит существенно снизить зависимость алгоритмов ГДЭ от специфики программ их представлений.

ПВ_25. ГДЭ оптимизированной и обфусцированной программы

Применение при сборке программы различных техник оптимизации кода (например, по скорости работы или размеру образа МК) приводит к некоторому усложнению отображения его логики в получаемом представлении и, как результат, затруднению всего ГДЭ. Например, все функции могут быть «слиты» в одну для уменьшения накладных расходов на их вызов. Применение же техник обфускации, изначально предназначенных для запутывания кода, качественно усложнит проведение ГДЭ [25]. Впрочем, это является общей проблемой реверс-инжиниринга ПО. Однако большой авторский практический опыт позволяет утверждать, что достаточно часто программы, применяемые в критических областях и устройствах, собираются без использования таких техник, поскольку риск случайных ошибок в коде, возникающих от их применения, оказывается выше эффекта снижения размера, увеличения скорости или изменения иных характеристик программы. В качестве же гипотетического разрешения самого проблемного вопроса можно рассмотреть возможность доработки алгоритмов ГДЭ и настройку их параметров, а также соответствующую адаптацию ГСП, применимых именно для такого нетипового МК.

Систематизация проблемных вопросов

Проведем систематизацию всех приведенных проблемных вопросов с позиции основных путей их устранения (таблица 1), указывая для этого в качестве критериев часть ГРИ для доработки:
«К.» – концепция (например, введение новых этапов или изменение взаимосвязи существующих);
«А.» – алгоритмы (в том числе разработка новых);
«П.» – представления (включая синтаксис ЯП и ГСП);
«У.» – уязвимости (например, их сигнатуры).

Значение же уровня требуемой доработки (и их балльную оценку) обозначим следующим образом:
« » – отсутствует (0 баллов);
«+/–» – количественная или частичная (0,5 балла);
«+» – качественная или полная (1 балл).

Просуммируем эти значения для каждой части ГРИ (в последней строке таблицы), что позволит оценить наиболее «проблематичные» и требующие внимания из них. Так, например, указание для проблемного вопроса по критерию «А.» значения «+/–» говорит о том, что для его разрешения требуется подстройка параметров алгоритмов.

Анализ критериальной систематизации проблемных вопросов (см. таблицу 1) позволяет сделать следующие выводы. Во-первых, Концепция показала свою устойчивость или обоснованность (при минимальном суммарном количестве баллов – 1,0).

ТАБЛИЦА 1. Систематизация проблемных вопросов генетического реверс-инжиниринга программы с позиции путей их устранения

TABLE 1. The Problematic Issues Systematization of a Program Genetic Reverse Engineering from the Standpoint of Ways to Eliminate Them

Проблемный вопрос	Части ГРИ для изменения			
	К.	А.	П.	У.
ПВ_1. Формирование входного синтаксиса			+	
ПВ_2. Восстановление неоптимального ИК			+/–	
ПВ_3. Восстановление слабо интерпретируемого ИК			+/–	
ПВ_4. Попадание в локальный максимум		+/–		
ПВ_5. Рост количества итераций ГДЭ от размера ГСП			+/–	
ПВ_6. Рост количества итераций ГДЭ от вложенности синтаксиса			+/–	
ПВ_7. Сложность подбора идентификаторов		+	+/–	
ПВ_8. Сложность подбора числовых константных значений		+	+/–	
ПВ_9. Сложность подбора строковых константных значений		+	+/–	
ПВ_10. Сложность восстановления группы функций вместо ИК одной	+/–	+		
ПВ_11. Генерация первоначальной популяции		+/–		
ПВ_12. Выбор первоначального размера хромосомы		+		
ПВ_13. Выбор частот скрещивания и мутации		+/–		
ПВ_14. Влияние качества функции приспособленности на сходимость		+		
ПВ_15. Время-затратность вычисления функции приспособленности		+		
ПВ_16. Идентификация средства преобразования особи		+		
ПВ_17. Идентификация синтаксиса представления		+		
ПВ_18. Использование АК вместо МК		+	+/–	
ПВ_19. Отсутствие формальных синтаксисов ряда представлений			+	
ПВ_20. Проверка Концепции ГДЭ на ограниченном количестве представлений			+	
ПВ_21. Зависимость сигнатур уязвимостей от синтаксиса			+/–	+/–
ПВ_22. Отсутствие учета семантики и динамики при поиске уязвимостей		+/–	+	+
ПВ_23. Неполный охват обнаруживаемых уязвимостей		+/–		+
ПВ_24. Частичная инвариантность алгоритмов от синтаксисов представлений	+/–	+/–	+/–	+/–
ПВ_25. ГДЭ оптимизированной и обфусцированной программы		+/–	+/–	
Всего	1,0	13,5	9,5	3,0

Поскольку ни один из проблемных вопросов не требует ее принципиального пересмотрения – отсутствует необходимость в качественной ее доработке (т. е. отсутствует значение «+» в столбце

«К.»). Частичное же изменение концепции (следуя ПВ_10 и ПВ_24) на данный момент представляется решаемой задачей, требующей, однако, проведения дополнительных научно-практических изысканий.

Во-вторых, наиболее требуемыми доработки могут считаться алгоритмы (имеющие максимальное суммарное количество баллов – 13,5), что вполне закономерно, поскольку за их счет происходит расширение и / или улучшение имеющегося функционала до уровня, необходимого для проведения ГДЭ. На 2-м месте по рейтингу суммарного количества баллов (равного 9,5) расположена доработка представлений, что, хотя является и трудоемкой из-за некоторой монотонности, но вполне решаемой задачей (как вручную, так и применением автоматических средств трансформации).

В-третьих, доработка уязвимостей в части их сигнатур позволит разрешить соответствующую немногочисленную группу проблемных вопросов (с суммарным количеством баллов в 3,0). Наиболее же масштабным с позиции изменения частей ГРИ может считаться ПВ_24 (0,5 балла по каждому критерию), что объясняется возможностью повышения инвариантности каждой из четырех указанных частей ГРИ без каких-либо качественных изменений уже полученных авторских решений.

Заключение

Проведенное исследование является заключительной частью более крупного и основополагающего, посвященного методологии ГРИ программ в интересах поиска в них уязвимостей. Приводятся 25 основных проблемных вопросов, выявленных при переходе от концепции ГРИ (состоящей из отдельных ГДЭ) к ее непосредственной реализации в виде Прототипа для проведения ГДК. Для каждого такого вопроса указан путь его разрешения, что позволяет говорить об отсутствии «научно-практического тупика» и в основном исследовании.

Основным полученным научным результатом является систематизация выделенных проблемных вопросов с позиции необходимых доработок частей ГРИ с использованием балльных оценок. Новизна результата заключается в том, что большинство этих вопросов подняты впервые, что, впрочем, объясняет оригинальность самого ГРИ.

Теоретическая значимость результата состоит в том, что каждый из затронутых вопросов, фактически, является отправной (а, точнее, проблемно-постановочной) точкой для начала нового полноценного исследования, проведение которого позволит получить новые научно-практические результаты, выходящие за рамки авторского ГРИ. Так, например, разрешение ПВ_12 разовьет достаточно редко используемое направление ГА, оперирующее переменной длиной хромосом; а изучение ПВ_22 может привести к созданию метасигнатур уязвимостей, которые, с одной стороны, не зависят от ЯП и процессора выполнения программы, а с другой стороны, учитывают логику ее функционирования; исследование же ПВ_3 гипотетически откроет новые парадигмы программирования [26], на данный момент не адаптированные для восприятия человеком.

Практическая же значимость результатов заключается в том, что для каждого такого вопроса указано общее направление его разрешения, не только теоретически, но и путем создания соответствующего практического инструментария.

Продолжением работы может стать выбор и разрешение наиболее «интересных» проблемных вопросов, в том числе, другими исследователями.

Список источников

1. Гетьман А.И., Горюнов М.Н., Мацкевич А.Г., Рыболовлев Д.А. Сравнение системы обнаружения вторжений на основе машинного обучения с сигнатурными средствами защиты информации // Труды Института системного программирования РАН. 2022. Т. 34. № 5. С. 111–126. DOI:10.15514/ISPRAS-2022-34(5)-7. EDN:LDJOUO
2. Израилов К.Е., Гололобов Н.В., Краскин Г.А. Метод анализа вредоносного программного обеспечения на базе Fuzzy Hash // Информатизация и связь. 2019. № 2. С. 36–44. EDN:DUIUJM
3. Израилов К.Е. Концепция генетической декомпиляции машинного кода телекоммуникационных устройств // Труды учебных заведений связи. 2021. Т. 7. № 4. С. 95–109. DOI:10.31854/1813-324X-2021-7-4-95-109. EDN:AIOFPM
4. Израилов К.Е. Концепция генетической деэволюции представлений программы. Часть 1 // Вопросы кибербезопасности. 2024. № 1(59). С. 61–66. DOI:10.21681/2311-3456-2024-1-61-66. EDN:CBCKRF
5. Израилов К.Е. Концепция генетической деэволюции представлений программы. Часть 2 // Вопросы кибербезопасности. 2024. № 2(60). С. 81–86. DOI:10.21681/2311-3456-2024-2-81-86. EDN:JUBPML
6. Скобцов Ю.А. От генетических алгоритмов к метаэвристикам // Информатика и кибернетика. 2021. № 1-2(23-24). С. 101–107. EDN:ILCTUW
7. Тотухов К.Е., Романов А.Ю., Лукьянов В.И. Исследование эффективности работы генетических алгоритмов с различными методами скрещивания и отбора // Электронный сетевой политематический журнал "Научные труды КубГТУ". 2022. № 6. С. 98–109. EDN:DPRWIJ
8. Емельянов А.А. Рефлексивная распознающая грамматика // Вестник Волжской государственной академии водного транспорта. 2016. № 46. С. 23–32. EDN:VPBBLP
9. Буйневич М.В., Израилов К.Е. Сигнатурный поиск уязвимостей в машинном коде на базе генетической декомпиляции // Защита информации. Инсайд. 2025. № 2(122). С. 2–11. (в печати)

10. Микулик И.И., Уткин Л.В., Голубева И.Э. Разработка и исследование методов локальной интерпретации сиамской нейронной сети на основе объяснительного интеллекта // Математические методы в технике и технологиях – ММТТ. 2020. Т. 10. С. 88–91. EDN:SBFYYB

11. Силенко Д.И., Лебедев И.Г. Алгоритм глобальной оптимизации, использующий деревья решений для выявления локальных экстремумов // Проблемы информатики. 2023. № 2(59). С. 21–33. DOI:10.24412/2073-0667-2023-2-21-33. EDN:MLGKOX

12. Пырнова О.А., Никоноров Д.П., Шарифуллина А.Ю. Разработка статического анализатора программного кода // Научно-технический вестник Поволжья. 2023. № 12. С. 522–525. EDN:AVFOIE

13. Израилов К.Е. Исследование распределения константных значений в исходном коде программ на языке C // Труды учебных заведений связи. 2024. Т. 10. № 5. С. 119–129. DOI:10.31854/1813-324X-2024-10-5-118-128. EDN:KARAVM

14. Hu W., Chen T., Zhang N., Ma J. Adjust ELF Format for Multi-core Architecture // Proceedings of the International Conference on Electronic Computer Technology (Macau, China, 20–22 February 2009). IEEE, 2009. PP. 388–391. DOI:10.1109/ICECT.2009.73

15. Цыганков В.А., Шабалина О.А., Катаев А.В. Исследование воздействия размера популяции на быстродействие генетического алгоритма // Известия ЮФУ. Технические науки. 2024. № 3(239). С. 168–176. DOI:10.18522/2311-3103-2024-3-168-176. EDN:IAFWKU

16. Израилов К.Е. Прогнозирование размера исходного кода бинарной программы в интересах ее интеллектуального реверс-инжиниринга // Вопросы кибербезопасности. 2024. № 4(62). С. 13–25. DOI:10.21681/2311-3456-2024-4-13-25. EDN:NRFCND

17. Буйневич М.В., Израилов К.Е. Авторская метрика оценки близости программ: приложение для поиска уязвимостейс помощью генетической деэволюции // Программные продукты и системы. 2025. Т. 38. № 1. С. 197–206. DOI:10.15827/0236-235X.149.197-206

18. Пикалов М.В., Письмеров А.М. Настройка параметров генетического алгоритма при помощи анализа ландшафта функции приспособленности и машинного обучения // Известия ЮФУ. Технические науки. 2024. № 2(238). С. 221–228. DOI:10.18522/2311-3103-2024-2-221-228. EDN:EFIXDB

19. Pan Z., Yan Y., Yu L., Wang T. Identification of binary file compilation information // Proceedings of the IEEE 5th Advanced Information Management, Communicates, Electronic and Automation Control Conference (Chongqing, China, 16–18 December 2022). IEEE, 2022. PP. 1141–1150. DOI:10.1109/IMCEC55388.2022.10019958

20. Kotenko I., Izrailov K., Buinevich M. Analytical Modeling for Identification of the Machine Code Architecture of Cyber-physical Devices in Smart Homes // Sensors. 2022. Vol. 22. Iss. 3. P. 1017. DOI:10.3390/s22031017. EDN:WPXNDJ

21. Kotenko I., Izrailov K., Buinevich M. The Method and Software Tool for Identification of the Machine Code Architecture in Cyberphysical Devices // Journal of Sensor and Actuator Networks. 2023. Vol. 12. Iss. 1. PP. 11. DOI:10.3390/jsan12010011. EDN:POQUEB

22. Beckman B., Haile J. Binary Analysis with Architecture and Code Section Detection using Supervised Machine Learning // Proceedings of the IEEE Security and Privacy Workshops (San Francisco, USA, 21–21 May 2020). IEEE, 2020. PP. 152–156. DOI:10.1109/SPW50608.2020.00041

23. Гусенко М.Ю. Создание обобщенной нотации программного интерфейса процессоров x86 для автоматизированного построения дизассемблера // Программные системы и вычислительные методы. 2024. № 2. С. 119–146. DOI:10.7256/2454-0714.2024.2.70951. EDN:EJJSYT

24. Долидзе А.Н. Обзор специфических функций языка FBD на примере программируемых реле LOGO! // Инженерный вестник Дона. 2022. № 11(95). С. 1–10. EDN:UZGJVM

25. Ding S.H.H., Fung B.C.M., Charland P. Asm2Vec: Boosting Static Representation Robustness for Binary Clone Search against Code Obfuscation and Compiler Optimization // Proceedings of the IEEE Symposium on Security and Privacy (San Francisco, USA, 19–23 May 2019). IEEE, 2019. PP. 472–489. DOI:10.1109/SP.2019.00003

26. Смольянинова М.О., Сидорова О.А. Об основных парадигмах современного программирования // Оригинальные исследования. 2023. Т. 13. № 7. С. 109–113. EDN:GJRBFF

References

1. Getman A.I., Goryunov M.N., Matskevich A.G., Rybolovlev D.A. A Comparison of a Machine Learning-Based Intrusion Detection System and Signature-Based Systems. *Proceedings of the Institute for System Programming of the RAS*. 2022;34(5): 111–126. (in Russ.) DOI:10.15514/ISPRAS-2022-34(5)-7. EDN:LDJOUO

2. Izrailov K.E., Gololobov N.V., Kraskin G.A. Method of Malware Analysis Based on Fuzzy Hash. *Informatization and communication*. 2019;2:36–44. (in Russ.) EDN:DUIUJM

3. Izrailov K. Genetic Decompilation Concept of the Telecommunication Devices Machine Code. *Proceedings of Telecommunication Universities*. 2021;7(4):95–109. (in Russ.) DOI:10.31854/1813-324X-2021-7-4-95-109. EDN:AIOFPM

4. Izrailov K.E. The Genetic De-Evolution Concept of Program Representations. Part 1. *Voprosy kiberbezopasnosti*. 2024;1(59):61–66. (in Russ.) DOI:10.21681/2311-3456-2024-1-61-66. EDN:CBCKRF

5. Izrailov K.E. The Genetic De-Evolution Concept of Program Representations. Part 2. *Voprosy kiberbezopasnosti*. 2024;2(60):81–86. (in Russ.) DOI:10.21681/2311-3456-2024-2-81-86. EDN:JUBPML

6. Skobtsov Yu.A. From Genetic Algorithms to Metaheuristics. *Informatika i kibernetika*. 2021;1-2(23-24):101–107. EDN:ILCTUW

7. Totukhov K.E., Romanov A.Yu., Lukyanov V.I. Investigation of the Effectiveness of Genetic Algorithms with Various Methods of Crossing and Selection. *Scientific Works of the Kuban State Technological University*. 2022;6:98–109. (in Russ.) EDN:DPRWIJ

8. Emelyanov A.A. The Reflexive Recognizing Grammar. *Bulletin of VSAWT*. 2016;46:23–32. (in Russ.) EDN:VPBBLP
9. Izrailov K.E., Buinevich M.V. Signature Search for Vulnerabilities in Machine Code Based on Genetic Decompilation. *Zaŝita informacii. Inside*. 2025;2(122):2–11. (in Russ.)
10. Mikulik I.I., Utkin L.V., Golubeva I.E. Development and Research of Methods for Local Interpretation of the Siaman Neural Network Based on Explanatory Intelligence. *Mathematical methods in technics and technologies - MMTT*. 2020;10:88–91. (in Russ.) EDN:SBFYYB
11. Silenko D.I., Lebedev I.G. Global Optimization Algorithm That Uses Decision Trees To Find Local Extrema. *Problems of Informatics*. 2023;2(59):21–33. (in Russ.) DOI:10.24412/2073-0667-2023-2-21-33. EDN:MLGKOX
12. Pyrnova O.A., Nikonorov D.P., Sharifullina A.Yu. Development of a Static Program Code Analyzer. *Nauchno-tekhnicheskii vestnik Povolzhia*. 2023;12:522–525. (in Russ.) EDN:AVFOIE
13. Izrailov K.E. Constant Values Distribution Investigation in the C Programs Source Code. *Proceedings of Telecommunication Universities*. 2024;10(5):119–129. (in Russ.) DOI:10.31854/1813-324X-2024-10-5-118-128. EDN:KARAVM
14. Hu W., Chen T., Zhang N., Ma J. Adjust ELF Format for Multi-core Architecture. *Proceedings of the International Conference on Electronic Computer Technology, 20–22 February 2009, Macau, China*. IEEE; 2009. p.388–391. DOI:10.1109/ICECT.2009.73
15. Tsygankov V.A., Shabalina O.A., Kataev A.V. Investigation of the Impact of Population Size on the Performance of a Genetic Algorithm. *Izvestiya SFedU. Engineering Sciences*. 2024;3(239):168–176. (in Russ.) DOI:10.18522/2311-3103-2024-3-168-176. EDN:IAFWKU
16. Izrailov K.E. Predicting the Size of the Source Code of a Binary Program in the Interests of Its Intellectual Reverse Engineering. *Voprosy kiberbezopasnosti*. 2024;4(62):13–25. (in Russ.) DOI:10.21681/2311-3456-2024-4-13-25. EDN:NRFCND
17. Izrailov K.E., Buinevich M.V. Author's metric for assessing proximity of programs: application for vulnerability search using genetic de-evolution. *Software & Systems*. 2025;38(1):197–206. (in Russ.) DOI:10.15827/0236-235X.149.197-206
18. Pikalov M.V., Pismerov A.M. Genetic Algorithm Parameter Tuning Using Exploratory Landscape Analysis and Machine Learning. *Izvestiya SFedU. Engineering Sciences*. 2024;2(238):221–228. (in Russ.) DOI:10.18522/2311-3103-2024-2-221-228. EDN:EFIXDB
19. Pan Z., Yan Y., Yu L., Wang T. Identification of binary file compilation information. *Proceedings of the IEEE 5th Advanced Information Management, Communicates, Electronic and Automation Control Conference, 16–18 December 2022, Chongqing, China.* IEEE; 2022. p.1141–1150. DOI:10.1109/IMCEC55388.2022.10019958
20. Kotenko I., Izrailov K., Buinevich M. Analytical Modeling for Identification of the Machine Code Architecture of Cyberphysical Devices in Smart Homes. *Sensors*. 2022;22(3):1017. DOI:10.3390/s22031017. EDN:WPXNDJ
21. Kotenko I., Izrailov K., Buinevich M. The Method and Software Tool for Identification of the Machine Code Architecture in Cyberphysical Devices. *Journal of Sensor and Actuator Networks*. 2023;12(1):11. DOI:10.3390/jsan12010011. EDN:POQUEB
22. Beckman B., Haile J. Binary Analysis with Architecture and Code Section Detection using Supervised Machine Learning. *Proceedings of the IEEE Security and Privacy Workshops, 21–21 May 2020, San Francisco, USA*. IEEE; 2020. PP. 152–156. DOI:10.1109/SPW50608.2020.00041
23. Gusenko M.Yu. Creating a Common Notation of the X86 Processor Software Interface for Automated Disassembler Construction. *Software systems and computational methods*. 2024;2:119–146. (in Russ.) DOI:10.7256/2454-0714.2024.2.70951. EDN:EJJSYT
24. Dolidze A.N. Overview of the Specific Functions of the FBD Language on the Example of Programmable Relays Logo! *Engineering journal of Don*. 2022;11(95):1–10. (in Russ.) EDN:UZGJVM
25. Ding S.H.H., Fung B.C.M., Charland P. Asm2Vec: Boosting Static Representation Robustness for Binary Clone Search against Code Obfuscation and Compiler Optimization. *Proceedings of the IEEE Symposium on Security and Privacy, 19–23 May 2019, San Francisco, USA*. IEEE; 2019. p.472–489. DOI:10.1109/SP.2019.00003
26. Smolyaninova M.O., Sidorova O.A. About the Main Paradigms of Modern Programming. *Originalnye issledovaniia*. 2023;13(7):109–113. (in Russ.) EDN:GJRBFF

Статья поступила в редакцию 20.12.2024; одобрена после рецензирования 22.01.2025; принята к публикации 05.02.2025.
The article was submitted 20.12.2024; approved after reviewing 22.01.2025; accepted for publication 05.02.2025.

Информация об авторе:

ИЗРАИЛОВ Константин Евгеньевич

кандидат технических наук, доцент, старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук

https://orcid.org/0000-0002-9412-5693

Автор сообщает об отсутствии конфликтов интересов.

The author declares no conflicts of interests.

Научная статья
УДК 004.056; 519.25
https://doi.org/10.31854/1813-324X-2025-11-1-99-112
EDN:OOPJJR

Анализ и прогнозирование временных рядов кибератак на информационную систему ведомственного вуза: возможности и ограничения методов

Владимир Николаевич Наумов[1], naumov122@list.ru
Михаил Викторович Буйневич[2] ✉, bmv1958@yandex.ru
Максим Юрьевич Синещук[2], smaxim@igps.ru
Марина Алексеевна Тукмачева[2], mtukmacheva@mail.ru

[1]Северо-Западный институт управления – филиал РАНХиГС,
Санкт-Петербург, 199178, Российская Федерация
[2]Санкт-Петербургский университет ГПС МЧС России,
Санкт-Петербург, 196105, Российская Федерация

Аннотация

Актуальность статьи *обусловлена ростом угроз компьютерной безопасности критических информационных ресурсов, в том числе в системе образования, разнообразием видов и направлений кибератак, требующих дифференциации известных методов анализа и прогнозирования, в том числе на основе использования теории временных рядов.* ***Целью*** *статьи является исследование возможностей и ограничений использования методов теории временных рядов для анализа и прогнозирования динамики кибератак на примере ведомственного вуза, готовящего специалистов многим видам безопасности: техносферной, пожарной, информационной и проч. Высказана и проверена гипотеза о влиянии характера исходных данных на выбор методов анализа и прогнозирования временных рядов числа кибератак, о первичности исходных данных на результативность решения указанных задач. Выполнен анализ логов мониторинга межсетевого экрана корпоративной информационной системы; на их основе построены временные ряды числа различных видов атак и решены задачи текущего прогнозирования.* ***Новизна*** *полученных результатов обусловлена применением известных методов теории прогнозирования временных рядов к задаче исследования динамики кибератак на корпоративную информационную систему ведомственного вуза.* ***Теоретическая значимость*** *состоит в установлении границ возможности их применения в силу вариативности исследуемых временных рядов, а также в подтверждении первичности качества исходных данных над существующими методами и моделями.* ***Практическая ценность*** *определяется построением моделей временных рядов, позволяющих решать задачи текущего прогнозирования числа кибератак.*

Ключевые слова: *кибератаки, ведомственная информационная система, логи программно-аппаратного межсетевого экрана, временные ряды, анализ и прогнозирование, стационарность временных рядов, фильтры экспоненциального сглаживания, модели авторегрессии проинтегрированного скользящего среднего, метод Prophet*

Источник финансирования: *Работа выполнена в рамках НИР «Кибермониторинг» рег. № НИОКТР 1024040800041-6-2.2.66.*

Ссылка для цитирования: Наумов В.Н., Буйневич М.В., Синещук М.Ю., Тукмачева М.А. Анализ и прогнозирование временных рядов кибератак на информационную систему ведомственного вуза: возможности и ограничения методов // Труды учебных заведений связи. 2025. Т. 11. № 1. С. 99–112. DOI:10.31854/1813-324X-2025-11-1-99-112. EDN:OOPJJR

Original research
https://doi.org/10.31854/1813-324X-2025-11-1-99-112
EDN:OOPJJR

Analyzing and Predicting the Time Series of Cyberattacks on Higher Education Departmental Institution Information System: Methods Opportunities and Limitations

Vladimir N. Naumov[1], naumov122@list.ru
Mikhail V. Buinevich[2] ✉, bmv1958@yandex.ru
Maksim Y. Sineshchuk[2], smaxim@igps.ru
Marina A. Tukmacheva[2], mtukmacheva@mail.ru

[1]North-West Institute of Management of the Russian Presidential Academy of National Economy and Public Administration,
St. Petersburg, 199178, Russian Federation
[2]Saint Petersburg University of State Fire Service of Emercom of Russia,
St. Petersburg, 196105, Russian Federation

Annotation

The article relevance *is due to the growing threats to computer security of critical information resources, including in the education system, cyberattacks types and trends diversity, requiring known analysis and forecasting methods differentiation, including those based on the use of time series theory.* ***The article aim*** *is to study the possibilities and limitations of using time series theory methods to analyses and predict the cyber attacks dynamics on the departmental university example that trains specialists in many security types: technosphere, fire, information and other. Hypothesis about the influence of the initial data nature on the methods for cyberattacks number time series analyzing and forecasting choice, and primacy of initial data on the solving these tasks effectiveness was stated and tested. Analyses of the corporate information system firewall monitoring logs are performed. On their basis, time series number of different types of attacks are constructed. The tasks of building mathematical models and current forecasting have been solved. An integrated approach to their solution based on preliminary processing, testing of statistical hypotheses about DS- and TS-stationarity and use of different forecasting methods was applied. The obtained* ***results novelty*** *is due to known methods of time series forecasting theory application to studying the dynamics of cyberattacks on the departmental university corporate information system.* ***Theoretical significance*** *consists in establishing the limits of their application possibility due to the studied time series variability, as well as in confirming the initial data primary quality over the existing methods and models. The* ***practical value*** *is determined by the time series models construction that allow solving tasks of cyberattacks number current forecasting.*

Keywords: *cyberattacks, departmental information system, firewall logs, time series, analysis and forecasting, stationarity of time series, exponential smoothing filters, auto-regression models of the pro-integrated moving average, Prophet method*

Funding: *The work was carried out under the R&D "Cybermonitoring" Reg. No. NIOCTR 1024040800041-6-2.2.66.*

For citation: Naumov V.N., Buinevich M.V., Sineshchuk M.Y., Tukmacheva M.A. Analyzing and Predicting the Time Series of Cyberattacks on Higher Education Departmental Institution Information System: Methods Opportunities and Limitations. *Proceedings of Telecommunication Universities.* 2025;11(1):99–112. (in Russ.) DOI:10.31854/1813-324X-2025-11-1-99-112. EDN:OOPJJR

Введение

Патриарх экономико-математической теории О. Моргерштерн указывал, что в триаде основных типов задач, решаемых учеными-исследователями, а именно – анализе, моделировании и прогнозировании, последняя является наиболее сильным вариантом постановки исследовательской проблемы [1]. Существует большое количество методов прогнозирования, качество которых зависит от имеющихся исходных данных. Если данные о прошлом представлены в числовой форме, а также имеются некоторые предположения, что выявленная на основе исследования ретроспективных данных тенденция может быть пролонгирована, то в этом случае используются количественные методы и, в частности, методы теории временных рядов.

За последние годы в ней разработано большое количество методов, алгоритмов и моделей, издается международный журнал прогнозирования, опубликовано множество книг, например [2, 3]. Создано значительное число пакетов прогнозирования для языков Python, R, что позволяет автоматизировать решение задач прогнозирования. Существующие статистические пакеты и графические надстройки, например, gretl, Loginom, JASP, jamovi позволяют в ходе исследования применять low-code, no-code подходы.

Популярность количественных методов прогнозирования увеличивается с возрастанием количества наборов данных, их размера (десятки гигабайт, например Kaggle). Только для решения задач прогнозирования на момент написания статьи их число превысило 8000. Более 500 датасетов посвящено проблемам кибербезопасности. Набор данных машинного обучения Калифорнийского университета UC Irvine Machine Learning Repository содержит 90 временных рядов, позволяющих решать задачи прогнозирования.

Анализ данных различной природы, включая и временные ряды, основан на модели, предложенной Дж. Тьюки, который утверждал, что «не метод определяет схему исследования, а характер данных». Вместо традиционно используемой последовательности исследования «модель – анализ – данные – результат», им была предложена схема «данные – разведочный анализ – модель – подтверждающий анализ». Первичной в этой схеме являются данные: их характер, используемые шкалы, объем, учет времени, качество, – все это определяет выбор инструмента исследования. Поэтому большинство публикаций, посвященных решению задач прогнозирования, в том числе и кибератак, непосредственно связано с характером исследуемых данных, наличием в них тренда, сезонных составляющих, характера случайной компоненты и др.

Так, например, в статье [4] исследуется динамика кибератак на веб-сервисы корпоративной сети, в том числе профили атак для различных стран. В основном использованы методы и инструменты графического и корреляционного анализа при допущении о стационарности исследуемых временных рядов. В [5] основное внимание уделяется прогнозированию общего числа атак, а также атак из определенных географических регионов на «сеть-приманку» (honeynet). Авторы использовали несколько подходов, таких как экспоненциальное сглаживание, ARIMA, SARIMA, GARCH и Bootstrapping. При этом показано, что различные методы обеспечивают различную точность для разных временных рядов. В [6] решена задача моделирования сезонных временных рядов количества атак на прикладное программное обеспечение с помощью гармонических составляющих. В этих статьях была дана характеристика источников данных и методики их предобработки.

В настоящей статье выполнен анализ динамики кибератак на информационную систему ведомственного вуза. Для получения исходных данных была использована BI-платформа, позволяющая графически представить динамику временных рядов в разрезе различных видов из разных стран. Периодичность поступления данных от источников позволяет сформировать временные ряды, получить многомерный временной ряд, сформировать панельные данные – то есть дополнительно к задачам визуального анализа решать задачи прогнозирования.

Методы и инструменты

В качестве источников статистических данных инцидентов информационной безопасности были использованы логи программно-аппаратного межсетевого экрана IDECO UTM производства компании ООО «Айдеко». В зависимости от версий, этот межсетевой экран имеет спектр модулей фильтрации трафика: контент-фильтр, контроль приложений, предотвращение вторжений, антивирус веб-трафика. Рассматривались ряды количества атак по уровню угрозы. Столбиковые диаграммы числа кибератак, построенные с помощью ведомственной BI, приведены на рисунке 1. Другие ее визуальные элементы позволяют построить и исследовать временные ряды для различных стран и типов заблокированных атак (рисунок 2).

В ходе анализа рассматривались логи за 3 месяца межсетевого экрана. Полученные статистические данные позволили построить следующие интервальные временные ряды числа критических и опасных атак, числа предупреждений, а также – суммарного числа атак.

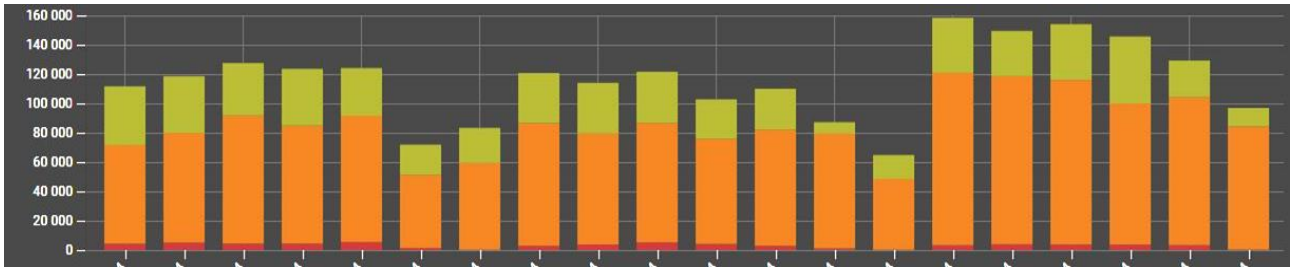
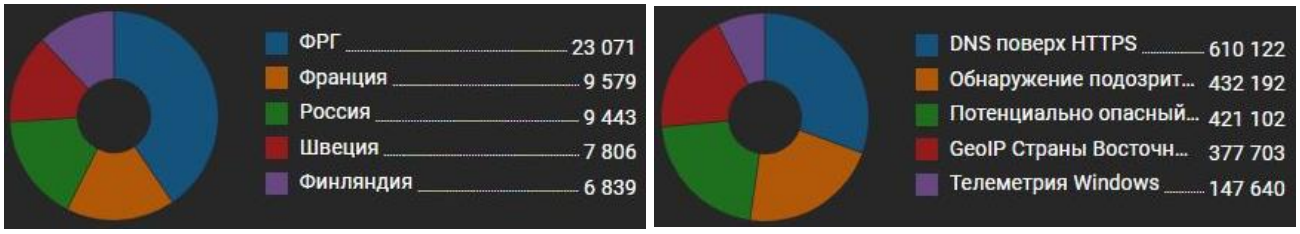


Рис. 1. Количество атак по уровню угрозы

Fig. 1. Number of Attacks by Threat Level



a) b)

Рис. 2. Статистика кибератак на информационную систему ведомственного вуза: a) Топ атакующих стран; b) Топ заблокированных типов атак

Fig. 2. Statistics of Cyber Attacks on the Departmental University Departmental University Corporate Information System: a) Top Attacking Countries; b) Top Blocked Types of Attacks

В качестве временного шага был выбран один час, что позволило построить сравнительно длинные ряды и сформулировать гипотезы о наличии сезонных составляющих, а также решить традиционные задачи разведывательного анализа: исследования стационарности временных рядов, построения их моделей и прогнозирования уровней исследуемых временных рядов с их помощью. В ходе исследования были использованы статистические пакеты JASP, jamovi, а также язык R и интегрированная среда разработки Rstudio. Выбор данных средств был обусловлен возможностью с их помощью автоматизировать большое количество задач прогнозирования, а в ряде случаев отказаться от разработки программных модулей. Реализовать технологию no-code. В частности, были применены следующие методы теории временных рядов:

– регрессионный анализ;
– экспоненциальное сглаживание;
– методы авторегрессии проинтегрированного скользящего среднего;
– байесовские методы пространства состояний;
– метод Prophet.

Такое большое количество методов позволило произвести сравнительный анализ результатов исследования, выбрать лучшие модели временных рядов и решить задачи прогнозирования с их помощью, а также дать характеристику динамики кибератак на исследуемую информационную систему. Так как данные методы разработаны на основе различных подходов, это позволяет учесть особенности анализируемых данных, реализовать модель Дж. Тьюки.

Результаты проведенного графического анализа исследуемых временных рядов с помощью Rstudio приведены на рисунке 3. Выполненный анализ показал, что временные ряды имеют сезонные составляющие, выявлена автокорреляция их уровней. Также установлено, что имеется большая дисперсия случайных составляющих, что усложняет их исследование.

Результаты

Результаты описательной статистики данных временных рядов приведены в таблице 1. Диаграммы, представленные на рисунке 3, а также результаты описательной статистики позволяют сделать следующие выводы.

Во-первых, имеется большая вариативность уровней временных рядов. Для дальнейшего их исследования целесообразно решать задачи сглаживания или удалять аномальные наблюдения.

Во-вторых, коэффициент автокорреляции для каждого временного ряда значимо отличается от нуля. Следовательно, можно решать задачи прогнозирования.

В-третьих, коррелограммы показывают, что существуют сезонные составляющие временных рядов с периодом сезонности, равным 24 часам. Наибольшее число атак приходится на период с 9 до 15 часов, т. е. на дневное время. На рисунке 4 показаны «ящичные» диаграммы, которые были построены для исследуемых временных рядов.

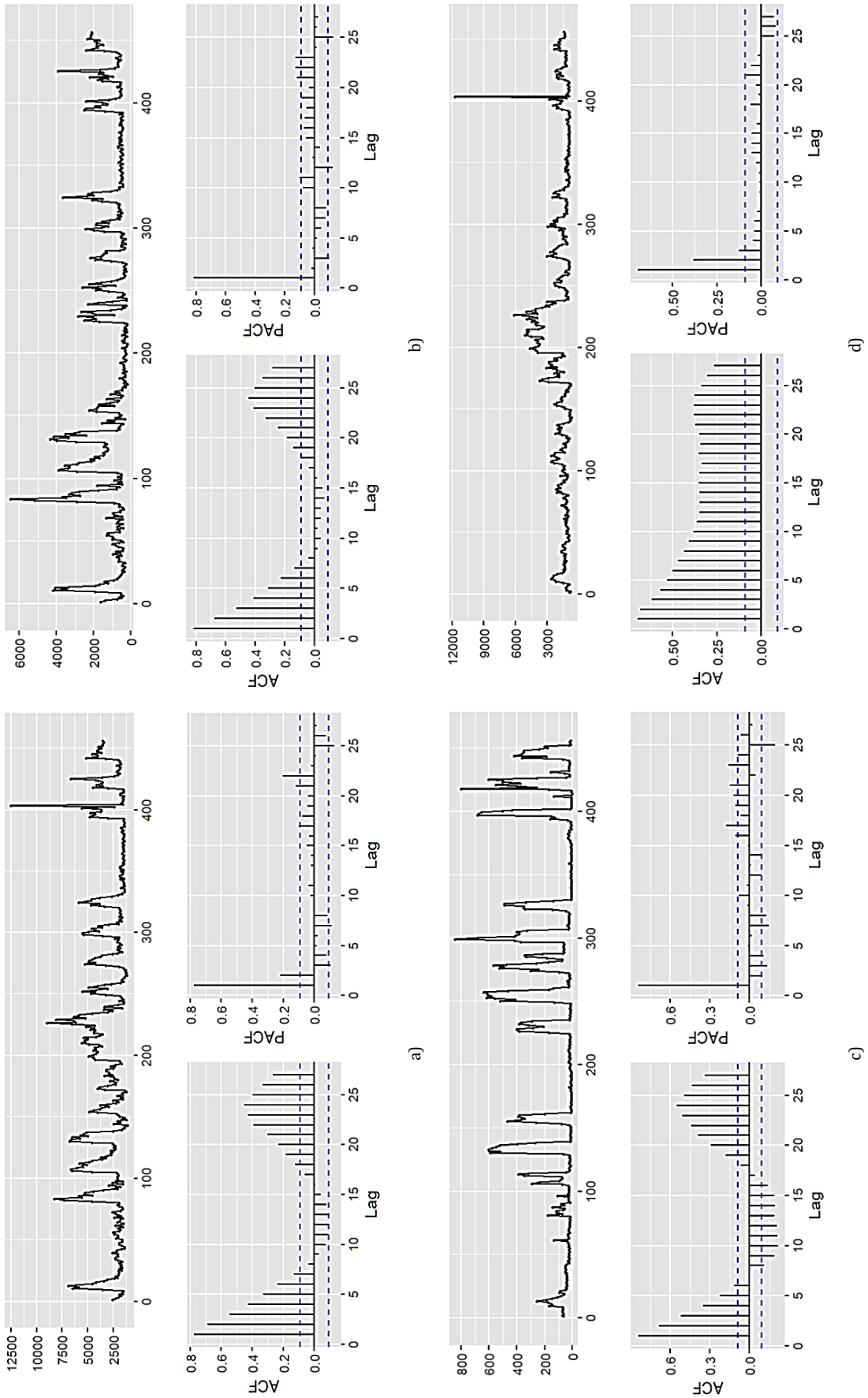


Рис. 3. Точечная диаграмма и коррелограммы автокорреляционной (ACF) и частной автокорреляционной (PACF) функций: суммарного числа атак (a), числа предупреждений (b), критических (c) и опасных (d) атак

Fig. 3. Dot Plot and Correlograms of Autocorrelation Function (ACF) and Private Autocorrelation Function (PACF): Total Number of Attacks (a), Number of Warnings (b), Critical (c) and Dangerous (d) Attacks

ТАБЛИЦА 1. Описательная статистика

TABLE 1. Descriptive Statistics

Показатели	Временные ряды			
	Критичные	Опасные	Предупреждение	ВСЕГО
Существующие	456	456	456	456
Пропущенные	0	0	0	0
Среднее	110,746	1705,908	1046,156	2862,809
Стандартное отклонение	169,834	1032,702	918,354	1566,028
Дисперсия	28 843,557	1 066 000	843 374,923	2 452 000
Размах	839	11013	6277	11441
Минимум	3	664	178	1060
Максимум	842	11677	6455	12501
Start	63	898	1597	2558
End	10	1414	2105	3529
Автокорреляция первого порядка	0,844	0,698	0,82	0,776

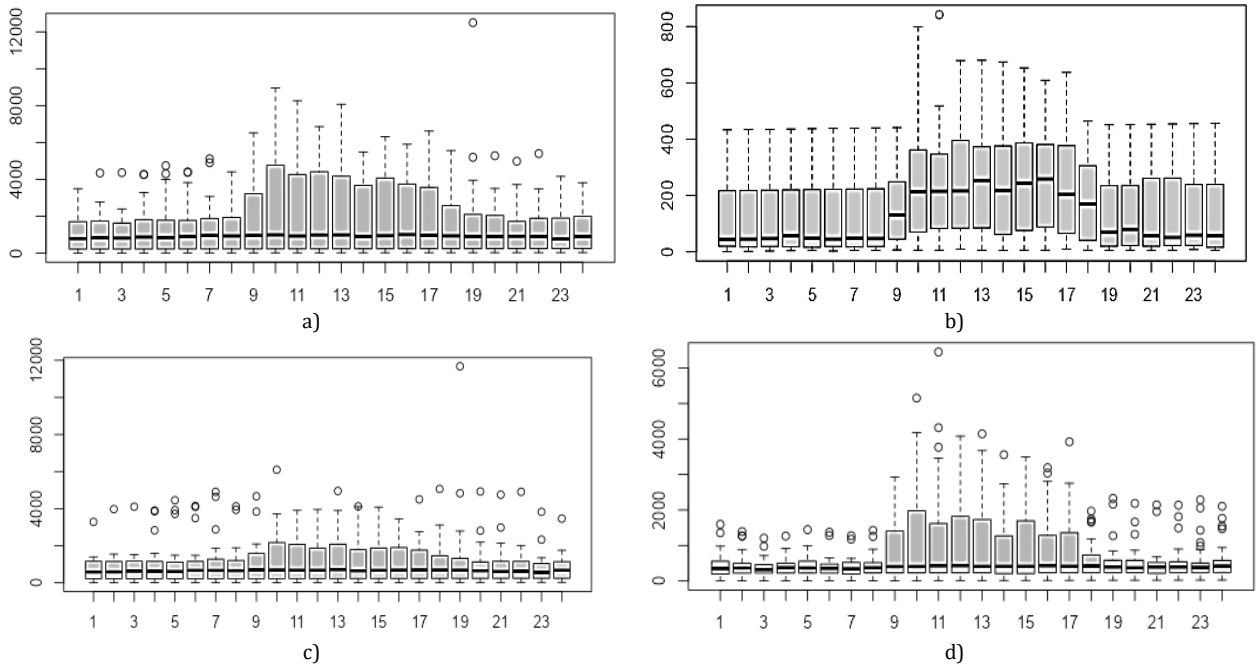


Рис. 4. «Ящичные» диаграммы числа: a) всех атак; b) критических атак; c) опасных атак; d) предупреждений

Fig. 4. "Box" Plots of the Number of all Attacks (a); Critical Attacks (b); Dangerous Attacks (c) and Alerts (d)

Наибольшие размеры «ящиков» (см. рисунок 4) также приходятся на дневное время. При этом характерно, что размах значений и длины верхних «усов» для анализируемого периода также максимальны. Диаграммы вновь подтверждают наличие выбросов, которые на диаграммах обозначены круглыми маркерами, расположенными над верхними «усами». Их число для разных рядов составляет от 19 до 33. Существуют и экстремальные значения, приходящиеся на 11 и 19 часов.

Для построения моделей временных рядов потребовалось выполнить анализ их стационарности с помощью статистических критериев Дикки – Фуллера, KPSS [7] и Филиппа – Перона [8]. Результаты проверки данных статистических гипотез приведены в таблице 2.

Данная таблица учитывает два вида стационарности временных рядов – DS- и TS-стационарность (*аббр. от англ.* Difference Stationary, разностно-стационарный и Trend Stationary, стационарный относительно тренда). В первом случае ряд является $I(k)$-интегрированным, например, случайным блужданием $I(1)$. Приведение его к стационарному осуществляется с помощью нахождения разностного ряда k-го порядка, т. е. получения так называемого $I(0)$-стационарного процесса. При TS-стационарности, частным случаем которой является $I(0)$-ряд (уровнево-стационарный ряд), из наблюдаемых значений необходимо вычесть значения детерминированной функции, описывающей тренд.

ТАБЛИЦА 2. Статистические критерии проверки стационарности временных рядов

TABLE 2. Statistical Criteria for Testing Stationarity of Time Series

Временной ряд	Критерий	Значение критерия	Значение лага	Уровень значимости (*p*-value)	Проверяемая гипотеза (H0): ряд …
Предупреждения	Критерий Дики – Фуллера	–2,826	4	0,234	не стационарен
	Критерий Филлипса – Перона	–20,355	3	0,055	не стационарен
	Критерий KPSS, уровневая стационарность	0,182	4	0,100	уровнево-стационарен
	Критерий KPSS, стационарность тренда	0,135	4	0,071	стационарен по тренду
Опасные атаки	Критерий Дики – Фуллера	–3,479	4	0,047	не стационарен
	Критерий Филлипса – Перона	–21,399	3	0,044	не стационарен
	Критерий KPSS, уровневая стационарность	0,160	4	0,100	уровнево-стационарен
	Критерий KPSS, стационарность тренда	0,147	4	0,050	стационарен по тренду
Критические атаки	Критерий Дики – Фуллера	–3,092	4	0,124	не стационарен
	Критерий Филлипса – Перона	–32,156	3	0,010	не стационарен
	Критерий KPSS, уровневая стационарность	0,517	4	0,038	уровнево-стационарен
	Критерий KPSS, стационарность тренда	0,206	4	0,014	стационарен по тренду
Все атаки	Критерий Дики – Фуллера	–2,948	4	0,184	не стационарен
	Критерий Филлипса – Перона	–18,364	3	0,086	не стационарен
	Критерий KPSS, уровневая стационарность	0,158	4	0,100	уровнево-стационарен
	Критерий KPSS, стационарность тренда	0,143	4	0,055	стационарен по тренду

Приведенное выше разнообразие видов стационарности определяет не только разнообразие применяемых статистических критериев, но и проверяемых статистических гипотез (последний столбец таблицы, содержащий описание нулевой статистической гипотезы). Отметим, что в четвертом столбце таблицы указано значение лага. Это позволяет при проверке стационарности использовать так называемые расширенные статистические тесты, предполагающие, что анализируемый случайный процесс не является авторегрессионным первого порядка, а описывается более сложной моделью с бóльшим, чем один числом лагов.

Значение уровней значимости (*p*-value) для критериев Дики – Фуллера и Филлипса – Перрона больше, например 0,05, позволяют сделать вывод, что временной ряд предупреждений является DS-стационарным. Чтобы его сделать уровнево-стационарным, необходимо построить ряд разностей. Итоговый временной ряд всех атак, а также временной ряд опасных атак не относятся к категории DS-рядов. С другой стороны, на уровне 0,055 они является уровнево-стационарными. Ряды не содержат тренда, и возможно, имеют ненулевое математическое ожидание своих уровней. И наконец, анализ стационарности временного ряда критических атак с помощью четырех критериев приводит к противоречиям: первые два критерия на уровне 0,05 не позволяют сделать вывод о DS-стационарности, а вторые два на этом же уровне значимости не отвечают на вопрос о стационарности по тренду или об уровневой стационарности. Напомним, что в этом случае возможно использовать поправку Бонферрони, являющуюся методом противодействия проблеме множественных сравнений при применении семейства статистических гипотез. Необходимо продолжить исследование, например, с помощью моделей ARIMA.

Сравнительный анализ результатов построения моделей для одного из анализируемых временных рядов (всех атак) разными методами приведен в таблице 3. Данные результаты показывают низкое качество для различных классов моделей. Здесь в качестве критериев оценки их качества использованы:

– показатель ранжированной оценки вероятности (CRPS, *аббр. от англ.* Continuous Ranked Probability Score) [9];

– показатель Дэвида – Себастьяни (DSS, *аббр. от англ.* Dawid-Sebastiani Score) [10];

– средняя абсолютная ошибка аппроксимации (MAE, *аббр. от англ.* Mean Absolute Error);

– квадратный корень из среднего квадрата ошибки аппроксимации (RMSE, *аббр. от англ.* Root Mean Squared Error);

– коэффициент детерминации (R^2).

ТАБЛИЦА 3. Результаты оценки качества модели

TABLE 3. Results of Model Quality Assessment

Класс модели	CRPS	DSS	MAE	RMSE	R^2
Линейная регрессия	927,678	15,940	1405,956	1663,859	0,012
Байесовская модель BSTS	2901,963	19,174	1888,910	2454,455	0,108
Байесовская авторегрессионная модель	1235,123	16,621	1659,680	2127,404	0,115
Prophet	1426,080	19,452	1790,740	2154,794	0,381

Если последние три критерия применяются сравнительно часто, то первые два нуждаются в пояснении. Так, показатель CRPS – непрерывная ранжированная оценка вероятности, является обобщением показателя MAE для случая вероятностных прогнозов; его меньшему значению соответствует лучшая модель. Показатель DSS оценивает средние значения вектора отклонений наблюдаемых и прогнозных значений; здесь также меньшему значению критерия соответствует лучшая модель. Приведенные значения показывают, что нет лучшей по всем показателям модели, но по большинству показателей лучшей является линейная регрессионная модель, что довольно неожиданно. Однако ее построение и оценка качества такой модели также не позволяет сделать вывод о ее применимости.

Таким образом, без предварительной обработки с целью повышения качества исходных данных задача прогнозирования не может быть решена. Поэтому дальнейшее исследование было проведено с учетом необходимости повышения качества исходных данных за счет преобразования временных рядов. Известны различные методы таких преобразований, например, логарифмирование или извлечение квадратного корня наблюдаемых уровней. Их обобщением является преобразование Бокса – Кокса [11], при выполнении которого необходимо задать или найти значение параметра данного преобразования λ. Однако в этом случае затрудняется интерпретация полученных результатов, и возникает необходимость обратного преобразования.

В качестве альтернативы выберем методы фильтрации, в частности, метод ETS (*аббр. от англ.* Triple Exponential Smoothing, тройного экспоненциального сглаживания) [12]; система уравнений такого фильтра позволяет сгладить уровни временно́го ряда, тренд, а также сезонные составляющие. При этом модель задается трехзначным символьным кодом, первый знак которого определяет тип случайной составляющей «E», второй – тип тренда «T», третий – характеризует сезонную составляющую «S». Такой код позволяет задать пятнадцать классов фильтров сглаживания. Будем использовать средства подгонки лучшего фильтра и оптимизации значений его параметров; их число зависит от выбора класса фильтра.

Для построения моделей временных рядов выполним композицию двух методов: экспоненциального сглаживания и авторегрессии ARIMA. Возможности применяемых программных средств позволяют использовать методологию autoML и подобрать с ее помощью нужные значения гиперпараметров, как для фильтров, так и для моделей ARIMA. Так как ее параметры подбираются автоматически, например, по значению информационных критериев, то при их определении возможно получение частных видов модели, например ARMA, AR и MA. В случае необходимости следует использовать расширения – SARIMA, ARIMAX, SARIMAX: их возможности позволят исследовать влияние рядов критических, опасных и атак-предупреждений на их общее число.

Лучшая модель фильтра позволяет получить сглаженные значения уровней временного ряда l_t. По сглаженным значениям можно построить модель ARIMA, откликом для которой будет значение уровня ряда на момент времени t. Ее вид и значения гиперпараметров при этом определяются автоматически.

Первый временной ряд, содержащий все атаки, может быть представлен моделью ARIMA (1, 0, 2) с ненулевым математическим ожиданием:

$$l_t = 2858{,}52 + 0{,}82 l_{t-1} + \varepsilon_t + 0{,}19\varepsilon_{t-2}, \varepsilon_t : N(0; 741).$$

Фильтр сглаживания относится к классу фильтра с мультипликативной (M) ошибкой («E» = M), с отсутствием (N – None) тренда («T» = N) и сезонной составляющей («S» = N); его уравнение имеет вид:

$$l_t = 0{,}77 y_t + 0{,}23 l_{t-1}, l_{init} = 2246{,}2,$$

где l_{init} – начальное состояние фильтра.

Построенная модель временного ряда позволяет выполнить интервальную оценку условного математического ожидания прогноза. На рисунке 5 приведена диаграмма прогнозирования на три дня с построением верхней и нижней границ 80- и 95-процентных доверительных интервалов. Сравнительно небольшая их ширина и медленный ее рост позволяют увеличить горизонт прогноза и с учетом знаков коэффициентов в уравнении предположить, что в среднем, в недалеком будущем общий поток атак не увеличится.

Аналогично решены задачи построения модели фильтра сглаживания, уравнения ARIMA и прогнозирования для других временны́х рядов. Так, временно́й ряд, содержащий критические атаки, может быть представлен моделью ARIMA (2, 0, 1) с ненулевым математическим ожиданием, имеющей вид:

$$l_t = 110{,}34 + 1{,}69 l_{t-1} + 0{,}75 l_{t-2} + \varepsilon_t - 0{,}77\varepsilon_{t-1},$$
$$\varepsilon_t : N(0{,}28; 8).$$

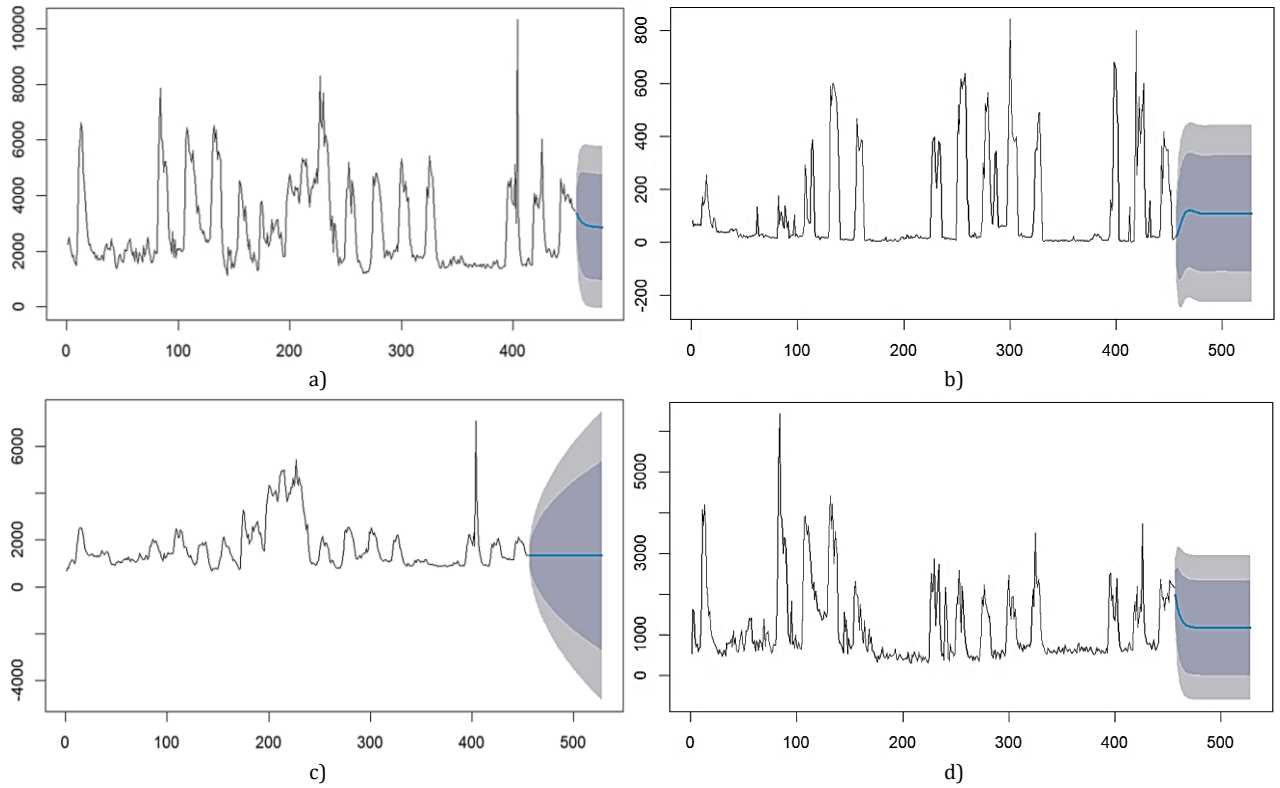


Рис. 5. Диаграмма прогнозирования уровней временного ряда числа: a) всех атак; b) критических атак; c) опасных атак; d) предупреждений

Fig. 5. Time Series Level Prediction Diagram of the Number of All Attacks (a), Critical Attacks (b), Dangerous Attacks (c) and Alerts (d)

Сглаженные уровни временного ряда l_t были получены с помощью фильтра простого экспоненциального сглаживания с параметром α = 1 и инициальным значением фильтра, равным 83,0. К сожалению, данный фильтр не сглаживает уровни временного ряда, поэтому диаграмма, приведенная на рисунке 5b, показывает большую ширину обоих доверительных интервалов. Возможной причиной такой ситуации может быть большое число выбросов и большой разброс значений уровней временного ряда. Тем не менее, полученный на три дня кратковременный прогноз также позволяет сделать вывод о стационарности временного ряда, т. е. подтвердить результаты ранее проверенных статистических гипотез по различным критериям.

Временной ряд, содержащий сведения об опасных атаках, описывается моделью авторегрессии-скользящего среднего ARIMA (0, 1, 0):

$$l_t = l_{t-1} + \varepsilon_t;\ \varepsilon_t : N(0; 370).$$

Для сглаживания его уровней с помощью autoML был определен аддитивный фильтр тройного экспоненциального сглаживания ETS с мультипликативной случайной составляющей (MAN).

Уравнения данного фильтра сглаживания содержат два оцененных параметра для каждого из них и имеют вид:

$$l_t = 0{,}5l_{t-1} + 0{,}49(l_{t-1} + b_{t-1}),$$
$$b_t = 0{,}02(l_t - l_{t-1}) = 0{,}98b_{t-1},$$
$$l_{init} = 704{,}1, b_{init} = -3{,}53.$$

Инициальные значения уровня ряда l_{init} и тренда b_{init} позволяют применять данный фильтр для решения задач сглаживания.

Построенная модель ARIMA позволяет сделать вывод, что данный временной ряд является DS-рядом, т. е. имеет стохастический тренд. С ростом времени прогнозирования растет ширина доверительного интервала прогноза, что не позволяет решать задачи долгосрочного прогнозирования уровней временного ряда. Это подтверждается колоколообразным видом доверительных интервалов прогноза, приведенных на рисунке 5c.

Последний временной ряд также может быть представлен моделью ARIMA с параметром авторегрессии p = 2 и параметром скользящего среднего q = 2 с ненулевым математическим ожиданием, имеющей следующий вид:

$$l_t = 116827 + 0{,}69l_{t-1} + 0{,}01l_{t-2} + \varepsilon_t + 0{,}24\varepsilon_{t-1} + \\ +0{,}13\varepsilon_{t-2}, \varepsilon_t : N(0; 467).$$

Сглаженные значения данного временного ряда получены с помощью соотношений:

$$l_t = 0{,}88l_{t-1} + 0{,}12(l_{t-1} + b_{t-1}),$$

$$b_t = 0{,}001(l_t - l_{t-1}) + 0{,}999b_{t-1},$$
$$l_{init} = 376{,}1, b_{init} = 155{,}59.$$

Диаграмма прогнозирования уровней временного ряда на три дня (см. рисунок 5d) также показывает, что доверительный интервал прогноза сравнительно невелик, поэтому можно увеличивать горизонт прогноза.

Полученные модели прогнозирования сглаженных уровней позволяют сделать вывод, что все анализируемые временные ряды, кроме опасных атак, относящихся к нестационарному ряду «случайное блуждание», являются TS-стационарными, а их случайные составляющие могут быть описаны авторегрессионными зависимостями. Отметим, что все коэффициенты, приведенные в уравнениях моделей ARIMA, значимо отличаются от нуля на сравнительно высоком уровне. Данный вывод сделан с помощью статистического критерия Стьюдента.

Дальнейшее исследование может быть направлено на анализ компонентов временных рядов, в частности тренда, сезонной и случайной составляющей, несмотря на то, что фильтры экспоненциального сглаживания не позволили выявить сезонные составляющие. С этой целью целесообразно использовать метод Prophet, который основан на подгонке аддитивных регрессионных моделей, включающих тренд g_t, сезонные колебания s_t, эффекты праздников h_t, а также случайную составляющую ε_t. Его выбор основан на том, что он хорошо работает в условиях годовой, недельной и ежедневной сезонности, реализован в языках аналитики R, Python, а также в их графических приложениях.

В общем виде аддитивная регрессионная модель временного ряда, построенная с помощью данного метода, принимает вид:

$$y_t = g_t + s_t + h_t + \varepsilon_t,$$

где g_t – тренд; s_t – совокупность сезонных составляюших; h_t – составляющая учитывающая эффекты праздников и других влиятельных событий; ε_t – случайная компонента.

Для выявления сезонных составляющих s_t используется разложение в ряд Фурье. При определении тренда применяются кусочные линейная или логистическая модели с использованием точек излома. Для построения модели и выявления ее компонент используем платформу jamovi, которую можно рассматривать как графическую надстройку языка R (https://www.jamovi.org). Результаты декомпозиции на основе построения кусочной линейной регрессионной модели с годовыми (yearly), недельными (weekly) и дневными (daily) колебаниями для исследуемых временных рядов приведены на рисунках 6–9.

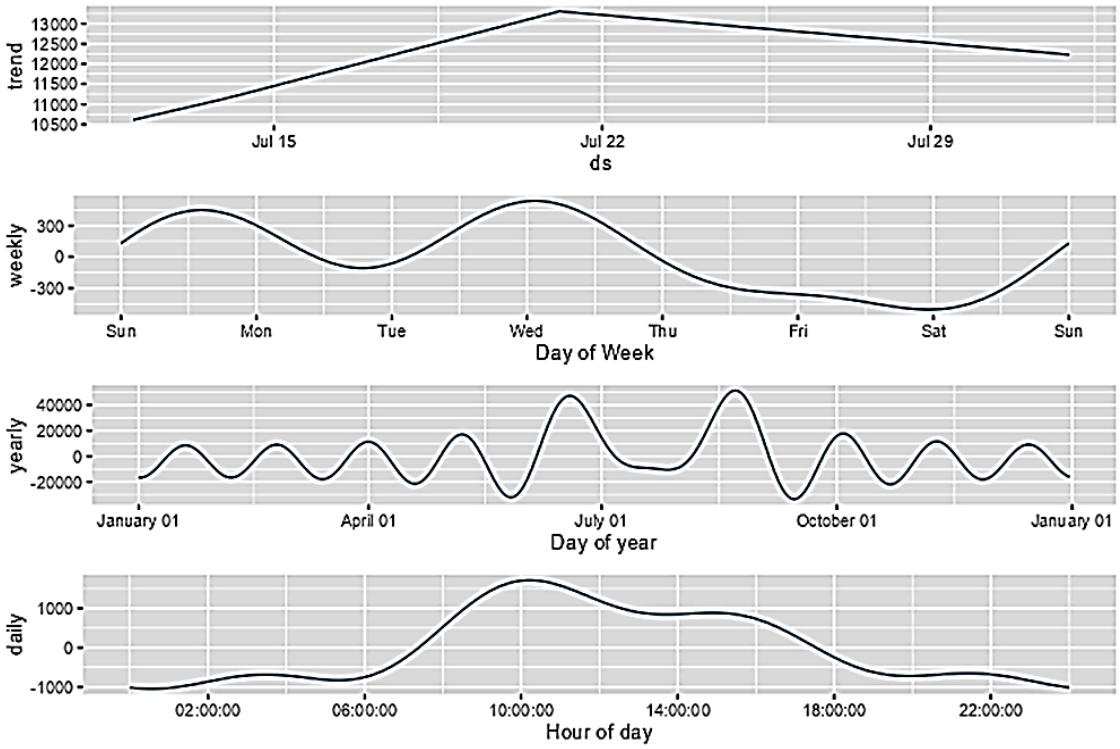


Рис. 6. Декомпозиция временного ряда общего числа атак

Fig. 6. Time Series Decomposition of Total Attacks Number

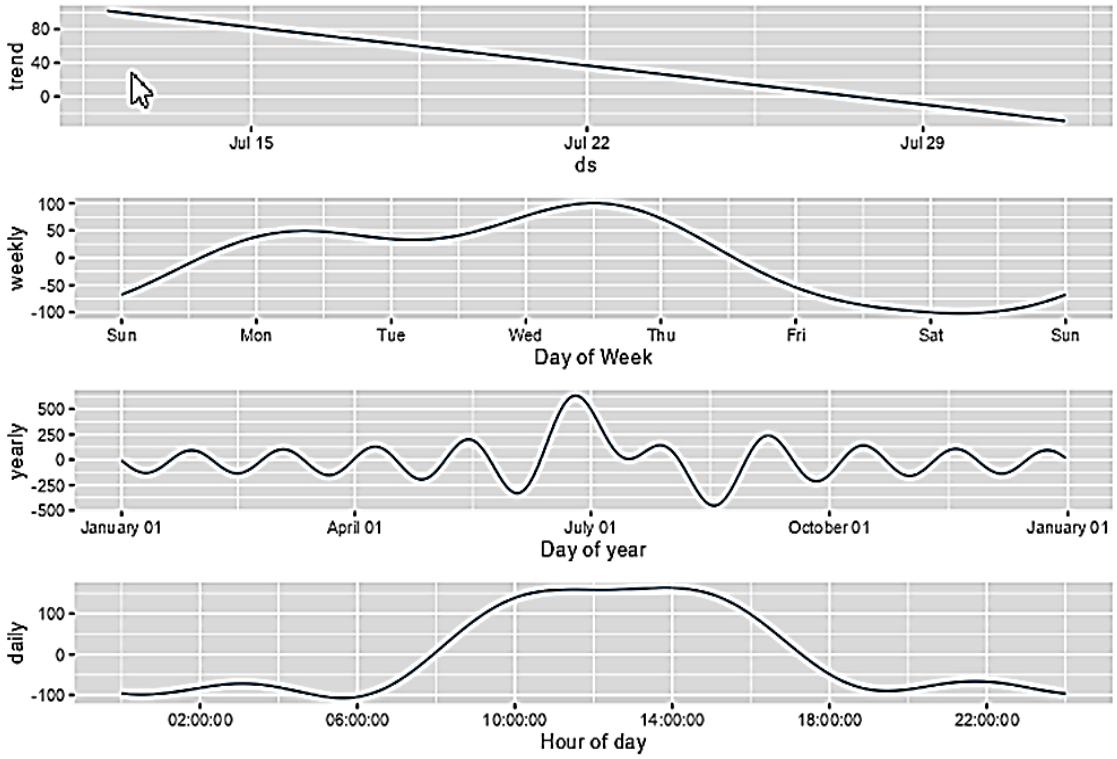


Рис. 7. Декомпозиция временного ряда числа критических атак

Fig. 7. Time Series Decomposition of Critical Attacks Number

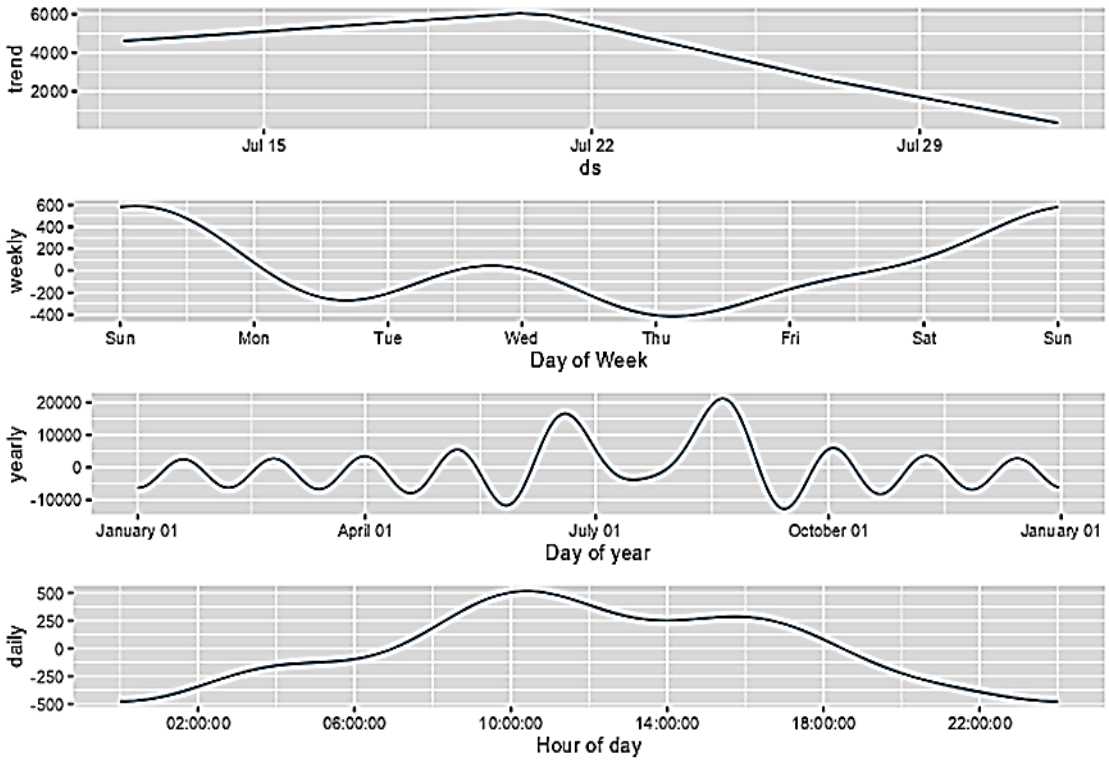
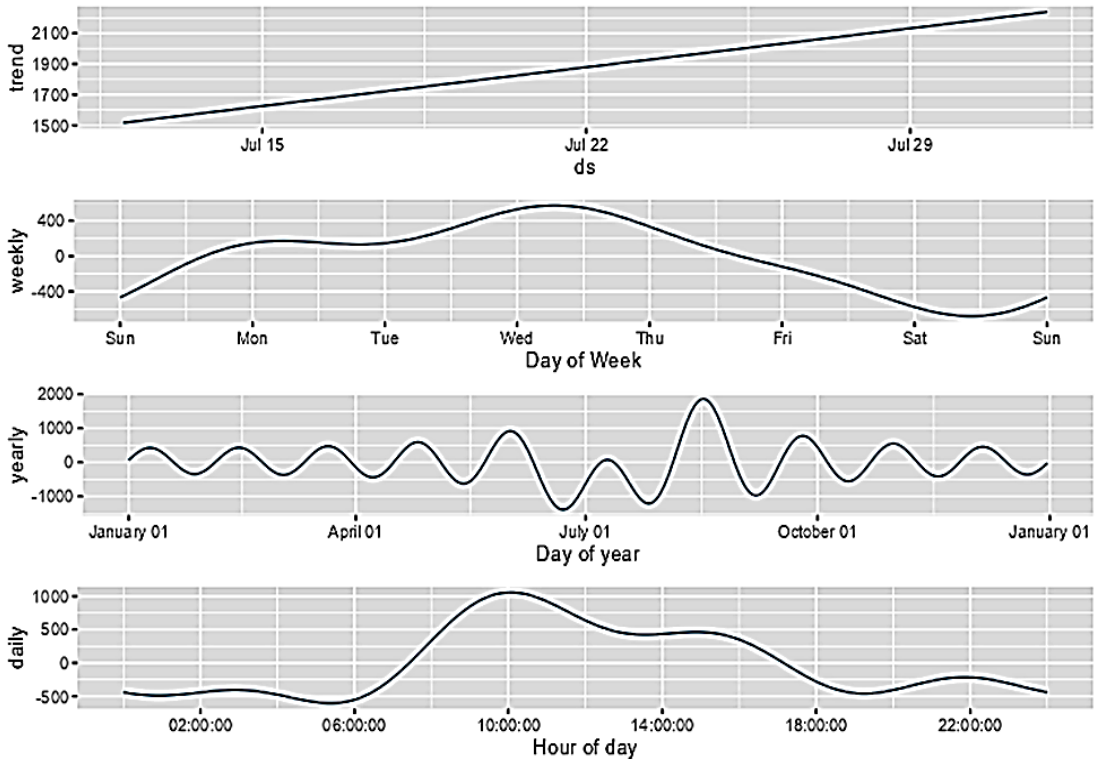


Рис. 8. Декомпозиция временного ряда числа опасных атак

Fig. 8. Time Series Decomposition of Dangerous Attacks Number



d)

Рис. 9. Декомпозиция временного ряда числа предупреждений

Fig. 9. Time Series Decomposition of Alerts Number

Декомпозиция показывает, что имеются точки излома тренда для двух временных рядов (общего числа атак и числа опасных атак). Таким образом, ряды могут содержать различные участки монотонности. Следовательно, с учетом их разведывательного анализа может возникнуть необходимость создавать их слайсы и для каждого слайса строить модель временного ряда. Вероятно, это сможет повысить качество модели.

Построенные модели сезонной декомпозиции показывают, что анализируемые ряды ведут себя по-разному. Так, например, для ряда с опасными атаками наибольшее число атак в среднем приходится на выходные. А для ряда, содержащего общее число атак и число критических атак – на среду. Эта информация является существенной для выбора и обоснования моментов повышенной готовности системы обнаружения и ликвидации последствий вторжений. Отметим, что для всех временных рядов, наибольшее число атак приходится на утренние часы, что также немаловажно для планирования работы системы обеспечения кибербезопасности.

Заключение

Полученные результаты показывают, что при решении задач прогнозирования кибератак на объекты информационной инфраструктуры целесообразно использовать методы теории временных рядов. Ее разработанность, наличие большого количества методов и инструментальных средств позволяют реализовать комплексный подход, основанный на их последовательном применении, построении различных моделей, а затем их сравнительном анализе. Проведенное исследование четырех временных рядов на примере информационной системы ведомственного вуза показывает, что в силу большой вариативности, зашумленности измерений, наличия случайной составляющей с большой дисперсией использование традиционных подходов к прогнозированию (например, методов регрессионного анализа), как правило, не эффективно. Так, коэффициент детерминации построенной модели для одного из временных рядов составляет не более 0,01, а исправленное его значение становится даже отрицательным!

Попытка предобработать временные ряды с использованием преобразования Бокса – Кокса также не позволяет существенно улучшить качество решаемой задачи. Поэтому в исследовании использованы методы экспоненциального сглаживания, позволяющие уменьшить дисперсию временных рядов. В дальнейшем результаты фильтрации могут быть применены при решении задач прогнозирования.

К сожалению, даже это не позволяет существенно улучшить качество исходных данных. Поэтому решение задачи прогнозирования возможно

только для небольшого горизонта прогноза, который в исследовании был задан равным трем суткам. Вероятно, его можно увеличить, но предварительно следует исследовать характер анализируемого временного ряда и возможность такого подхода. В любом случае, большая зашумленность данных не позволяет решать задачи долгосрочного прогнозирования. Задача прогнозирования кибератак является задачей краткосрочного или текущего прогнозирования и, следовательно, должна быть включена в средства мониторинга и бизнес-аналитики, например, в BI-платформы. Отметим, что в существующих рейтингах BI-платформ, таких как квадрант Гартнера, в 2023 г. появился критерий оценки «Интеграция с data science».

За последние годы появилось много новых методов прогнозирования временных рядов, например, STL [13], BSTS [14], Prophet [15]; широкое применения нашли методы пространства состояний, байесовской статистики и др. Возможно, их использование позволит повысить качество прогнозирования. Однако следует помнить, что нет «серебряной пули» – не метод, а качество исходных данных может обеспечить успех в прогнозировании. Заметим, что эта задача очень трудоемка (авторы статьи еще раз убедились в этом, формируя анализируемые временные ряды) и не может быть решена без разработки специальных средств парсинга данных.

Можно предположить, что использование «мягких вычислений» и нейронных сетей наряду с традиционными методами прогнозирования позволит получить более обоснованные результаты.

Список источников

1. Глазьев С.Ю. Теория долгосрочного технико-экономического развития. М.: ВлаДар, 1993. EDN:YSXIUV
2. Нильсен Э. Практический анализ временных рядов. Прогнозирование со статистикой и машинное обучение. СПб.: Диалектика, 2021. 544 с.
3. Хайндман Р., Атанасопулос Дж. Прогнозирование: принципы и практика. Пер. с англ. М.: ДМК Пресс, 2023. 458 с.
4. Исаев С.В., Кононов Д.Д. Исследование динамики и классификация атак на веб-сервисы корпоративной сети // Сибирский аэрокосмический журнал. 2022. Т. 23. № 4. С. 593–601. DOI:10.31772/2712-8970-2022-23-4-593-601. EDN:RUSJWB
5. Zuzčák M., Bujok P. Using honeynet data and a time series to predict the number of cyber attacks // Computer Science and Information Systems. 2021. Vol. 18. Iss. 4. PP. 1197–1217. DOI:10.2298/CSIS200715040Z
6. Ларионов К.О. Прогнозирование статистических данных атак на прикладное программное обеспечение // Проблемы современной науки и образования. 2021. № 6(163). С. 57–63. DOI:10.24411/2304-2338-2021-10606. EDN:PGVALC
7. Hobijn B., Franses P.H., Ooms M. Generalization of the KPSS-test for stationarity // Statistica Neerlandica. 2004. Vol. 58. Iss. 4. PP. 482–502. DOI:10.1111/j.1467-9574.2004.00272.x
8. Phillips P.C.B., Perron P. Testing for a Unit Root in Time Series Regression // Biometrika. 1988. Vol. 75. Iss. 2. PP. 335–346. DOI:10.1093/biomet/75.2.335. EDN:ILNEET
9. Hersbach H. Decomposition of the Continuous Ranked Probability Score for Ensemble Prediction Systems // Weather and Forecast. 2000. Vol. 15. Iss. 5. PP. 559–570. DOI:10.1175/1520-0434(2000)015<0559:DOTCRP>2.0.CO;2
10. Dawid A.P., Sebastiani P. Coherent Dispersion Criteria for Optimal Experimental Design // Annals of Statistics. 1999. Vol. 27. Iss. 1. PP. 65–81.
11. Bickel P.J., Doksum K.A. An Analysis of Transformations // Journal of the American Statistical Association. 1981. Vol. 76. Iss. 374. PP. 296–311. DOI:10.2307/2287831
12. Hyndman R.J., Koehler A.B., Snyder R.D., Grose S. A state space framework for automatic forecasting using exponential smoothing methods // International Journal Forecasting. 2002. Vol. 18. Iss. 3. PP. 439–454.
13. Cleveland R.B., Cleveland W.S., McRae J.E., Terpenning I.J. STL: A Seasonal-Trend Decomposition Procedure Based on Loess // Journal of Official Statistics. 1990. Vol. 6. Iss. 1. PP. 3–33.
14. Scott S., Varian H.R. Predicting the Present with Bayesian Structural Time Series // SSRN Electronic Journal. 2014. Vol. 5. Iss. 1/2. PP. 4–23. DOI:10.1504/IJMMNO.2014.059942
15. Мастицкий С.Э. Анализ временных рядов с помощью R. 2020. URL: https://ranalytics.github.io/tsa-with-r (дата обращения 19.12.2024)

References

1. Glazyev S.Yu. *Theory of Long-Term Technical and Economic Development*. Moscow: VlaDar Publ.; 1993. (in Russ.) EDN:YSXIUV
2. Nielsen E. *Practical Time Series Analysis. Forecasting with Statistics and Machine Learning*. St. Petersburg: Dialektika Publ.; 2021. 544 p. (in Russ.)
3. Hyndman R.J., Athanasopoulos G. *Forecasting: principles and practice.* OTexts; 2017. 292 p.
4. Isaev S.V., Kononov D.D. A Study of Dynamics and Classification of Attacks on Corporate Network Web Services. *The Siberian Aerospace Journal*. 2022;23(4):593–601. (in Russ.) DOI:10.31772/2712-8970-2022-23-4-593-601. EDN:RUSJWB
5. Zuzčák M., Bujok P. Using honeynet data and a time series to predict the number of cyber attacks. *Computer Science and Information Systems*. 2021;18(4):1197–1217. DOI:10.2298/CSIS200715040Z

6. Larionov K.O. Forecasting Attack Statistics on Applied Software. *Problemy sovremennoi nauki i obrazovaniia*. 2021;6(163):57–63. (in Russ.) DOI:10.24411/2304-2338-2021-10606. EDN:PGVALC
7. Hobijn B., Franses P.H., Ooms M. Generalization of the KPSS-test for stationarity. *Statistica Neerlandica*. 2004;58(4): 482–502. DOI:10.1111/j.1467-9574.2004.00272.x
8. Phillips P.C.B., Perron P. Testing for a Unit Root in Time Series Regression. *Biometrika*. 1988;75(2):335–346. DOI:10.1093/biomet/75.2.335. EDN:ILNEET
9. Hersbach H. Decomposition of the Continuous Ranked Probability Score for Ensemble Prediction Systems. *Weather and Forecast*. 2000;15(5):559–570. DOI:10.1175/1520-0434(2000)015<0559:DOTCRP>2.0.CO;2
10. Dawid A.P., Sebastiani P. Coherent Dispersion Criteria for Optimal Experimental Design. *Annals of Statistics*. 1999; 27(1):65–81.
11. Bickel P.J., Doksum K.A. An Analysis of Transformations. *Journal of the American Statistical Association*. 1981;76(374): 296–311. DOI:10.2307/2287831
12. Hyndman R.J., Koehler A.B., Snyder R.D., Grose S. A state space framework for automatic forecasting using exponential smoothing methods. *International Journal Forecasting*. 2002;18(3):439–454.
13. Cleveland R.B., Cleveland W.S., McRae J.E., Terpenning I.J. STL: A Seasonal-Trend Decomposition Procedure Based on Loess. *Journal of Official Statistics*. 1990;6(1):3–33.
14. Scott S., Varian H.R. Predicting the Present with Bayesian Structural Time Series. *SSRN Electronic Journal*. 2014;5(1/2):4–23. DOI:10.1504/IJMMNO.2014.059942
15. Mastitsky S.E. *Time series analysis using R*. 2020. URL: https://ranalytics.github.io/tsa-with-r [Accessed 19.12.2024]

Статья поступила в редакцию 20.12.2024; одобрена после рецензирования 27.01.2025; принята к публикации 12.02.2025.
The article was submitted 20.12.2024 approved after reviewing 27.01.2025; accepted for publication 12.02.2025.

Информация об авторах:

НАУМОВ Владимир Николаевич
доктор военных наук, профессор, заведующий кафедрой бизнес-информатики Северо-Западного института управления – филиала РАНХиГС
https://orcid.org/0000-0002-0385-3530

БУЙНЕВИЧ Михаил Викторович
доктор технических наук, профессор, профессор кафедры прикладной математики и безопасности информационных технологий Санкт-Петербургского университета ГПС МЧС России
https://orcid.org/0000-0001-8146-0022

СИНЕЩУК Максим Юрьевич
заместитель начальника центра информационных и коммуникационных технологий Санкт-Петербургского университета ГПС МЧС России
https://orcid.org/0009-0005-8108-3198

ТУКМАЧЕВА Марина Алексеевна
адъюнкт факультета подготовки кадров высшей квалификации Санкт-Петербургского университета ГПС МЧС России
https://orcid.org/0009-0004-2496-7117

Буйневич М.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.

Buinevich M.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.

План издания научной литературы 2025 г., п. 12

Усл.-печ. л.	Формат	Заказ
15,5	$60\times84_{1/8}$	№ 1616

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