

НАУКОЕМКИЕ ТЕХНОЛОГИИ В КОСМИЧЕСКИХ ИССЛЕДОВАНИЯХ ЗЕМЛИ

HIGH TECHNOLOGIES IN EARTH SPACE RESEARCH

Журнал **H&ES Research** издается с 2009 года, освещает достижения и проблемы российских инфокоммуникаций, внедрение последних достижений отрасли в автоматизированных системах управления, развитие технологий в информационной безопасности, исследования космоса, развитие спутникового телевидения и навигации, исследование Арктики. Особое место в издании уделено результатам научных исследований молодых ученых в области создания новых средств и технологий космических исследований Земли.

Журнал H&ES Research входит в перечень изданий, публикации в которых учитываются Высшей аттестационной комиссией России (ВАК РФ), в систему российского индекса научного цитирования (РИНЦ), а также включен в Международный классификатор периодических изданий.

Тематика публикуемых статей в соответствии с перечнем групп специальностей научных работников по Номенклатуре специальностей:

- 2.2.15 Системы, сети и устройства телекоммуникаций (техн. науки)
- 2.3.1 Системный анализ, управление и обработка информации (техн. науки)
- 2.3.5 Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей (техн. науки)
- 2.3.6 Методы и системы защиты информации, информационная безопасность (техн. науки)
- 2.5.13 Проектирование, конструкция и производство летательных аппаратов (техн. науки)
- 2.5.16 Динамика, баллистика, управление движением летательных аппаратов (техн. науки)

ИНДЕКСИРОВАНИЕ ЖУРНАЛА H&ES RESEARCH

• NEICON • CyberLenika (Open Science) • Google Scholar • OCLC WorldCat • Ulrich's Periodicals Directory • Bielefeld Academic Search Engine (BASE) • eLIBRARY.RU • Registry of Open Access Repositories (ROAR)

Все номера журнала находятся в свободном доступе на сайте журнала www.hes.ru и библиотеке elibrary.ru.

Всем авторам, желающим разместить научную статью в журнале, необходимо оформить ее согласно требованиям и направить материалы на электронную почту: HT-ESResearch@yandex.ru.

С требованиями можно ознакомиться на сайте: www.H-ES.ru.

Язык публикаций: русский, английский.

Периодичность выхода – 6 номеров в год.

Свидетельство о регистрации СМИ ПИ № ФС 77-60899 от 02.03.2015

Территория распространения: Российская Федерация, зарубежные страны

Тираж 1000 экз. Цена 1000 руб.

Плата с аспирантов за публикацию рукописи не взимается.

© ООО "ИД Медиа Паблишер", 2023

H&ES Research is published since 2009. The journal covers achievements and problems of the Russian infocommunication, introduction of the last achievements of branch in automated control systems, development of technologies in information security, space researches, development of satellite television and navigation, research of the Arctic. The special place in the edition is given to results of scientific researches of young scientists in the field of creation of new means and technologies of space researches of Earth.

The journal H&ES Research is included in the list of scientific publications, recommended Higher Attestation Commission Russian Ministry of Education for the publication of scientific works, which reflect the basic scientific content of candidate and doctoral theses. IF of the Russian Science Citation Index.

Subject of published articles according to the list of branches of science and groups of scientific specialties in accordance with the specialties:

- 2.2.15 Telecommunication systems, networks and devices
- 2.3.1 System analysis, management and information processing
- 2.3.5 Mathematical and software support for computing systems, complexes and computer networks
- 2.3.6 Methods and systems of information security
- 2.5.13 Design, construction and production of aircraft
- 2.5.16 Dynamics, ballistics, aircraft motion control

JOURNAL H&ES RESEARCH INDEXING

All issues of the journal are in a free access on a site of the journal www.hes.ru and elibrary.ru.

All authors wishing to post a scientific article in the journal, you must register it according to the requirements and send the materials to your email: HT-ESResearch@yandex.ru.

The requirements are available on the website: www.H-ES.ru.

Language of publications: Russian, English.

Periodicity – 6 issues per year.

Media Registration Certificate PI No. FS77-60899, Date of issue: March 2, 2015.

Distribution Territory: Russian Federation, foreign countries

Circulation of 1000 copies. Price of 1000 Rub.

Postgraduate students for publication of the manuscript will not be charged

© "Media Publisher", LLC, 2023

Учредитель:

ООО "ИД Медиа Паблшер"

Издатель:

ДЫМКОВА С.С.

Главный редактор:

ЛЕГКОВ К.Е.

Редакционная коллегия:

БОБРОВСКИЙ В.И., д.т.н., доцент;
БОРИСОВ В.В., д.т.н., профессор,
Действительный член академии военных наук РФ;

БУДКО П.А., д.т.н., профессор;

БУДНИКОВ С.А., д.т.н., доцент,

Действительный член Академии информатизации образования;

ВЕРХОВА Г.В., д.т.н., профессор;

ГОНЧАРОВСКИЙ В.С., д.т.н.,

профессор, заслуженный деятель науки и техники РФ;

КОМАШИНСКИЙ В.И., д.т.н., профессор;

КИРПАНЕВ А.В., д.т.н., доцент;

КУРНОСОВ В.И., д.т.н., профессор,

академик Международной академии информатизации, Действительный член Российской академии естественных наук;

МОРОЗОВ А.В., д.т.н., профессор,

Действительный член Академии военных наук РФ;

МОШАК Н.Н., д.т.н., доцент;

ПАВЛОВ А.Н., д.т.н., профессор;

ПРОРОК В.Я., д.т.н., профессор;

СЕМЕНОВ С.С., д.т.н., доцент;

СИНИЦЫН Е.А., д.т.н., профессор;

ШАТРАКОВ Ю.Г., д.т.н., профессор,

заслуженный деятель науки РФ.

Адрес издателя:

111024, Россия, Москва,
ул. Авиамоторная, д. 8, корп. 1, офис 323.

Адрес редакции:

194044, Россия, Санкт-Петербург,
Лесной Проспект, 34-36, к. 1,
Тел.: +7(911) 194-12-42.

Адрес типографии:

Россия, Москва, ул. Складочная, д. 3,
кор. 6.

Мнения авторов не всегда совпадают с точкой зрения редакции.

За содержание рекламных материалов редакция ответственности не несет.

Материалы, опубликованные в журнале – собственность ООО "ИД Медиа Паблшер".

Перепечатка, цитирование, дублирование на сайтах допускаются только с разрешения издателя.

СОДЕРЖАНИЕ

АВИАЦИОННАЯ И РАКЕТНО-КОСМИЧЕСКАЯ ТЕХНИКА

Бестугин А.Р., Киршина И.А., Коврегин В.Н., Антохин Е.А., Саута О.И.

Способ проактивной компенсации мешающих отражений при радиолокационном наблюдении малоразмерных объектов на фоне подстилающей поверхности

4

РАДИОТЕХНИКА И СВЯЗЬ

Будко Н.П., Аллакин В.В., Каретников В.В.

Метод передачи аварийных сигналов на распределенной информационно-телекоммуникационной сети Росморречфлота

10

Столбинский Д.В., Бем П.П., Андреев В.А., Матвеев Д.В.

Воздействие внешних условий на работоспособность радиоэлектронных средств (РЭС)

18

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

Бужин И.Г., Деревянкин А.Ю., Антонова В.М., Перевалов А.П., Миронов Ю.Б.

Эффективность фреймворков для передачи информации в виртуализированной сети связи с микросервисной архитектурой

23

Уймин А.Г., Никитин О.Р.

Сравнение производительности алгоритмов классификации в рамках сетевой инфраструктуры

33

Маркевич Д.В., Харланова В.В., Хомоненко А.Д.

Интеграция систем бизнес-аналитики с системами управления базами данных на транспорте

41

Воронин Е.А., Козлов С.В., Кубанков А.Н.

Идентификация угроз средствами обеспечения безопасности и выбор защиты методами машинного обучения

49



CONTENTS

AVIATION, SPACE-ROCKET HARDWARE

**Bestugin A.R., Kirshina I.A., Kovregin V.N.,
Antochin E.A., Sauta O.I.**

A method for proactive compensation of interfering reflections during radar observation of small-sized objects against the background of the underlying surface

4

RF TECHNOLOGY AND COMMUNICATION

Budko N.P., Allakin V.V., Karetnikov V.V.

Method of transmission of emergency signals on the distributed information and telecommunication network of Rosmorrechflot

10

Stolbinsky D.V., Bem P.P., Andreev V.A., Matveev D.V.

The impact of external conditions on the performance of radio-electronic means (RES)

18

INFORMATICS, COMPUTER ENGINEERING AND CONTROL

**Buzhin I.G., Derevyankin A. Yu., Antonova V.M.,
Perevalov A.P., Mironov Yu.B.**

The effectiveness of frameworks for transmitting information in a virtualized communication network with a microservice architecture

23

Uimin A.G., Nikitin O.R.

Comparison of classification algorithms performance within network infrastructure

33

Markevich D.V., Kharlanova V.V., Khomonenko A.D.

Integration of business intelligence systems with database management systems in transport

41

Voronin E.A., Kozlov S.V., Kubankov A.N.

Threats identification by security and protection selection by machine learning methods

49

Founder:

"Media Publisher", LLC

Publisher:

DYMKOVA S.S.

Editor in chief:

LEGKOV K.E.

Editorial board:

BOBROWSKY V.I., PhD, Docent;
BORISOV V.V., PhD, Full Professor;
BUDKO P.A., PhD, Full Professor;
BUDNIKOV S.A., PhD, Docent,
Actual Member of the Academy of
Education Informatization;
VERHOVA G.V., PhD, Full Professor;
GONCHAREVSKY V.S., PhD, Full
Professor, Honored Worker of Science
and Technology of the Russian Federation;
KOMASHINSKIY V.I., PhD, Full Professor;
KIRPANEV A.V., PhD, Docent;
KURNOSOV V.I., PhD, Full Professor,
Academician of the International Academy
of Informatization, law and order, Member
of the Academy of Natural Sciences;
MOROZOV A.V., PhD, Full Professor,
Actual Member of the Academy of Military
Sciences;
MOSHAK N.N., PhD, Docent;
PAVLOV A.N., PhD, Full Professor;
PROROK V.Y., PhD, Full Professor;
SEMEV S.S., PhD, Docent;
SINICYN E.A., PhD, Full Professor;
SHATRAKOV Y.G., PhD, Full Professor;
Honored Worker of Science of the Russian
Federation.

Address of publisher:

111024, Russia, Moscow,
st. Aviamotornaya, 8, bild. 1, office 323

Address of edition:

194044, Russia, St. Petersburg,
Lesnoy av., 34-36, h.1,
Phone: +7 (911) 194-12-42.

Address of printing house:

Russia, Moscow, st. Skladochnaya, 3, h. 6

The opinions of the authors don't always coincide with the point of view of the publisher. For the content of ads, the editorial Board is not responsible. All articles and illustrations are copyright. All rights reserved. No reproduction is permitted in whole or part without the express consent of Media Publisher Joint-Stock company.

doi: 10.36724/2409-5419-2023-15-2-4-9

СПОСОБ ПРОАКТИВНОЙ КОМПЕНСАЦИИ МЕШАЮЩИХ ОТРАЖЕНИЙ ПРИ РАДИОЛОКАЦИОННОМ НАБЛЮДЕНИИ МАЛОРАЗМЕРНЫХ ОБЪЕКТОВ НА ФОНЕ ПОДСТИЛАЮЩЕЙ ПОВЕРХНОСТИ

БЕСТУГИН

Александр Роальдович¹

КИРШИНА

Ирина Анатольевна²

КОВРЕГИН

Валерий Николаевич³

АНТОХИН

Евгений Александрович⁴

САУТА

Олег Иванович⁵

Сведения об авторах:

¹ д.т.н., профессор, директор института "Радиотехники, электроники и связи", ГУАП, Санкт-Петербург, Россия, freshguar@mail.ru

² к.э.н., доцент, кафедра "Кафедра конструирования и технологий электронных и лазерных средств", ГУАП, Санкт-Петербург, Россия, ikirshina@mail.ru

³ к.т.н., доцент, кафедра аэрокосмических измерительно-вычислительных комплексов, ГУАП, Санкт-Петербург, Россия, kovregin@mail.ru

⁴ к.т.н., кафедра радиотехнических систем, ГУАП, Санкт-Петербург, Россия, fresguar@mail.ru

⁵ д.т.н., кафедра "Кафедра конструирования и технологий электронных и лазерных средств", ГУАП, Санкт-Петербург, Россия, sauta-oleg@yandex.ru

АННОТАЦИЯ

Введение: Низкая вероятность радиолокационного обнаружения малоразмерного летательного аппарата (МЛА) определяется как его малой эффективной поверхностью рассеяния радиоволн, так и наличием мешающих (перотраженных) радиосигналов, формируемых при отражении зондирующего сигнала радиолокатора от подстилающей земной поверхности, на фоне которой производится поиск и наблюдение МЛА. Мощность таких отраженных сигналов может значительно превышать мощность сигналов, отраженных от самого МЛА, а многолепестковый характер диаграммы направленности антенны радиолокатора в еще большей степени способствует маскировке полезного сигнала (отражения от МЛА) при его поиске. Для повышения вероятности радиолокационного обнаружения МЛА применяется множество различных способов, связанных с формированием специальных зондирующих сигналов, с различными видами пространственной и частотной фильтрации, с разработкой специальных конструкций антенн и антенных решеток. Однако, большинство применяемых способов требует достаточно сложных технических решений, практическая реализация которых зачастую невозможна или чрезмерно затруднена. **Предложен способ** повышения вероятности обнаружения МЛА на фоне отраженных от рельефа сигналов за счет использования в алгоритмах вторичной обработки радиолокационных сигналов проактивного способа расчета поля помех, основанного на синтезе сигнала, формируемого с использованием модели рельефа подстилающей поверхности и компенсации в выходном сигнале приемника радиолокатора составляющей, обусловленной отражением от рельефа. Реализация предложенного способа основана на использовании математического аппарата теории распространения радиоволн в приближении геометрической оптики. Приведены требования к основным характеристикам цифровой модели подстилающей поверхности и ресурсам вычислительного устройства для реализации такого способа. Дана экспертная оценка повышения вероятности обнаружения МЛА. **Результаты работы** могут быть использованы в бортовых вычислительных устройствах радиолокационных системах для задач обнаружения МЛА, определения координат и прогнозирования траектории их движения.

Исследование выполнено при финансовой поддержке Российского Научного Фонда, проект № 22-19-00058.

КЛЮЧЕВЫЕ СЛОВА: радиолокация, цифровая карта местности, диаграмма направленности, летательный аппарат.

Для цитирования: Бестугин А.Р., Киршина И.А., Коврегин В.Н., Антохин Е.А., Саута О.И. Способ проактивной компенсации мешающих отражений при радиолокационном наблюдении малоразмерных объектов на фоне подстилающей поверхности // Научные технологии в космических исследованиях Земли. 2023. Т. 15. № 2. С. 4-9. doi: 10.36724/2409-5419-2023-15-2-4-9



Введение. Постановка задачи исследования

В настоящее время для бортовых авиационных радаров сохраняет актуальность проблема обеспечения возможности обнаружения малоскоростных маловысотных малоразмерных летательных аппаратов (МЛА) в условиях, когда относительно слабый доплеровский сигнал ЛА перекрывается спектром мощных мешающих (маскирующих) отражений от подстилающей поверхности (МОП) по направлениям главного (ГЛ) и/или боковых лепестков (БЛ) диаграммы направленности антенны РЛС. Актуальность разрешения этой проблемы сейчас значительно возрастает в связи с интенсивным развитием/применением беспилотных ЛА, причем преимущественно МЛА, обнаружение которых на фоне МОП типовыми РЛС затруднено и во многих практических случаях не представляется возможным.

При поиске/обнаружении МЛА бортовой РЛС типичными являются ситуации: а) при малой высоте РЛС ее ГЛ ориентирован в околоразностное свободное пространство и МОП формируются только на участках поверхности, облучаемых БЛ; б) при большой высоте РЛС ее ГЛ и некоторые БЛ ориентированы вниз и МОП формируется на соответствующих участках земли.

В настоящее время ведутся активные исследования по разрешению указанной проблемы в таких ситуациях [1-5]. Используются различные подходы и методы, например: разработка специальных конструкций антенн и антенных решеток РЛС [4]; в ситуации а) применение специальных режимов ЛЧМ-излучения, обеспечивающих частотное разнесение спектров МОП и эхосигнала МЛА [2, 3]; различные способы компенсации МОП [1].

В настоящей работе рассматривается проактивный способ компенсации мощных МОП, маскирующих относительно слабый сигнал от МЛА. Способ основан на цифровом синтезе модели сигнала, отраженного от поверхности с использованием модели рельефа поверхности для аналитического расчета параметров отраженного сигнала. При синтезе модели отраженного сигнала также учитывается форма и текущая ориентация ДНА, параметры траектории фазового центра антенны, определяемые средствами микронавигации РЛС [2, 5], в том числе и относительно элементов (ячеек) модели рельефа земной поверхности – цифровой карты местности (ЦКМ).

Для иллюстрации ситуации б), в основном рассматриваемой в данной работе, на рис.1 показано относительное расположение самолета с РЛС, МЛА (например, квадрокоптера) и элементов ЦКМ, где эллипсом выделена область поверхности, «засвечиваемая» РЛС и показаны элементы (факеты) ЦКМ, от которых происходит зеркальное отражение зондирующих сигналов.

Следует отметить, что современные ЦКМ, широко используемые в авиационных приложениях, характеризуются высокой точностью и надежностью представления данных [6], содержат информация об отражающих свойствах поверхности, искусственных и естественных объектах на ее поверхности и др.

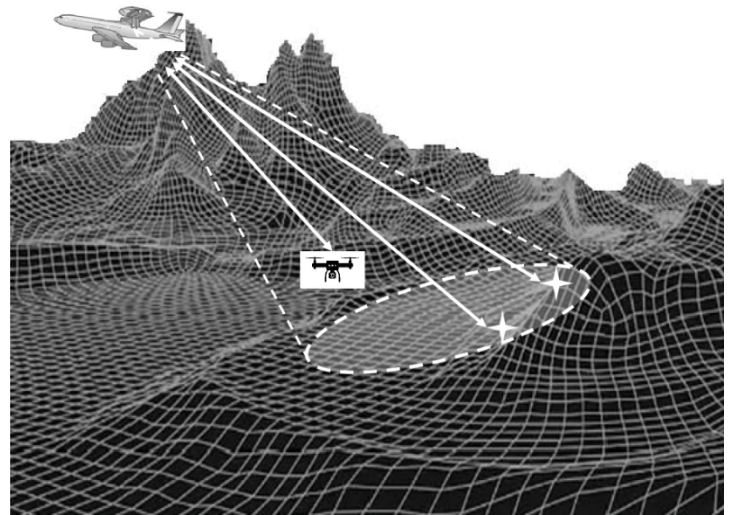


Рис. 1. Иллюстрация относительного расположения РЛС, малоразмерного летательного аппарата и факетов ЦКМ (отмечены звездой)

Это позволяет создать адекватную модель отраженных от подстилающей поверхности сигналов. Использование такой модели для компенсации пассивных помех от земли позволит повысить вероятность обнаружения полезного сигнала на фоне МОП в ситуации б) и повысить высокоточную адаптивную режекцию МОП в процедурах адаптивно-робастного наблюдения МЛА на основе ЛЧМ-излучений [2, 3].

1. Цифровой синтез отраженных радиолокационных сигналов

Существует несколько способов математического моделирования отраженного сигнала в раскрыве антенны, которые можно обобщить следующим образом:

- способы моделирования, основанные на решении задачи распространения радиоволн или задачи дифракции электромагнитного поля на подстилающей поверхности с присутствием ей пространственными и электрическими характеристиками;

- способы, в основу которых положен феноменологический подход, при котором исключают из рассмотрения механизм рассеяния и отражения электромагнитного поля поверхностью и заменяются пространственно-электрические характеристики поверхности на соответствующие характеристики отраженного сигнала, известные в большинстве случаев из экспериментальных данных для конкретных типовых случаев и физических представлений;

- способы моделирования, основанные на чисто эмпирических данных об отраженных сигналах, которые, как и предыдущие, не затрагивают реального механизма рассеяния и являются по существу моделью сигнала; при этом на основании знания законов распределения параметров отраженного сигнала и корреляционных связей строится статистический эквивалент самого сигнала.

Бортовая реализация ряда известных способов в реальном масштабе времени затруднена в рамках типичных ограничений по вычислительно-интерфейсному ресурсу РЛС. В то же время могут использоваться разновидности геометрических моделей, в которых все отражающие поверхности представляются совокупностью отражателей или плоских площадок – фасетов [7-11], а сигнал на входе приемной антенны равен сумме сигналов, отраженных от всех видимых, но, как правило, статистически независимых фасетов.

Этот принцип позволяет заменить сложные пространственно-электрические характеристики реальных поверхностей на обобщенную характеристику – эффективную поверхность рассеяния (или отражения), заданную для фиксированных поляризации, длины волны и угла облучения (см. рис. 2), зависящую от типа подстилающей поверхности и диаграммы обратного рассеяния (ДОР).

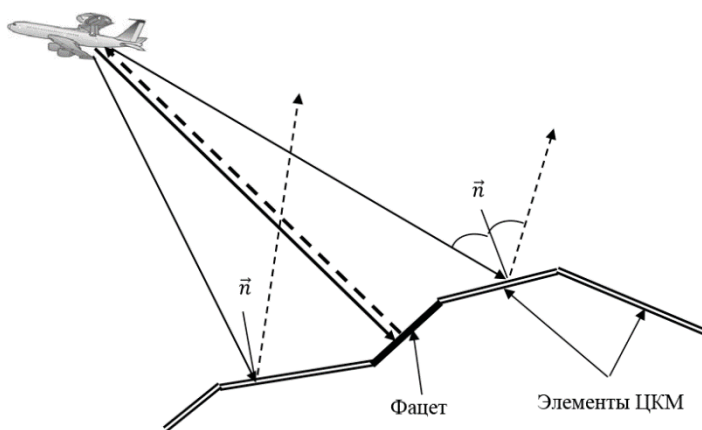


Рис. 2. Иллюстрация учета лучей в алгоритме синтеза модели сигнала, отраженного от фасета ЦКМ в приближении геометрической оптики (вертикальная плоскость)

Предполагается, что отражение от каждого фасета происходит как от точечного отражателя. При этом, каждый фасет, кроме своих координат в ЦКМ, может иметь дополнительные параметры: коэффициент отражения, форму ДОР, сдвиг фазы при отражении, смещение (отклонение) по высоте относительно среднего уровня горизонтальной плоскости и углы отклонения нормали фасета от оси ДОР и др. Важную роль в моделировании МОП играет вопрос рационального (оптимального) определения размера и количества фасетов (по критерию вида «адекватность модели/вычислительная сложность».)

В рассматриваемом нами способе вычисляется сигнал от каждого фасета и суммируется с учетом фазы. Оптимальное число фасетов по дальности выбирается исходя из разрешающей способности РЛС, и в общем случае число фасетов равно числу разрешаемых элементов или числу элементов ЦКМ в зоне, засвечиваемой ДН антенны РЛС. По азимуту в режиме обзора разбиение осуществляется на основании скорости сканирования, длительности накапливаемого сигнала и разрешающей способности РЛС. Известно, что наиболее удачные модели, построенные на основе описанного способа, хорошо согласуются с экспериментальными данными [6-9].

В общем виде алгоритм моделирования отраженного сигнала включает в себя следующие этапы:

- трассировка лучей до всех фасетов в области подстилающей поверхности, облучаемой (засвечиваемой) ДН антенны РЛС в текущий момент времени,
- расчет радиометрических характеристик отраженных от фасетов сигналов: амплитуды и фаза;
- суммирование ансамбля отраженных лучей с учетом их амплитуды и фазы.

Моделирование проводится в приближении геометрической оптики [7]. Лучи последовательно трассируются из положения фазового центра антенны РЛС с некоторым угловым шагом по углу места и азимуту в направлении подстилающей поверхности (ЦКМ). После того как все лучи трассированы и получена отражательная способность поверхности из точек падения лучей в направлении к радару, то происходит их суммирование с учетом ДНА РЛС и процесс повторяется для следующего положения и ориентации ЛА в пространстве. Интенсивность отражения лучей рассчитывается согласно модели диффузного и зеркального отражения. Интенсивность диффузного отражения получается путем вычисления выражения:

$$I_d = d \langle \vec{n} \cdot \vec{r} \rangle, \quad (1)$$

где d – коэффициент диффузного отражения от фасета, \vec{n} – вектор нормали к поверхности фасета, \vec{r} – направление падающего луча. Интенсивность зеркального отражения:

$$I_s = s \langle \vec{n} \cdot \vec{h} \rangle, \quad (2)$$

где s – представляет коэффициент зеркального отражения фасета, \vec{h} – вектор разности между вектором, в направлении к антенне РЛС и направлением вектора отраженного луча.

Обобщенная структурная схема способа компенсации МОП в интересах повышения вероятности обнаружения МЛА на фоне земной поверхности представлена на рисунке 3.

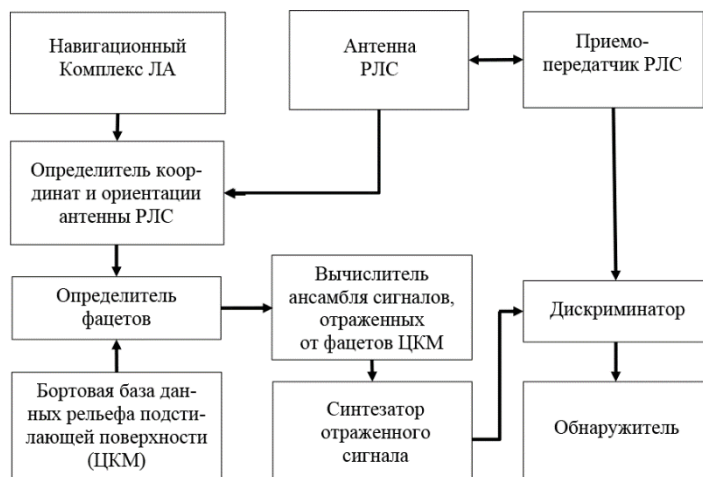


Рис. 3. Способ проактивной компенсации МОП для повышения вероятности обнаружения МЛА на фоне подстилающей земной поверхности

В соответствии с рисунком 3 рассматриваемый способ включает: определение координат и ориентации антенны РЛС на основе информации от навигационного комплекса ЛА и системы управления антенной РЛС, определение (выделение) фазетов в засвечиваемой области ЦКМ, вычисление сигналов, отраженных от выбранных фазетов и синтез суммарного отраженного сигнала. Далее, в дискриминаторе, из поступившего с выхода приемника РЛС сигнала осуществляется вычитание модели синтезированного сигнала и разностный сигнал поступает на вход обнаружителя.

Следует отметить, что для сокращения объема вычислений при расчете ансамбля сигналов, отраженных от фазетов ЦКМ (см. рис. 2), естественно применять метод «обратной трассировки» [7], когда отслеживание лучей производится не от источника, а в обратном направлении и учитываются только те лучи, которые формируют суммарный сигнал. Метод предусматривает геометрические преобразования, например, разбиение геометрических моделей на примитивы (полигоны, сплайны или др.) и модельные преобразования, включающие аффинные операции переноса, поворота и изменения масштаба.

2 Компенсация отраженного сигнала

Мощность сигнала, которая приходит в антенну РЛС от всех k фазетов ЦКМ, попавших в данный момент в пятно «засвета» на ЦКМ от ДНА, может быть рассчитана на основе обобщенного уравнения радиолокации [8] следующим образом:

$$P_c = \sum_{i=1}^k \left(\frac{P_u G^2 \lambda^2 \sigma_i}{(4\pi)^3 R_i^4} \right) I_i, \quad (3)$$

где P_c – средняя мощность пришедшего к антенне отраженного сигнала, P_u – мощность, излученная через антенну, G – коэффициент усиления антенны, λ – длина волны излучения, σ_i – эффективная поверхность рассеяния фазета, от которого происходит отражение, R_i – дальность до i -ого фазета.

Коэффициент интенсивности отражения лучей I_i от i -ого фазета, используемый в выражении (3), представляет собой сумму интенсивностей диффузного и зеркального отражения, определяемые в соответствии с выражениями (1) и (2):

$$I_i = I_d^i + I_s^i. \quad (4)$$

Иллюстрация эффекта компенсации в выходном сигнале приемника составляющей, обусловленной отражением зондирующих сигналов от рельефа земной поверхности, при использовании в вычислительном устройстве РЛС рассмотренного в настоящей работе способа, приведена на рисунке 4, на котором ось абсцисс – время (t), а ось ординат – напряжение (v).

Следует также отметить, что в настоящее время для аппроксимации рельефа широко используются фрактальные поверхности [13], состоящие из случайно заданных полигональных или биполиномиальных поверхностей. Одно из преимуществ таких поверхностей состоит в том, что для них можно получить любой уровень детализации, независимо от того, насколько близко мы к ним находимся.

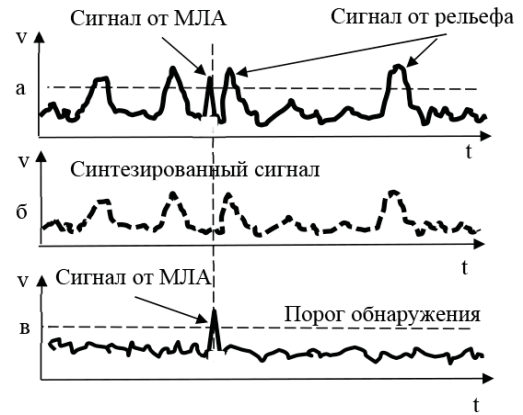


Рис. 4. Иллюстрация эффекта компенсации отраженного сигнала в задаче наблюдения МЛА на фоне рельефа подстилающей поверхности: а – сигналы от рельефа и наблюдаемого МЛА на выходе приемника РЛС; б – синтезированный на основе ЦКМ отраженный сигнал; в – разностный сигнал на выходе дискриминатора

Этим свойством широко пользуются, например, в машинной графике, так как фракталы реализуются простыми и быстрыми итерационными алгоритмами.

Таким образом, при моделировании сигналов, отраженных от элементов ЦКМ, с использованием фрактальных поверхностей имеются дополнительные возможности повышения адекватности представления синтезируемых отраженных сигналов и одновременного снижения требований к вычислительным ресурсам.

Заключение

В настоящей работе рассматривается проактивный способ компенсации мощных МОП, маскирующих относительно слабый сигнал от МЛА. Способ основан на цифровой синтезе модели сигнала, отраженного от поверхности с использованием модели рельефа поверхности для аналитического расчета параметров отраженного сигнала.

Основным преимуществом предлагаемого способа является отсутствие необходимости аппаратной модернизации бортовых радиолокационных систем и относительно невысокие требования к ресурсам бортового вычислительного комплекса.

Предложенный в работе способ дополняет известные методы повышения вероятности обнаружения радиолокационных сигналов и может использоваться совместно с ними.

Литература

1. *Авиационные системы радиовидения* / Под ред. Г.С. Кондратенкова. М.: Радиотехника, 2015. 648 с.
2. *Коврегин В.Н., Коврегина Г.М.* Адаптивно-робастные методы обнаружения, захвата и сопровождения зависших, мало- и высокоскоростных объектов в интегрированных радиолокационно-инерциальных системах с квазинепрерывным излучением // Сборник материалов «XXVIII Санкт-Петербургской международной конференции по интегрированным навигационным системам», Санкт-Петербург, 2021. С. 76-79.
3. *Коврегин В.Н., Коврегина Г.М.* Способ обнаружения, изменения дальности и скорости низколетящей малоскоростной цели в

импульсно-доплеровских радиолокационных станциях при высокой частоте повторения импульсов и инвертируемой линейной частотной модуляцией. Патент на изобретение № 2697509 от 15.08.2019.

4. *Бахолдин В.С., Гаврилов В. А., Шалдаев А.В.* Алгоритмы формирования радиолокационных изображений земной поверхности при использовании сигналов ГЛОНАСС // Изв. вузов. Приборостроение. Т. 55, № 9, 2012. С. 24-29.

5. *Чернодаров А.В., Патрикеев А.П., Коврегин В.Н., Коврегина Г.М.* Использование инерциально-спутниковой навигационной системы для определения параметров движения фазового центра антенны радиолокатора // XXIII Санкт-Петербургская международная конференция по интегрированным навигационным системам. СПб: ОАО «Концерн «ЦНИИ «Электроприбор», 2016. С. 266-274.

6. *Марков Ю.В., Боков А.С., Важенин В.Г., Мухин В.В., Нестеров М.Ю., Иофин А.А.* Моделирование отраженных радиолокационных сигналов для многоканальной системы дистанционного зондирования земли // Надежность и качество сложных систем. 2020. № 1 (29). С. 24-34. DOI 10.21685/2307-4205-2020-1-3.

7. *Голованов Н.Н.* Геометрическое моделирование. М.: Издательство Физико-математической литературы, 2002. 472 с.

8. *Сосновский А.А., Хаймович И.А., Лутин Э.А., Максимов И.Б.* Авиационная радионавигация: справочник; под ред. А.А. Сосновского. М.: Транспорт, 1990. 264 с.

9. *Жердев Д.А., Минаев Е.Ю., Фурсов В.А.* Моделирование радиолокационных изображений с использованием программно-моделирующего конструктора радиолокационных карт // Информационные технологии и нанотехнологии. 2016. С. 586-590.

10. Комплексное геоинформационно-фотограмметрическое моделирование рельефа: учебное пособие. М.: Изд-во МИИГАиК. 2019. 175 с.

11. *Борисов С.В., Выболдин Ю.К.* Исследование точности измерения радиальных размеров подповерхностных объектов при георадиолокации // В сборнике: Инновации и перспективы развития горного машиностроения и электромеханики: IPDME-2021. Санкт-Петербург, 2021. С. 327-328.

A METHOD FOR PROACTIVE COMPENSATION OF INTERFERING REFLECTIONS DURING RADAR OBSERVATION OF SMALL-SIZED OBJECTS AGAINST THE BACKGROUND OF THE UNDERLYING SURFACE

ALEXANDER R. BESTUGIN

St. Petersburg, Russia, freshguap@mail.ru

IRINA A. KIRSHINA

St. Petersburg, Russia, ikirshina@mail.ru

VALERY N. KOVREGIN

St. Petersburg, Russia, kovregin@mail.ru

EVGENIY A. ANTOCHIN

St. Petersburg, Russia, fresguap@mail.ru

OLEG I. SAUTA

St. Petersburg, Russia, sauta-oleg@yandex.ru

ABSTRACT

Introduction: The low probability of radar detection of a small-sized aircraft (MLA) is determined both by its small effective scattering surface of radio waves and by the presence of interfering (re-reflected) radio signals generated by the reflection of the radar sounding signal from the underlying earth's surface, against which the search and observation are carried out MLA. The power of such reflected signals can significantly exceed the power of the signals reflected from the MLA itself, and the multi-lobe nature of the radar antenna pattern further contributes to masking the useful signal (reflections from the MLA) during its search. To increase the probability of radar detection of MLA, many different methods are used, associated with the formation of special probing signals, with various types of spatial and frequency filtering, with the development of special designs of antennas and antenna arrays. However, most of the **methods** used require rather complex technical solutions, the practical implementation of which is often impossible or excessively difficult. A method is proposed for increasing the probability of detecting MLA

KEYWORDS: radar, digital map of the area, radiation pattern, aircraft

against the background of signals reflected from the relief by using a proactive method for calculating the interference field in the algorithms for secondary processing of radar signals, based on the synthesis of a signal generated using a relief model of the underlying surface and compensation in the output signal. radar receiver component due to reflection from the terrain. **Results:** The implementation of the proposed method is based on the use of the mathematical apparatus of the theory of radio wave propagation in the approximation of geometric optics. The requirements for the main characteristics of the digital model of the underlying surface and the resources of the computing device for the implementation of this method are given. An expert assessment of increasing the probability of detecting MLA is given. The results of the work can be used in on-board computing devices and radar systems for the tasks of detecting small aircraft, determining coordinates and predicting their trajectory. The paper deals with the problems of managing the management of a multi-functional satellite communication system in solving problems of information exchange using cloud technologies.

REFERENCES

1. Aircraft radio vision systems / Ed. G.S. Kondratenkov. Moscow: Radiotekhnika, 2015. 648 p.
2. V.N. Kovregin, G.M. Kovregina. Adaptive-robust methods for detecting, capturing and tracking hovering, low- and high-speed objects in integrated radar-inertial systems with quasi-continuous radiation. *Collection of materials "XXVIII St. Petersburg International Conference on Integrated Navigation Systems"*, St. Petersburg, 2021, pp. 76-79.
3. V.N. Kovregin, G.M. Kovregina. A method for detecting, measuring the range and speed of a low-flying low-speed target in pulse-Doppler radar stations at a high pulse repetition rate and inverted linear frequency modulation. Patent for invention No. 2697509 dated 08/15/2019.
4. V.S. Bakhoidin, V.A. Gavrilov, A.V. Shaldaev. Algorithms for the formation of radar images of the earth's surface using GLONASS signals. *Izv. universities. Instrumentation*. Vol. 55, No. 9, 2012, pp. 24-29.
5. A.V. Chernodarov, A.P. Patrikeev, V.N. Kovregin, G.M. Kovregina. Using an inertial satellite navigation system to determine the motion parameters of the phase center of the radar antenna. *XXIII St. Petersburg International Conference on Integrated Navigation Systems*. St. Petersburg: OJSC "Concern" Central Research Institute "Elektropribor", 2016, pp. 266-274.
6. Yu.V. Markov, A.S. Bokov, V.G. Vazhenin, V.V. Mukhin, M.Yu. Nesterov, A.A. Iofin. Modeling of reflected radar signals for a multi-channel earth remote sensing system. *Reliability and quality of complex systems*. 2020. No. 1 (29), pp. 24-34. DOI 10.21685/2307-4205-2020-1-3.
7. N.N. Golovanov. Geometric modeling. M.: Publishing House of Physical and Mathematical Literature, 2002. 472 p.
8. A.A. Sosnovsky, I.A. Khaimovich, E.A. Lutin, I.B. Maksimov. Aviation radio navigation: a reference book; ed. A.A. Sosnovsky. Moscow: Transport, 1990. 264 p.
9. D.A. Zherdev, E.Yu. Minaev, V.A. Fursov. Modeling of radar images using a software-simulating constructor of radar maps. *Information technologies and nanotechnologies*. 2016, pp. 586-590.
10. Integrated geoinformation-photogrammetric modeling of relief: a tutorial. Moscow: Publishing house MIIGAiK. 2019. 175 p.
11. S.V. Borisov, Yu.K. Vyboldin. Investigation of the accuracy of measuring the radial dimensions of subsurface objects in georadar. *Innovations and prospects for the development of mining engineering and electromechanics: IPDME-2021*. St. Petersburg, 2021, pp. 327-328.

INFORMATION ABOUT AUTHORS:

- A.R. Bestugin**, Dr. Sc. (Tech.), Professor, Director of the Institute of " Radio engineering, electronics and communications ", SUAI, St. Petersburg, Russia, freshguap@mail.ru
- I.A. Kirshin**, Ph.D.(Econ), Associate Professor, Department of Design and Technologies of Electronic and Laser Devices, SUAI, St. Petersburg, Russia, ikirshina@mail.ru
- V.N. Kovregin**, Ph.D.(Tech), Associate Professor, Department of Aerospace Measuring and Computing Complexes, SUAI, St. Petersburg, Russia, kovregin@mail.ru
- E.A. Antochin**, Ph.D.(Tech), Associate Professor, Department of of Radio Engineering Systems, SUAI, St. Petersburg, Russia, fresguap@mail.ru.
- O.I. Sauta**, Dr. Sc. (Tech.), Department of Design and Technologies of Electronic and Laser Devices, SUAI, St. Petersburg, Russia, sauta-oleg@yandex.ru

For citation: Bestugin A.R., Kirshina I.A., Kovregin V.N., Antochin E.A., Sauta O.I. A method for proactive compensation of interfering reflections during radar observation of small-sized objects against the background of the underlying surface. *H&ES Reserch*. 2023. Vol. 15. No. 2. P. 4-9. doi: 10.36724/2409-5419-2023-15-2-4-9 (In Rus)

МЕТОД ПЕРЕДАЧИ АВАРИЙНЫХ СИГНАЛОВ НА РАСПРЕДЕЛЕННОЙ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ РОСМОРРЕЧФЛОТА

БУДКО

Никита Павлович¹

АЛЛАКИН

Владимир Васильевич²

КАРЕТНИКОВ

Владимир Владимирович³

Сведения об авторах:

¹ аспирант, ФГБОУ ВО "Государственный университет морского и речного флота имени адмирала С.О. Макарова".
г. Санкт-Петербург, Россия,
budko62@mail.ru

² ФГБОУ ВО "Государственный университет морского и речного флота имени адмирала С.О. Макарова".
г. Санкт-Петербург, Россия,
vladimir@duduh.ru

³ заведующий кафедрой судоходства на внутренних водных путях ФГБОУ ВО "Государственный университет морского и речного флота имени адмирала С.О. Макарова", доктор технических наук,
г. Санкт-Петербург, Россия, доцент,
kaf_svp@gumrf.ru

АННОТАЦИЯ

Актуальность: Представлен метод передачи аварийных сигналов на распределенной информационно-телекоммуникационной сети общего пользования, позволяющий осуществлять помехоустойчивое доведение измерительной информации о состоянии элементов географически распределённой телекоммуникационной структуры ведомства с использованием декаметровых радиолиний на базе применения линейно-частотно-модулированных, а также дискретных линейно-частотно-модулированных сигналов, что позволяет улучшить помехоустойчивость подсистемы удаленного мониторинга состояния географически распределенной информационно-телекоммуникационной сети. **Цель работы:** повышение помехоустойчивости сигналов аварии на телеметрической системе распределенной сетевой инфраструктуры, функционирующей в условиях сложной помеховой обстановки и иных дестабилизирующих факторов. **Используемые методы:** формирование перспективной сигнально-кодовой конструкции в каналах радиосвязи телеметрической системы; использование в интересах передачи измерительной информации режима изменения рабочей частоты по псевдослучайному закону. **Новизна:** повышение возможностей подсистемы удаленного мониторинга за счет расширения степеней свободы оператора телеметрической системы – слуховой, визуальный и автоматический прием аварийных сигналов. **Полученный результат** заключается в графическом отображении принятых бинарных посылок сигналов аварии на спектрограмме типа "водопад", при этом вместо "точек" и "тире" кода Морзе отображаются линейно-частотно-модулированные либо дискретно-линейно-частотно-модулированные сигналы с убывающим, либо возрастающим градиентом наклона.

КЛЮЧЕВЫЕ СЛОВА: информационно-телекоммуникационная сеть, измерительная информация, помехоустойчивость, спектрограмма, телеметрическая система

Для цитирования: Будко Н. П., Аллакин В. В., Каретников В. В. Метод передачи аварийных сигналов на распределенной информационно-телекоммуникационной сети Росморречфлота // Научные исследования в космических исследованиях Земли. 2023. Т. 15. № 2. С. 10-17. doi: 10.36724/2409-5419-2023-15-2-10-17



Введение

Многоуровневую модель подсистемы удаленного мониторинга состояния географически распределенной информационно-телекоммуникационной сети (ИТКС) общего пользования возможно представить диспетчерским, телекоммуникационным и сенсорным уровнями. При этом именно телекоммуникационный уровень является наиболее сложным с позиции обеспечения устойчивого функционирования ИТКС в связи с такими её ярко выраженными характерными особенностями применения в Росморречфлоте как: глобальные расстояния и вытекающие из этого задержки на сети; разнородность (гетерогенность) как среды передачи измерительной информации (ИИ), так и каналов связи; открытость системы с точки зрения воздействия дестабилизирующих факторов и значительной нестационарности радиоканалов, вызываемой дрейфом основных параметров среды распространения радиоволн.

Перечисленные особенности относят такие каналы радиосвязи к категории каналов с высоким коэффициентом ошибок. Поэтому в работе особое внимание уделено методам передачи измерительной информации от сенсорного уровня (объектов контроля к диспетчерскому уровню (ситуационным центрам ведомства) по каналам радиосвязи, как наиболее вероятным для использования на ИТКС Росморречфлота и наиболее сложным в их математическом описании.

Рост числа источников ИИ на современных распределенных гетерогенных ИТКС, влечет за собой увеличение специфичности и сложности задач, решаемых при удаленном мониторинге их технического состояния, что повышает требования к современным телеметрическим системам (ТМС) до уровня требований к системам телекоммуникаций [1]. В то же время, применение таких ТМС и систем мониторинга на распределенных ИТКС Росморречфлота характеризуется низкой помехоустойчивостью при доведении аварийных сигналов на ситуационный центр от объектов контроля, функционирующих при наличии естественных и искусственных дестабилизирующих факторов, существенно понижая общую эффективность функционирования ИТКС ведомства.

Существующими на сегодня алгоритмами не всегда удается осуществить сбор и трансляцию ИИ в условиях влияния шумов, случайных и преднамеренных помех с достоверностью не хуже заданной [2], что влияет в целом на снижение эффективности сетевой инфраструктуры. При этом усложнение корабельных и береговых комплексов связи, а также других средств навигационного оборудования как объектов мониторинга приводит к тому, что в вопросе обеспечения требований по устойчивости ИТКС искажение ИИ или даже кратковременные перерывы в ее поступлении крайне нежелательны [1, 2]. Все это делает разработку новых и перспективных методов удаленного мониторинга, повышающих помехоустойчивость телеметрической системы, актуальным и востребованным.

Цель статьи – повышение помехоустойчивости аварийных сигналов в подсистеме удаленного мониторинга на ИТКС, функционирующей в условиях воздействия дестабилизирующих факторов различной физической природы.

Анализ предметной области исследования

К одному из активно используемых в настоящее время методов передачи телеметрической информации с глобально удаленных технических систем морского, наземного и воздушного базирования на диспетчерские пункты управления можно отнести применяемый с начала XX века способ радиосообщения построенные на сигнально кодовой конструкции (СКК) кода Морзе [3], в котором бинарная посылка передается путем трансляции длинных («тире») и коротких («точек») сигналов, причем при кодировке символов алфавита базовой единицей времени считается длина одной «точки». При этом длина одного «тире» равна длительности трёх «точек», внутри буквы межзнаковая пауза равнозначна длине одной «точки», пауза между буквами соответствует длине «тире» (т. е. три «точки»), а между словами внутри сообщения – семь «точек». Изначально при передаче сигналов кода Морзе используется режим амплитудной телеграфии (АТ) на фиксированной частоте, а прием осуществляется радиотелеграфистом на слух (на головные телефоны). Применение данного метода столь длительно и безальтернативно более 100 лет связано с уникальными возможностями слуха человека, по сравнению с автоматической идентификацией сигналов кода Морзе в условиях шумов и помех. При этом в качестве недостатков способа отмечается низкая скорость передачи и слабая помехозащищенность в связи с высокой подверженностью радиоканала сосредоточенным помехам и замираниями сигнала в среде распространения радиоволн.

Существенно повысить помехоустойчивость радиосообщения на ТМС возможно путём применения линейно-частотно-модулированных (ЛЧМ¹) сигналов, когда на передающей стороне формируется сигнально-кодовая конструкция, соответствующая битовому информационному нулю «0» – по линейно возрастающему, а битовому информационному единице «1» – по линейно убывающему закону изменения несущей частоты [4, 5]. При этом на приёмной стороне как правило могут применяться корреляционный метод или согласованная фильтрация. К недостаткам данного подхода также относят низкую помехозащищенность при автоматическом приеме сигналов и их идентификации в условиях шумов и помех.

Также известен способ радиосообщения [6], при котором в процессе передачи значения несущей частоты сначала модулируют информационной последовательностью с применением известных узкополосных методов, а затем изменяют рабочую частоту расширяющей кодовой последовательностью по псевдослучайному закону (так называемый режим ППРЧ с расширением спектра скачками частоты) и излучают в эфир.

¹ **Линейная частотная модуляция (ЛЧМ)** сигнала – это вид частотной модуляции, при которой частота несущего сигнала изменяется по линейному закону

На приёмной стороне частота первого гетеродина меняется по правилам расширяющей кодовой последовательности, принятым в формирователе сигнала передающей стороны, а далее для селективной фильтрации сигнал после гетеродинирования переносят на фиксированную промежуточную частоту. Недостатком изложенного способа являются сложности в реализации приемного устройства, сопряженные с обеспечением быстрой перестройки фильтров, что влияет на снижение качества фильтрации.

Говоря о достижении поставленной цели, направленной на повышение помехоустойчивости ТМС, наиболее близким решением является способ из области авиационной техники, предназначенный для помехоустойчивого функционирования средств посадки и радионавигации. В условиях шумов и помех повышение помехоустойчивости в нём достигается расширением спектра сигнала при передаче в режиме ППРЧ, и восстановлением бинарных посылок путем обратного преобразования принятого сигнала в исходную форму на приемной стороне [7]. При этом используется режим т. н. «внутрибитовой» ППРЧ, когда длина бинарной посылки соответствует отношению длины информационного бита к числу скачков рабочей частоты внутри него, меняющихся по принятому на передающей стороне псевдослучайному закону.

На приёмной стороне информационный бит восстанавливается через преобразование в начальную частотную форму принятого сигнала путём перемножения сформированного сигнала гетеродина с применением частотной матрицы ППРЧ. Данная процедура исключает ручной режим приёма и реализуется исключительно в автоматическом режиме. В сложной помеховой обстановке наращивание помехоустойчивости для радиоканалов с высоким коэффициентом ошибок (например, декаметровых) в этом случае зачастую обеспечивают увеличением мощности радиопередающего устройства. Недостатком способа является то, что использование в реальном масштабе времени метода анализа панорамных спектрограмм визуально не позволяет оператору демодулировать и декодировать транслируемые в режиме ППРЧ группы коротких (менее 0,1 с) импульсов. При этом важно наличие высокоточной синхронизации.

Анализ научно-методического аппарата формирования радиолиний ТМС и выявленные недостатки рассмотренных методов показал востребованность исследований по поиску и формированию новых подходов, позволяющих осуществлять помехоустойчивый приём измерительной информации на телекоммуникационном уровне подсистем мониторинга распределенных ИТКС.

Разработка метода передачи аварийных сигналов на распределенной ИТКС

Исходя из проведенного анализа научно-методического аппарата и применимости современных интеллектуальных технологий в интересах удаленного мониторинга распределенных ИТКС и повышения их помехоустойчивости разработан метод, основанный на использовании перспективных СКК для передачи аварийных сигналов от сенсорного к диспетчерскому уровням ТМС. Предложено использовать графическое изображение

аварийных сигналов на диспетчерский пункт управления или ситуационный центр ведомства в виде спектрограмм, соответствующих визуализации передачи/приему информационной «1» и информационного «0», соответствующих ЛЧМ-сигналам, а также дискретно меняющимся по ЛЧМ закону (ДЛЧМ) сигналам с повышающим, либо понижающим градиентом² модуляции. На рисунке 1 показаны блок-схемы вариантов построения алгоритмов выполнения метода.

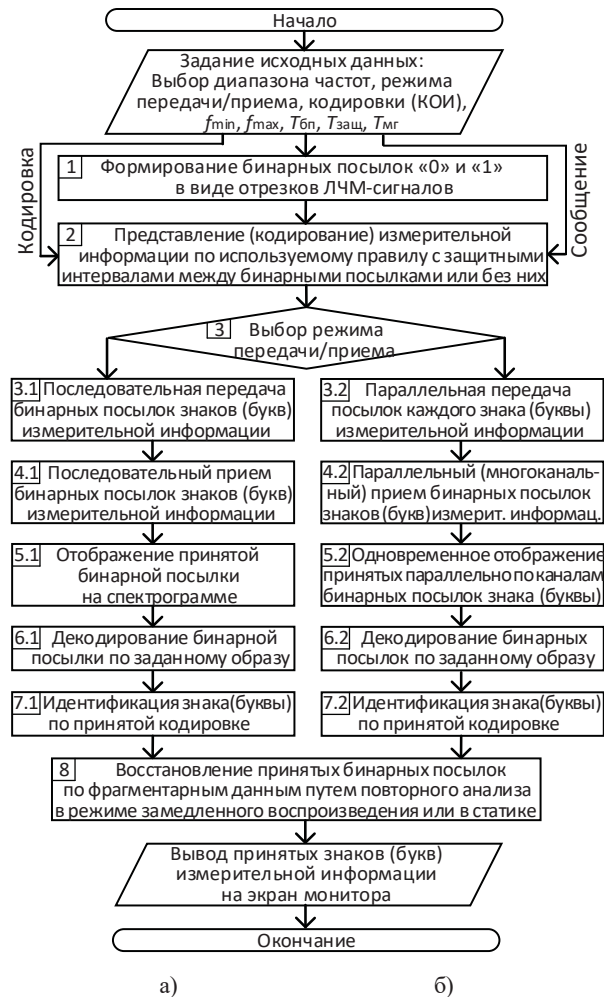


Рис. 1. Алгоритмы передачи аварийных сигналов состояния элементов ИТКС: а) на основе применения ЛЧМ сигналов; б) с использованием сигналов ДЛЧМ в режиме «быстрой» ППРЧ

Представленные алгоритмы состоят из последовательности действий, реализующих процесс доведения ИИ от сенсорного уровня подсистемы контроля и мониторинга ИТКС до диспетчерского пункта, а также процессы последующей её обработки и идентификации принятого аварийного сигнала. Предложенные алгоритмы предусматривают осуществление обмена хранящейся в различных базах данных и базах состояний распределенной ИТКС информацией для их репликации.

² На спектрограмме в частотно-временной области помеха отображена вертикальной линией и любые одночастотные сигналы типа азбуки Морзе (унаследованная сигнально-кодовая конструкция) при совпадении с нею неразличимы (градиент отличия равен нулю).

Первый алгоритм (рис. 1, а) заключается в том, что на низовом уровне ТМС от сенсоров поступают пакеты ИИИ, представленные бинарными посылками в виде отрезков ЛЧМ-сигналов с линейно-убывающими или линейно-возрастающими градиентами наклона, соответствующие передаче информационного нуля «0» или информационной единице «1», рис. 2 а) и б).

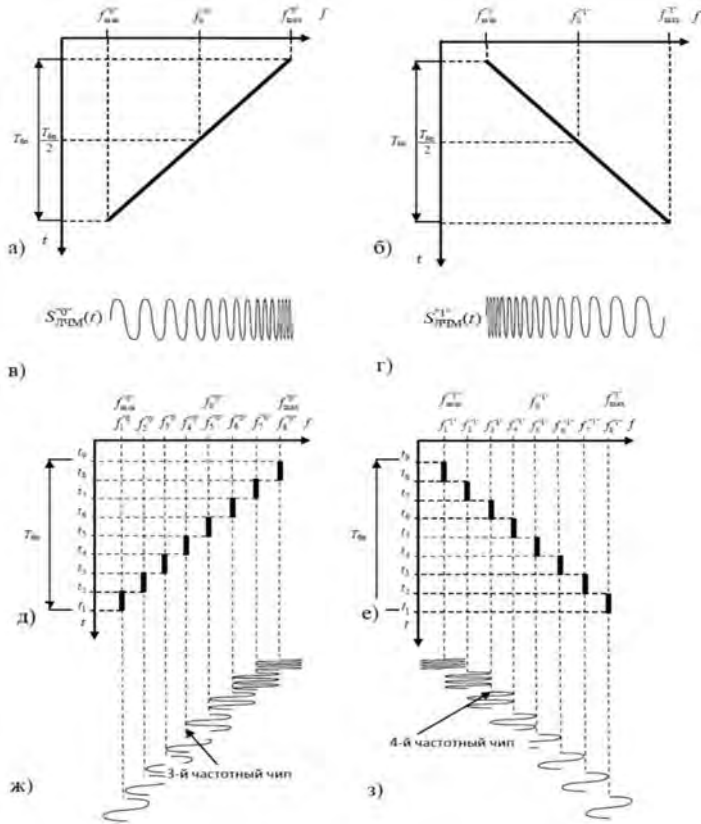


Рис. 2. Внешний вид ЛЧМ- и ДЛЧМ-сигналов: а) частотно-временная характеристика (ЧВХ) сигнально-кодовой конструкции, построенной по закону линейно возрастающего изменения рабочей частоты (в); б) ЧВХ СКК, построенному по закону линейно убывающего изменения рабочей частоты (г); д) ЧВХ СКК, построенной на основе многочастотного ДЛЧМ-сигнала с законом линейно возрастающего изменения рабочей частоты (ж); е) ЧВХ многочастотного ДЛЧМ-сигнала с законом линейно убывающего изменения рабочей частоты (з)

Их приём может осуществляться как в ручном режиме так и автоматически, с визуализацией на мониторе АРМ оператора диспетчерского пункта (автоматизированной системы управления движения судов, ситуационного центра) в виде спектрограммы типа «водопад», где сигнал отображают отрезками разных градиентов наклона, отличных от вертикальных прямых, представляющих сосредоточенные помехи в плоскости «время-частота» (рис. 3).

Математически процесс синтеза бинарных посылок, соответствующих информационному нулю или информационной единице («0» и «1») выглядит в виде аналитических выражений, представляющих ЛЧМ-сигнал с линейно возрастающим

$$S_{\text{ЛЧМ}}^{+1}(t) = S_0 \cos \{ \varphi_0 + \varphi(t) \} = S_0 \cos \{ \varphi_0 + 2\pi [f_0 t + (b/2)t^2] \} \quad (1)$$

и линейно убывающим законами изменения частот

$$S_{\text{ЛЧМ}}^{-1}(t) = S_0 \cos \{ \varphi_0 - \varphi(t) \} = S_0 \cos \{ \varphi_0 - 2\pi [f_0 t + (b/2)t^2] \} \quad (2)$$

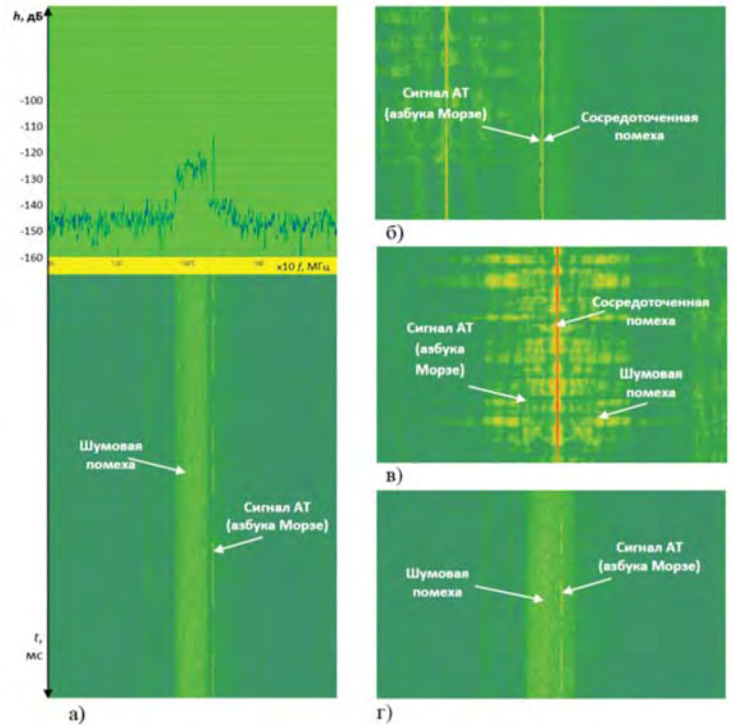


Рис. 3. Вариант визуализации спектрограмм и амплитудно-частотной характеристики сигналов АТ при воздействии: а) шумовой помехи рядом с сигналом; б) сосредоточенной по спектру помехи; в) мощных шумовой и сосредоточенной помехами; г) под шумовой помехой

В выражениях (1) и (2): S_0 – амплитуда сигнала, φ_0 – начальная фаза сигнала, $f_0 = (f_{\max} + f_{\min}) / 2$ – центральное значение несущей частоты, f_{\max} и f_{\min} – максимальное и минимальное значения частоты радиосигнала, $b = (f_{\max} - f_{\min}) / T_c$ – параметр скорости изменения частоты во времени, T_c – длительность сигнала (рис. 2 а, б).

На рисунке 2 а) и б) в плоскости «время-частота» описанные математически бинарные посылки отображены линейными отрезками с правым или левым градиентами наклона линейного изменения закона модуляции сигнала.

Во втором варианте реализации алгоритма предлагаемого метода применён режим т.н. «быстрой» ППРЧ (рис. 1, б и рис. 2, д-з). В работе [8] описан режим ППРЧ, используемый для повышения помехозащищённости декаметровых радиолиний. Эффективность такого подхода заключается в уменьшении влияния случайных и преднамеренных помех на функционирование радиолинии и минимизации вероятности группирования ошибок из-за наличия глубоких замираний сигналов в принятых сообщениях.

Там же показано, что применение многоканальных радиолиний с параллельным излучением бит сообщения узкополосными и сверхузкополосными сигналами с использованием режима ППРЧ позволяет повысить качества приема сообщений с сохранением скорости передачи.

При этом сначала формируется СКК в виде многочастотного дискретного сигнала, включающего n чипов, каждый из которых передаётся на частоте псевдослучайного кода, а при приёме сигнал восстанавливается путём преобразования в исходную частотную форму. Причем, трансляция каждого i -го частотного чипа ($i = 1, 2, \dots, n$) бинарных посылок информационных нулей и единиц («0», «1»), обозначающих несущие колебания частот f_i^{00} (f_i^{11}) дискретно изменяется с равномерным шагом до преобразования частот по псевдослучайному закону (ППРЧ)

$$\Delta f = f_i^{00(11)} - f_{i-1}^{00(11)} = f_{i+1}^{00(11)} - f_i^{00(11)}, \quad (3)$$

с дискретно понижающим или повышающим на заданных интервалах времени для нулевой бинарной посылки $T_{\text{БИ}}^{00}$ или единичной бинарной посылке $T_{\text{БИ}}^{11}$ изменением рабочих частот так, что несущие колебания частоты на временном интервале i -го частотного чипа t_i остаются неизменны: $f_i^{00} = \text{const}$, $f_i^{11} = \text{const}$.

На приёмной стороне производится преобразование сигнала по обратному псевдослучайному закону. На спектрограмме в плоскости «время-частота» принятый многочастотный ДЛЧМ-сигнал, включающий n частотных чипов, отображают в виде группы бинарной посылки с соответствующим градиентом наклона автоматически или визуальным оператором диспетчерского пункта (ситуационного центра). Далее принятый информационный бит ИИ декодируют в соответствии с заданным образом двоичного алфавита. Завершающим действием алгоритма является идентификация знака сообщения (бинарной последовательности) автоматически или визуальным.

Оценка эффективности предложенного метода

В предложенном методе передачи аварийных сигналов ТМС выигрыш в помехозащищенности осуществим путём введения последовательности действий (шагов), приведённых на рисунке 1 б) блок-схемы алгоритма путём автоматической или визуальной идентификации новой СКК ИИ в режиме внутрибитовой ППРЧ. Причем приращение помехозащищенности в данном случае происходит за счёт фактического преобразования радиоканала с прицельными преднамеренными помехами в радиоканал со случайными сосредоточенными помехами с последующим выделением бинарных посылок ИИ на фоне помех путём автоматической или визуальной идентификации. При этом процесс автоматической идентификации обеспечивается согласованной фильтрацией в радиоприёмном устройстве, а визуализация – за счёт способности зрительного анализатора человека доводить до нейронной сети головного мозга до 90 % информации об окружающем мире (спектрограмме) [9-11].

Испытания, проведенные с использованием *SDR*-радиоприёмного устройства, отображающем на мониторе спектрограмму сигнала в частотно-временной области, показали, что визуализация бинарных посылок новой СКК способствует их зрительной идентификации, даже в случае, когда в слуховом режиме из-за низкого отношения сигнал/шум (ОСШ) нет уверенного приёма (рис. 4).

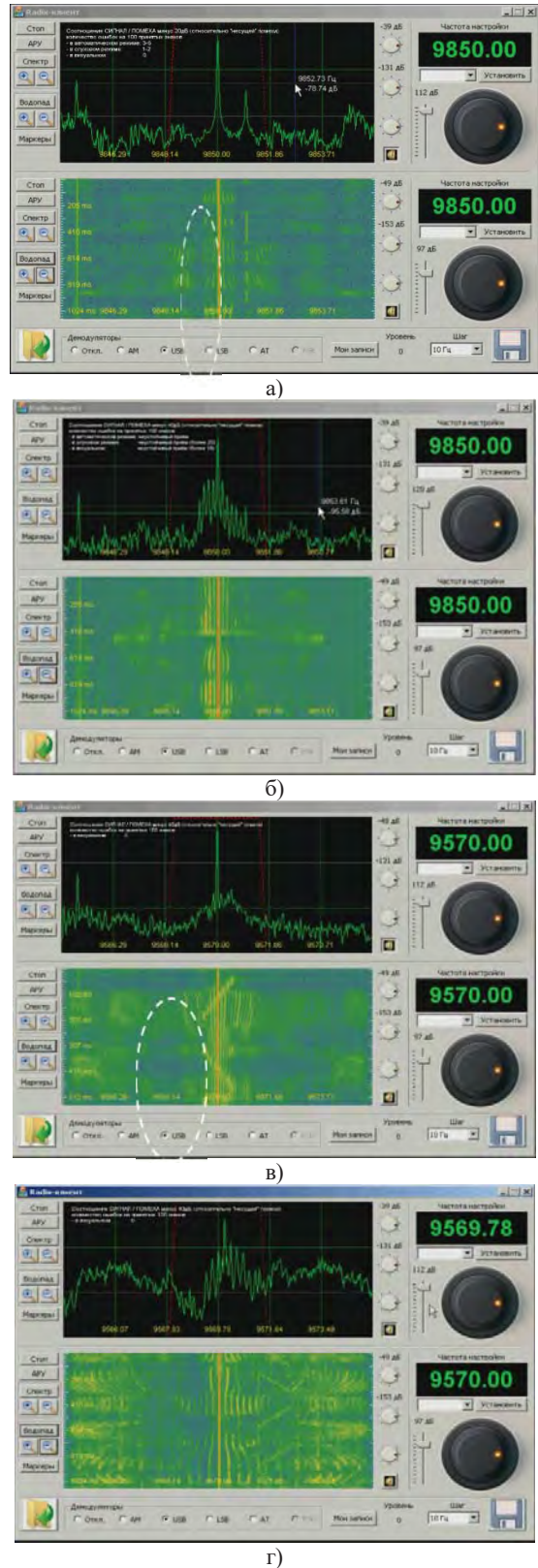


Рис. 4. Экранные формы отображения принятых сигналов на мониторе АРМ оператора: а) и б) – для унаследованной СКК (Азбука Морзе); в) и г) – для предложенной СКК (ДЛЧМ); а) и в) ОСШ \approx минус 20 дБ; б) и г) ОСШ \approx минус 40 дБ

При соотношении сигнал/помеха (относительно уровня «несущей» помехи) для унаследованного сигнала Азбуки Морзе 0 Бд обеспечивается прием со следующими характеристиками: количество ошибок на 100 принятых знаков в автоматическом режиме – 0; в слуховом режиме – 0; в визуальном режиме – 0. При соотношении сигнал/помеха (относительно уровня «несущей» помехи) для унаследованной СКК минус 20 Бд обеспечивается прием со следующими характеристиками: количество ошибок на 100 принятых знаков в автоматическом режиме – 3-5; в слуховом режиме – 1-2; в визуальном режиме – 0, что хорошо просматривается на варианте экранной формы рис. 4 а).

При соотношении сигнал/помеха (относительно уровня «несущей» помехи) для унаследованной СКК минус 40 Бд обеспечивается прием со следующими характеристиками: количество ошибок на 100 принятых знаков в автоматическом режиме – неустойчивый прием; в слуховом режиме – неустойчивый прием (более 20 ошибок); в визуальном режиме – неустойчивый прием (более 10 ошибок), что представлено на варианте экранной формы рис. 4 б).

При использовании предложенной СКК (передача «точки» – левый градиент наклона при визуализации на спектрограмме, передача «тире» – правый градиент наклона), в отличие от использования сигнала с унаследованной структурой даже при соотношении сигнал/помеха \approx минус 40 дБ обеспечивается устойчивый визуальный прием независимо от положения сигнала относительно частоты «несущей» помехи, что видно на вариантах экранных форм рис. 4 в) и г).

На рис. 5 показаны варианты идентификации аварийного сигнала по алгоритмам рис. 1, где бинарные посылки с правым и левым градиентами наклона достаточно хорошо наблюдаются в режиме реального времени не только на свободном от шумов и помех участке диапазона частот, (рис. 5 а), но и под сосредоточенной по спектру помехой (рис. 5 б). Как видно из рис. 5, если перенести сигнал с новой СКК в полосу частот, занятой мощной сосредоточенной помехой, то он также легко визуально идентифицируется по бинарным посылкам левого и правого градиента наклона даже при ОСШ $h_n = -40$ дБ, см. результаты эксперимента в таблице 1.

Таблица 1

Помехоустойчивость ТМС при соотношении уровня сигнал/помеха в канале декаметрового радиосвязи и число ошибок при приеме аварийного сообщения из 40 знаков

| Соотношение сигнал/помеха относительно «несущей» помехи, дБ | Режим автоматического приёма, всего ошибок | Режим слухового приёма, всего ошибок | Визуальный режим, всего ошибок |
|---|--|--------------------------------------|-------------------------------------|
| -20 | 3 – 5 | 1 – 2 | 0 |
| -40 | неустойчивый прием | неустойчивый прием, более 20 ошибок | неустойчивый прием, более 10 ошибок |

Для повышения оперативности передачи аварийных сигналов (что важно на низкоскоростных радиоканалах, например декаметрового диапазона), излучение бинарных посылок можно осуществлять в режиме параллельной многоканальной передачи/приема, реализуемой с использованием многоканальных возбуждательного и радиоприемного устройств.

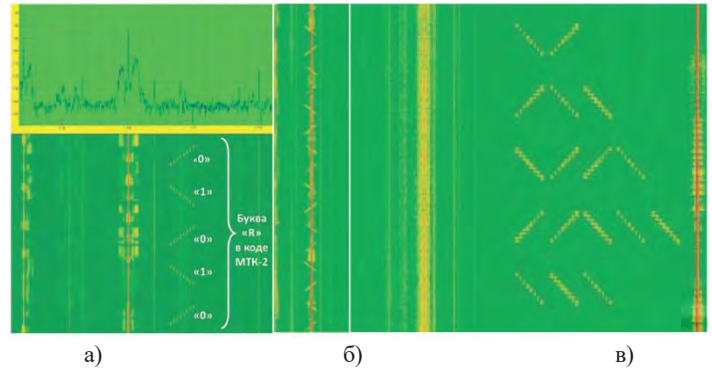


Рис. 5. Варианты реализации новой СКК в ходе визуализации на приемной стороне: при последовательной передаче бинарных посылок а), в том числе и под сосредоточенной помехой б), при реализации параллельной многоканальной передачи/приема знаков в целом в)

При этом за время излучения необходимого для последовательной передачи одной бинарной посылки можно передать знак (букву) в целом при использовании многоканальной передачи, что видно из правых ветвей блок-схем алгоритмов, показанных на рис. 1 а) (шаги 3.2 – 7.2) и на рис. 1 б) (шаги 3.2 – 8.2). Такой параллельный режим работы кратно (исходя из рис. 5 а) и в) – в пять раз) повышает оперативность доведения аварийных сигналов на радиолиниях телеуправления-телесигнализации ТМС критически важных элементов сетевых инфраструктур Росморречфлота, требующих немедленного вмешательства оператора АСУ движения судов в предотвращение аварии (катастрофы).

Современные комплексы средств автоматизации имеют возможность записи в карту памяти, а также репликации баз данных на АРМ операторов подсистемы мониторинга диспетчерских пунктов и ситуационных центров (автоматизированной системы управления движением судов) для документирования с последующим анализом и восстановлением ИИ. Поэтому предлагаемый метод может применяться для передачи любых бинарных последовательностей с различной скоростью передачи.

В таблице 2 приведена эффективность предлагаемого метода передачи аварийных сигналов на распределенной ИТКС с применением режима «быстрой» ППРЧ для варианта функционирования в сложной помеховой обстановки, путем оценки через вероятность безошибочного приема измерительной информации в слуховом режиме (радиотелеграфистом), при автоматическом и визуальном приеме.

Таблица 2

Оценка помехоустойчивости новой СКК, оптимизированной под визуальный прием аварийных сигналов (сообщения длиной 40 знаков) в сложной помеховой обстановке

| Вид помехи | Штатный код Морзе | | | СКК, оптимизированная для визуального приема | | Режим ППРЧ | |
|-----------------|-------------------|-----------------------------|----------------------|--|----------------------|------------------|----------------------|
| | Слуховой прием | Слуховой + визуальный прием | Автоматический прием | Визуальный прием | Автоматический прием | Визуальный прием | Автоматический прием |
| Сосредоточенная | 0,67 | 0,73 | 0,57 | 1,0 | 0,99 | 1,0 | 1,0 |
| Широкополосная | 0,83 | 0,92 | 0,71 | 0,98 | 0,68 | | |

Значимость предложенного метода для теории и практики эксплуатации телеметрических систем Росморречфлота

Значимость предложенного метода для теории и практики комплексом управления функционирования распределенных ИТКС Росморречфлота состоит:

- в росте помехоустойчивости ТМС распределённой ИТКС Росморречфлота за счет фактического преобразования радиоканала с прицельными преднамеренными помехами в радиоканал со случайными сосредоточенными помехами с последующим выделением бинарных посылок аварийных сигналов (измерительной информации) на фоне помех путём автоматической или визуальной идентификации;
- повышении различимости приема сигналов кода Морзе на слуховом фоне;
- простоте согласованной фильтрации автоматического приема ЛЧМ-сигнала;
- асширении степеней свободы радиотелеграфиста при реализации методов приема ИИ – слуховой, визуализированный или автоматизированный приём;
- обеспечение одинаковой помехоустойчивости для приема «ЛЧМ-тире» и «ЛЧМ-точек», т. е. равновероятный прием предложенной СКК на базе ЛЧМ-сигналов. В настоящее время в наследованном способе приёма кода Морзе для «точек» и «тире» помехоустойчивость различается за счёт того, что под мощной сосредоточенной помехой «точка» легко может быть трансформирована в «тире»;
- возможность применения метода на унаследованных средствах связи исходя из правила, что широкополосный сигнал не создаёт шумов узкополосному;
- легкость ведения параметрического контроля новой СКК по скажности следования бинарных посылок, снижению глубины модуляции градиента их наклона;
- повышение скорости передачи ИИ в ТМС за счет параллельной трансляции бинарных посылок в режиме ППРЧ и исключения защитных интервалов между ними в буквах (цифрах, знаках) и словах передаваемых сообщений в новой СКК;
- овышение скорости приёма аварийных сигналов и измерительной информации в ТМС за счет перехода от побитной (последовательной) идентификации ИИ оператором (радиотелеграфистом) к её восприятию (чтению) позначно (цифрами, буквами) в параллельном режиме передачи/приёме в радиолинии и визуализации спектрограмм на мониторе оператора диспетчерского пункта (ситуационного центра).

Заключение

Новизной предложенного метода передачи аварийных сигналов на распределенной ИТКС Росморречфлота является возможность передачи/приема аварийных сигналов и измерительной информации от удаленных средств связи и навигационного оборудования на диспетчерский пункт

автоматизированной системы управления движения судов бассейна рек внутренних водных путей России (в ситуационный центр ведомства), на основе представленных перспективных сигнально-кодовых конструкций, построенных на базе применения ЛЧМ (ДЛЧМ) сигналов с противоположными градиентами наклона $\pm 45^\circ$, отличающихся от вертикальных прямых с нулевым градиентом на спектрограммах принятой ИИ в плоскости «время-частота».

Причём бинарные посылки, представляющие информационный нуль и информационную единицу ИИ, на передающей стороне представляется отрезками ЛЧМ- или ДЛЧМ-сигналов с изменением частоты по линейно убывающему или линейно возрастающему закону, а приемной стороне идентифицируемые визуально или автоматически с использованием банка фильтров.

Помехоустойчивость предложенного в статье метода также будет зависеть от состояния среды распространения радиоволн, выбранного диапазона частот, числа частотных чипов, применяемых при её формировании, а также их длительности, влияющей на длительность бинарной посылки в целом.

Литература

1. *Винограденко А.М.* Методология интеллектуального контроля технического состояния автоматизированной системы связи специального назначения. Монография. СПб.: Научное издание, 2020. 180 с.
2. *Zelensky E.G., Kononov Yu.G., Fedorenko V.V., Vinogradenko A.M., Samoylenko V.V.* Development of a distributed multi-agent system monitoring and control networks of 0.4–35 kV // Proceedings of 2017 IEEE 2nd International Conference on Control in Technical Systems, (CTS 2017). 2017. Vol. 2. P. 271-274. doi: 10.1109/CTS2017.8109543.
3. *История отечественных средств связи / Под ред. А.С. Якунина.* М.: Издательский дом «Столичная энциклопедия», 2013. 576 с.
4. *Гоноровский И.С.* Радиотехнические цепи и сигналы. М.: Радио и связь, 1986. 513 с.
5. *Марычев Д.С., Морозов О.А., Хмелев С.Л.* Оценка параметров ЛЧМ сигналов методом цифровой адаптивной фильтрации // Радиотехника (Электронный журнал). 2012. № 3. С. 1-8.
6. *Макаренко С.И., Иванов М.С., Попов С.А.* Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты. Монография. Пб.: Свое издательство, 2013. 166 с.
7. *Беккиев А.Ю., Борисов В.И.* Базовые принципы создания помехозащищенных систем радиосвязи // Теория и техника радиосвязи. 2014. № 1. С. 3-16.
8. *Жуков Г.А., Будко П.А.* Широкополосные и узкополосные сигналы в радиолиниях декаметрового диапазона волн // Морская радиоэлектроника. 2020. № 2 (72). С. 32-37.
9. *Евин И.А.* Синергетика мозга. М.: Регулярная и хаотическая динамика, 2005. 108 с.
10. *Айзман Р.И., Герасёв А.Д., Дюкарев И.А.* Молекулярные основы физиологии человека: Компендиум. Новосибирск: НГПУ, 2010. 306 с.
11. *Кордуэлл М.* Психология. А-Я. Словарь-справочник. М.: ФайрПресс, 2000. 448 с.



METHOD OF TRANSMISSION OF EMERGENCY SIGNALS ON THE DISTRIBUTED INFORMATION AND TELECOMMUNICATION NETWORK OF ROSMORRECHFLOT

NIKITA P. BUDKO

St. Petersburg, Russia, budko62@mail.ru

VLADIMIR V. ALLAKIN

St. Petersburg, Russia, vladimir@duduh.ru

VLADIMIR V. KARETNIKOV

St. Petersburg, Russia, kaf_svp@gumrf.ru

ABSTRACT

Relevance: A method of transmitting alarm signals on a distributed public information and telecommunications network is presented, which allows for noise-resistant transmission of measuring information about the state of elements of a geographically distributed telecommunications structure of the department using decimeter radio lines based on the use of linear-frequency-modulated, as well as discrete linear-frequency-modulated signals, this makes it possible to improve the noise immunity of the subsystem for remote monitoring of the state of a geographically distributed information and telecommunications network. **The purpose of the work** is to increase the noise immunity of accident signals on a telemetry system of a distributed network infrastructure operating in a complex

KEYWORDS: *information and telecommunication network, measuring information, noise immunity, spectrogram, telemetry system.*

interference situation and other destabilizing factors. **Methods used:** formation of a promising signal-code structure in radio channels of a telemetry system; the use of the mode of changing the operating frequency according to a pseudo-random law in the interests of transmitting measuring information. **Novelty:** increasing the capabilities of the remote monitoring subsystem by expanding the degrees of freedom of the operator of the telemetry system - auditory, visual and automatic reception of alarms. **The result** obtained is a graphical representation of the received binary parcels of the accident signals on a waterfall-type spectrogram, while instead of "dots" and "dashes" of the Morse code, linear-frequency-modulated or discrete-linear-frequency-modulated signals with a decreasing or increasing slope gradient are displayed.

REFERENCES

1. Vinogradenko A.M. Methodology for intelligent control of the technical condition of an automated communication system for special purposes. Monograph. St. Petersburg. *Naukoyemkiye tekhnologii*, 2020. 180 p.
2. Zelensky E.G., Kononov Yu.G., Fedorenko V.V., Vinogradenko A.M., Samoylenko V.V. Development of a distributed multi-agent system monitoring and control networks of 0.4-35 kV. *Proceedings of 2017 IEEE 2nd International Conference on Control in Technical Systems, (CTS 2017)*, St. Petersburg, 2017, vol. 2, pp. 271-274. doi: 10.1109/CTSIS.2017.8109543. (in Russian)
3. Yakunin A.S. History of domestic means of communication. Moscow, Capital encyclopedia Publ., 2013. 576 p. (in Russian)
4. Gonorovsky I.S. Radio circuits and signals. Moscow, RIS, 1986. 513 p. (in Russian)
5. Marychev D.S., Morozov O.A., Khmelev S.L. Estimation of chirp signal parameters by digital adaptive filtering. *Radiotekhnika* (Electronic journal). 2012. No. 3, pp. 1-8.
6. Makarenko S.I., Ivanov M.S., Popov S.A. Noise immunity of communication systems with pseudo-random tuning of the operating frequency. Monograph. St. Petersburg: Svoye izdatel'stvo, 2013. 166 p.
7. Bekkiev A.Yu., Borisov V.I. Basic Principles of Creation of Noise-Proof Radio Communication Systems. *Theory and technique of radio communication*, 2014, no. 1, pp. 3-16. (in Russian)
8. Zhukov G.A., Budko P.A. Broadband and narrowband signals in decimeter radio lines. *Marine radioelectronics*. 2020. No. 2 (72), pp. 32-37.
9. Evin I.A. Brain synergetics. Moscow, Regular and chaotic dynamics, 2005, 108 p. (in Russian)
10. Ayzman R.I., Gerasyov A.D., Dyukarev I.A. Molecular foundations of human physiology. Novosibirsk, NGPU, 2010, 306 p. (in Russian)
11. Korduel M. Psihologiya. A-Ya. Psychology. A-Z. Dictionary reference. Moscow, Fair-Press, 2000, 448 p. (in Russian)

INFORMATION ABOUT AUTHORS:

Nikita P. Budko, postgraduate student, Federal State Budgetary Educational Institution of Higher Education "Admiral S. O. Makarov State University of the Sea and River Fleet", St. Petersburg, Russia, budko62@mail.ru

Vladimir V. Allakin, postgraduate student, Federal State Budgetary Educational Institution of Higher Education "Admiral S. O. Makarov State University of the Sea and River Fleet", St. Petersburg, Russia, vladimir@duduh.ru

Vladimir V. Karetnikov, Head of the Department of Navigation on Inland Waterways of the Admiral S.O. Makarov State University of Marine and River Fleet, Doctor of Technical Sciences, Associate Professor, St. Petersburg, Russia, kaf_svp@gumrf.ru

For citation: Budko N. P., Allakin V. V., Karetnikov V. V. Method of transmission of emergency signals on the distributed information and telecommunication network of Rosmorrechflot. H&ES Reserch. 2023. Vol. 15. No. 2. P. 10-20. doi: 10.36724/2409-5419-2023-15-2-10-17 (In Rus)

ВОЗДЕЙСТВИЕ ВНЕШНИХ УСЛОВИЙ НА РАБОТОСПОСОБНОСТЬ РАДИОЭЛЕКТРОННЫХ СРЕДСТВ (РЭС)

СТОЛБИНСКИЙ
Денис Владимирович¹

БЕМ
Павел Петрович²

АНДРЕЕВ
Вадим Алексеевич³

МАТВЕЕВ
Дмитрий Викторович⁴

Сведения об авторах:

¹ аспирант, Самарский национальный исследовательский университет имени академика С.П. Королева, г. Самара, Россия, denver7074@yandex.ru

² аспирант, Самарский национальный исследовательский университет имени академика С.П. Королева, г. Самара, Россия, bem@testelektro.ru

³ аспирант, Самарский национальный исследовательский университет имени академика С.П. Королева, г. Самара, Россия, andreev.rus.vasilevka@yandex.ru

⁴ студент, Самарский национальный исследовательский университет имени академика С.П. Королева, г. Самара, Россия, matveev_d.v.1993@mail.ru

АННОТАЦИЯ

Введение. с момента возникновения первых радиопередатчиков, конструкторы задавались проблемами обеспечения их бесперебойной работы и безопасной эксплуатации. Однако, внешние условия продолжают формировать негативные факторы, которые влияют на работоспособность техники. В то же время, не возможно спрогнозировать все возможные ситуации, которые могут повлиять на работоспособность радиоэлектронных средств (РЭС). **Цель работы** рассмотреть ключевые внешние факторы, которые могут оказать негативное влияние на работоспособность радиоэлектронных средств. **Используемые методы:** синтез эмпирических данных, анализ практических исследований, компиляция данных научных исследований. Эти методы позволят раскрыть вопросы методологии с позиции отечественных и зарубежных исследователей, а так же определить ключевые факторы оказывающие влияние на работоспособность РЭС. **Новизна работы** заключается в систематизации взглядов отечественных и зарубежных исследователей по проблеме контроля деятельности РЭУ. Кроме того, выявлены не учтенные внешние факторы. **Результат:** в статье будут сделаны выводы о возможном предупреждении негативного влияния ключевых внешних факторах, влияющих на работоспособность радиоэлектронной техники. **Практическая значимость:** представленный анализ может быть использован, как основа для прикладных исследований, а так же как руководство, для предприятий, устанавливающих радиоэлектронные устройства.

КЛЮЧЕВЫЕ СЛОВА: радиоэлектронные устройства, внешние факторы, контроль и безопасность системы.

Для цитирования: Столбинский Д.В., Бем П.П., Андреев В.А., Матвеев Д.В. Воздействие внешних условий на работоспособность радиоэлектронных средств (РЭС) // Научные исследования в космических исследованиях Земли. 2023. Т. 15. № 2. С. 18-22. doi: 10.36724/2409-5419-2023-15-2-18-22

Введение

В то время как население мира постоянно растет, наш глобальный мир, кажется, становится меньше, поскольку мы можем общаться с людьми так, как никогда не могли себе представить. Радио и телевидение были одними из первых участников этой новой формы средств массовой информации и сыграли роль в воздействии на мировые политические взгляды и религиозные убеждения.

Хотя изобретение радио восходит к 1820-м годам, когда Ганс Кристиан Орстед обнаружил взаимосвязь между электричеством и магнетизмом, только между 1916 и 1920 годами транслировалась первая известная радионовостная программа. Со временем мир радио рос как по масштабам, так и по популярности, и многие радиопередачи стали поражать радиоволны. Радио стало важным связующим звеном с информацией и имело возможность влиять на мнение людей так, как никогда раньше [1].

По мере развития технологий возможность предоставления средств массовой информации изменила способ доставки информации и положила начало информатизации общества, а вместе с тем и распространению различных эмпирических исследований на тему оптимизации работы радиоэлектронных устройств.

Актуальность темы исследования обусловлена практическим интересом к вопросам оптимизации радиосистем, и как следствие обеспечения их бесперебойной работы, в независимости от влияния каких-либо внешних факторов. Данная проблема заботит как отечественных исследователей, так и предпринимателей, а также обывателей, так как радиосистемы – это неотъемлемая часть жизни современного общества.

Цель работы – рассмотреть ключевые виды внешних факторов влияющих на работу радиоэлектронных систем.

Новизна работы заключается в систематизации взглядов отечественных и зарубежных исследователей по проблеме контроля деятельности РЭУ. Кроме того, выявлены не учтенные внешние факторы.

Используемые методы: синтез эмпирических данных (в рамках исследования были проанализированы работы отечественных и зарубежных авторов и обобщен опыт данных работ), анализ практических исследований (проведена выборка ключевых внешних факторов, на которые указывают как отечественные, так и зарубежные авторы), компиляция данных научных исследований (сделаны выводы и приведены результаты анализа собранной информации в форме общих характеристик и умозаключений).

Отечественные и зарубежные исследователи о внешних факторах, оказывающих влияние на работу радиоэлектронных устройств

Вопрос работоспособности радиоэлектронных устройств волновал производителей с момента возникновения первых образцов оборудования. С тех пор шел процесс оптимизации работы и совершенствования технологий. Одновременно с этим прослеживались и попытки классификации ключевых внешних факторов, оказывающих влияние на работу радиоэлектронного оборудования.

Зарубежные исследователи, Вербеке В., Дитц Б. и Вервал Э. отмечают, что для выявления наиболее значимых факторов, оказывающих влияние на работу РЭС, необходимо проведение всеобъемлющего обзора всего спектра факторов, влияющих на эффективность и работоспособность радиоэлектронного оборудования. И все же они выделяют две крупные группы факторов, с разветвленной системой подпунктов. Первая группа – это антропогенные факторы, связанные с работой человека и его использованием радиоэлектронных систем. Вторая группа – природные факторы, которые, как отмечают авторы, крайне сложно предупредить, а следовательно, и обезопасить работу РЭС [2].

Однако, отечественные авторы не согласны с позиции зарубежных исследователей, считая, что как раз антропогенные факторы можно считать более непредсказуемыми, в то время как природные явления в полной мере закономерны и цикличны, а следовательно, радиоэлектронное оборудование необходимо подбирать таким образом, чтобы оно подходило для тех условий, в которые будет помещено [3].

Лященко В.В. отмечает, что для создания физической модели защиты кабельных линий и радиоэлектронных средств государственных и промышленных объектов от внешнего электромагнитного воздействия, эмпирическим путем подтверждена необходимость обеспечения полной нейтрализации энергии электромагнитного воздействия, как основного фактора поддержания надлежащего технического состояния кабельных линий и радиоэлектронных средств.

Функциональная аналогия между электричеством и пневматикой (гидравликой), которые являются основой для развития защиты кабельных линий и РЭС в направлении замены наиболее уязвимых элементов говорит о том, что вычислить воздействие возможно при помощи электронных измерительных систем, а также цифровых и аналоговых потоковых вычислителей. Для создания защиты каналов связи используются пневматические устройства (гидроавтоматы) и волоконно-оптические материалы. Исследователь утверждает, что такая система позволит обеспечить безопасность работы РЭС, даже в случаях ЧП [4. с.119-126].

Безусловно, в работах отечественных исследователей встречаются исследования разнообразных внешних факторов, которые оказывают влияние на работоспособность радиоэлектронных систем. Так, Юрков Н.К. провел обзор отечественной литературы на данную тему и выявил ключевые факторы, которые исследуют конструкторы-технологи, изучают практики и теоретики радиоэлектроники. К таким факторам можно отнести следующие: воздействие вибрации, воздушных потоков, шумов, ударов, электромагнитного поля и радиации [5. с.5-13].

В зарубежной литературе делается упор на внешние – природные факторы, такие как погода, солнце, сейсмическая активность. Отечественные исследования дополняют экспериментальную базу зарубежных коллег, но не могут отрицать влияния и указанных выше факторов.

Виды внешнего воздействия на работу радиоэлектронного оборудования: воздействие вибрации, удары, линейные ускорения, акустические шумы, электромагнитные поля, радиация

Рассматривая вопрос механических воздействий, можно сказать, что к ним принято относить: удары, давление, оказываемое ускорением, атмосферой или же вибрацией и шумом. Это существенно снижает работоспособность и надежность радиоэлектронных устройств, что может привести к сбою в работе всей системы. Для повышения надежности, снижения стоимости РЭС, а также для уменьшения или устранения влияния климатических, биологических, температурных и других дестабилизирующих факторов применяют герметизацию этих устройств различными способами, например, с помощью тонкопленочной технологии для инкапсуляции устройств [6. С.20-27].

Внешние вибрации воздействуют на уплотняющую крышку устройства и вызывают механические нагрузки в элементах конструкции. При этом силы, действующие на элементы конструкции, будут наибольшими и могут быть даже разрушительными. Типы вибрации могут отличаться и варьироваться сила колебаний, однако, наносимый урон работоспособности радиоэлектронного оборудования, прослеживается всегда [7. С.10-18].

Удар, его интенсивность, амплитуда, форма и длительность ударного импульса так же несут в себе разрушения и деформации оказывающие непосредственное влияние на работоспособность РЭС. После удара возникают вибрации, которые могут войти в резонанс с собственными колебаниями элементов конструкции, такое положение только ускорит сбой работы. Потому необходим защитный жесткий каркас и использование амортизаторов, ограничивающих движение. Так же перспективно применение противоударной защиты на основе нелинейных пружинных амортизаторов и амортизаторов с мягким покрытием [8. С.69-80].

Давление, как линейные ускорения будут влиять на работу и конструкцию РЭС всех типов. Потому конструкторы и производители давно отдали предпочтение поискам прочным материалам с высокой плотностью и наличием упругих элементов в конструкции радиоэлектронных устройств, так как других способов противостоять данным воздействиям пока не найдено [9. с.16-19].

Следующим механическим воздействием, которое оказывает влияние на работоспособность РЭС, можно назвать шум, который включает в себя как неизбежный шум, присущий любой электронной системе, так и внешний шум, который можно уменьшить с помощью экранирования и других средств. Ухудшение работы радиоэлектронного устройства проявляется в снижении точности вывода информации, и в ухудшение или ограничение сигнала на выходе электронного устройства [10. С.81-89]. Можно сказать, что шум, в независимости от его типа, оказывает даже больше негативного влияние на детали радиоэлектронных устройств. Потому конструкторам остается только предлагать пользователям проводить периодическую проверку ключевых деталей устройства или их замену.

При электромагнитном воздействии (ЭМИ) достаточного уровня возможно временное нарушение функционирования, обработки, передачи информации в радиоэлектронном оборудовании. После прохождения через защитный корпус устройства, энергия электромагнитного поля может воздействовать на систему экранированных радиоэлектронных средств (РЭА), что приводит к негативным последствиям, таким как ухудшение работы и возможное нанесение вреда здоровью пользователей. Также возможны негативные последствия при определенных условиях от влияния скин-эффекта, воздействия электростатического разряда на оборудование и электромагнитных импульсов на радиоэлектронные устройства [11. с.81-89].

Конструктивный способ защиты РЭС от воздействия внешних электромагнитных факторов заключается в снижении собираемой и передаваемой энергии ЭМП за счет усовершенствования конструкции, размещения и монтажа оборудования. Компоненты некоторых вендоров для систем 5G, устойчивые к внешним помехам, позволяют использование структурных, схемных и структурно-функциональных методов обеспечения ЭМС. Новый стандарт 5G (пятое поколение) будет работать на более высоких рабочих частотах по сравнению с предыдущими поколениями [12. С.253-261].

Что касается радиации, то воздействие радиочастотного излучения также пагубно, но менее заметно. В данной области проводится множество исследований, однако данных недостаточно, чтобы давать четкие прогнозы и утверждать взаимосвязь тех или иных нарушений в работе именно с влиянием радиации. Потому, как отечественные, так и зарубежные исследователи проводят различные опыты и стремятся найти подтверждения тем или иным причинно-следственным связям нарушений в работе РЭС [13. С.69-80].

Следовательно, можно сказать, что есть два способа защититься от воздействия внешних факторов влияющих на работоспособность радиоэлектронных устройств – это внешняя защита или определенные методы предотвращения и контроля коллизий [14,15].

Заключение

Подводя итог, можно выделить следующее:

Как отечественные, так и зарубежные исследователи, изучая внешние факторы, влияющие на работоспособность радиоэлектронных устройств, делают обзоры современной литературы и подчеркивают, что прогресс исследований последнего десятилетия по предотвращению и минимизации различных нежелательных эффектов был очень велик.

В то же время, большое внимание уделяется механическим воздействиям, а также антропогенному фактору, который оказывает непосредственное влияние на работоспособность радиоэлектронных устройств. А работы, рассматривавшие вопросы климатического и геологического (магнитного) воздействия относятся к XX веку и могут считаться устаревшими, так как современные технологии позволяют углубиться в изучение данной темы.

Можно высказать предположение, что для исследователей, а также заинтересованных в развитии радио технологий

людей, будет интересно дальнейшее развитие темы природных факторов оказывающих влияние на работоспособность радиоэлектронных устройств.

Литература

1. Стефанишин Д., Кенделл Дж. Влияние радио и телевидения на культуру, грамотность и образование [Электронный ресурс]. Режим доступа: <https://blogs.ubc.ca/etec540sept12/2012/10/28/1687/> (дата обращения: 30. 12.2022).
2. Вербеке В., Дитц Б., Вервал Э. Драйверы эффективности работы радиосистем: современный метаанализ // <https://link.springer.com/article/10.1007/s11747-010-0211-8>
3. Парфенов В.И., Ле В.Д. Применение беспроводной сенсорной системы для защиты работоспособности радиоэлектронных систем // Компьютерная оптика. 2021. №45(3). С. 367-371.
4. Лященко В.В. Физическая модель защиты кабельных линий и радиоэлектронных средств государственных промышленных объектов от внешнего электромагнитного воздействия в условиях предупреждения чрезвычайных ситуаций // Социальное развитие и безопасность. 2019. №9(3). С. 119-126.
5. Юрков Н.К. Современное состояние исследований в области создания высоконадежной радиоэлектронной аппаратуры // НиКСС. 2021. №4 (36). С. 5-13.
6. Лысенко И.Е., Ткаченко А.В., Ежова О.А., Коноплев Б.Г. и др. Механические воздействия, влияющие на конструкцию радиочастотных МЭМС-переключателей // Электроника. 2021. №9(2). С. 20-27.
7. Ши И., Шэнь Чж. Последние достижения в области защиты радиочастотных передатчиков // Микромашины. 2022. №13(7). С.10-18.

8. Ли Б., Хэ Ц., Чжен Ю. Технологии защиты систем радиопередачи Copyright © 2020 China Electric Power Press. С. 978.
9. Розоринов Г.А., Гресь А.А., Русин В.В., Шпатарь П.А. Среды электромагнитной совместимости радиоэлектронных средств связи//Информатика и Автоматика. 2021. №1. С. 16-19.
10. Абдимуратов Ж.С., Манбетова Ж.Д., Иманкул М.Н., Чежимбаева К.С., Сагындинова А.Ж. Способы защиты оборудования сотовой (мобильной) связи от электромагнитного воздействия // Новости НАН Республики Казахстан. 2021. №335(1). С. 81-89.
11. Соколов С.С., Иванов Д.А., Федулов Ю.В., Зобнин А.К. Функциональная модель устойчивости радиоэлектронных средств в условиях электромагнитных излучений // Известия ТулГУ. Технические науки. 2022. №9. С. 253-261.
12. Ху Ц., Цзю Х., Ли Я. Воздействие радиочастотного электромагнитного излучения // Радиация и здоровье. 2021. №10. С. 69-80.
13. Сысуев В.А., Яньков Р.В., Лысенко А.В., Алмаметов В.Б., Тюрина Л.А. Современные средства защиты бортовых радиоэлектронных устройств от внешних механических воздействий // НиКа. 2021. №1. С. 70-75.
14. Электромагнитная среда [Электронный ресурс]. Режим доступа: <https://www.sciencedirect.com/topics/engineering/radio-interference/> (дата обращения: 01. 01.2023).
15. Влияние внешних факторов на надежность электронной аппаратуры и компонентов – тепла, холода, влаги, радиации, деградации полупроводников [Электронный ресурс]. Режим доступа: <https://intellect.ml/the-influence-of-external-factors-on-the-reliability-of-electronic-equipment-and-components-heat-cold-moisture-radiation-the-degradation-of-semiconductors-9063/>(дата обращения: 30. 12.2022).

THE IMPACT OF EXTERNAL CONDITIONS ON THE PERFORMANCE OF RADIO-ELECTRONIC MEANS (RES)

DENIS V. STOLBINSKY,
Samara, Russia

PAVEL P. BEM,
Samara, Russia

VADIM A. ANDREEV,
Samara, Russia

DMITRY V. MATVEEV
Samara, Russia

ABSTRACT

Introduction: Ever since the first radio transmitters appeared, designers have been concerned with ensuring their smooth operation and safe operation. However, external conditions continue to form negative factors that affect the performance of equipment. At the same time, it is not possible to predict all possible situations that may affect the performance of radio electronic equipment (RES). **The purpose of the work** is to consider key external factors that can have a negative impact on the performance of electronic equipment. **Methods used:** synthesis of empirical data, analysis of practical studies, compilation of research data. These methods will allow

KEYWORDS: *electronic devices, external factors, system control and safety.*

revealing the issues of methodology from the position of domestic and foreign researchers, as well as identifying the key factors influencing the performance of the RES. The novelty of the work lies in the systematization of the views of domestic and foreign researchers on the problem of monitoring the activities of the PRUE. In addition, external factors that were not taken into account were identified. **Result:** the article will draw conclusions about the possible prevention of the negative impact of key external factors affecting the performance of electronic equipment. **Practical significance:** the presented analysis can be used as a basis for applied research, as well as a guide for enterprises installing radio electronic devices.

REFERENCES

1. Stefanishin D., Kendell J. The influence of radio and television on culture, literacy and education [Electronic resource]. Access mode: <https://blogs.ubc.ca/etec540sept12/2012/10/28/1687/> (accessed 30.12.2022).
2. Werbeke W., Dietz B., Verval E. Drivers of radio system efficiency: a modern meta-analysis // <https://link.springer.com/article/10.1007/s11747-010-0211-8>
3. Parfenov V.I., Le V.D. The use of a wireless sensor system to protect the performance of radio electronic systems. *Computer Optics*. 2021. No. 45(3), pp. 367-371.
4. Lyashchenko V.V. Physical model of protection of cable lines and radio-electronic means of state industrial facilities from external electromagnetic influence in the conditions of emergency prevention. *Social development and safety*. 2019. No. 9 (3), pp.119-126.
5. Yurkov N.K. The current state of research in the field of creating highly reliable radio electronic equipment. 2021. No. 4 (36), pp. 5-13.
6. Lysenko I.E., Tkachenko A.V., Ezhova O.A., Konoplev B.G. and etc. Mechanical effects affecting the design of RF MEMS switches. *Electronics*. 2021. No. 9(2), pp. 20-27.
7. Shi Y., Shen Zh. Recent advances in the field of protection of radio frequency transmitters. *Micromachines*. 2022. No. 13(7), pp. 10-18.
8. Li B., He Q., Zheng Yu. Protection technologies for radio transmission systems Copyright © 2020 China Electric Power Press, p.978.
9. Rozorinov G.A., Gres A.A., Rusin V.V., Shpatar P.A. Environments of electromagnetic compatibility of radio-electronic means of communication. *Informatics and Automation*. 2021. No. 1, pp.16-19.
10. Abdimuratov Zh. S., Manbetova Zh. D., Imankul M. N., Chezhimbaeva K. S., Sagyndikova A. Zh. Ways to protect cellular (mobile) communication equipment from electromagnetic effects. *News of the National Academy of Sciences of the Republic of Kazakhstan*. 2021. No. 335(1), pp.81-89.
11. Sokolov S. S., Ivanov D. A., Fedulov Yu. V., Zobnin A. K. Functional model of stability of radio-electronic means under conditions of electromagnetic radiation. *Izvestiya TulGU. Technical science*. 2022. No. 9, pp. 253-261.
12. Hu Q., Tszu H., Li Ya. Exposure to radio frequency electromagnetic radiation. *Radiation and health*. 2021. No. 10, pp. 69-80.
13. Sysuev V.A., Yankov R.V., Lysenko A.V., Almametov V.B., Tyurina L.A. Modern means of protection of on-board radio-electronic devices from external mechanical influences. *NiKa*. 2021. No. 1, pp. 70-75.
14. Electromagnetic environment [Electronic resource]. Access mode: <https://www.sciencedirect.com/topics/engineering/radio-interference/> (accessed 01.01.2023).
15. Influence of external factors on the reliability of electronic equipment and components - heat, cold, moisture, radiation, degradation of semiconductors [Electronic resource]. Access mode: <https://intellect.ml/the-influence-of-external-factors-on-the-reliability-of-electronic-equipment-and-components-heat-cold-moisture-radiation-the-degradation-of-semiconductors-9063/> (Accessed 30.12.2022).

INFORMATION ABOUT AUTHORS:

Denis V. Stolbinsky, postgraduate student, Samara National Research University named after Academician S.P. Koroleva, Samara, Russia, denver7074@yandex.ru

Pavel P. Bem, postgraduate student, Samara National Research University named after Academician S.P. Koroleva, Samara, Russia, bem@testelektro.ru

Vadim A. Andreev, postgraduate student, Samara National Research University named after Academician S.P. Koroleva, Samara, Russia, andreev.rus.vasilevka@yandex.ru

Dmitry V. Matveev, student, Samara National Research University named after Academician S.P. Koroleva, Samara, Russia, matveev_d.v.1993@mail.ru

For citation: Stolbinsky D.V., Bem P.P., Andreev V.A., Matveev D.V. The impact of external conditions on the performance of radio-electronic means (RES). *H&ES Reserch*. 2023. Vol. 15. No. 2. P. 18-22. doi: 10.36724/2409-5419-2023-15-2-18-22 (In Rus)



doi: 10.36724/2409-5419-2023-15-2-23-32

ЭФФЕКТИВНОСТЬ ФРЕЙМВОРКОВ ДЛЯ ПЕРЕДАЧИ ИНФОРМАЦИИ В ВИРТУАЛИЗИРОВАННОЙ СЕТИ СВЯЗИ С МИКРОСЕРВИСНОЙ АРХИТЕКТУРОЙ

БУЖИН

Игорь Геннадьевич¹

ДЕРЕВЯНКИН

Алексей Юрьевич²

АНТОНОВА

Вероника Михайловна³

ПЕРЕВАЛОВ

Алексей Павлович⁴

МИРОНОВ

Юрий Борисович⁵

Сведения об авторах:

¹к.т.н., доцент кафедры "Сети и системы фиксированной связи", Московский Технический Университет Связи и Информатики, Москва, Россия, i.g.buzhin@mtuci.ru

²магистрант, Московский Технический Университет Связи и Информатики, Москва, Россия, alexeyderevyankin@yahoo.com

³к.т.н., доцент, зав. кафедры "Сети и системы фиксированной связи", Московский Технический Университет Связи и Информатики, Москва, Россия, v.m.antonova@mtuci.ru

⁴аспирант, Московский Технический Университет Связи и Информатики, Москва, Россия, a.p.perevalov@mtuci.ru

⁵к.т.н., декан факультета "Сети и системы связи", Московский Технический Университет Связи и Информатики, Москва, Россия, i.b.mironov@mtuci.ru

АННОТАЦИЯ

Введение: При проектировании различных информационных систем наблюдается переход от классической монолитной архитектуры построения сети к микросервисной. В связи с этим возникает необходимость устанавливать требования к показателям соединений между микросервисами, которые реализуются с помощью различных фреймворков. **Цель исследования:** сравнительный анализ фреймворков для передачи данных в микросервисной архитектуре по нескольким критериям, выработка рекомендаций по эффективному выбору средств для коммуникации микросервисов. **Результаты:** проведен сравнительный анализ RPC-фреймворков по следующим критериям: наличие центра регистрации, наличие встроенных средств безопасности на уровне фреймворка, основные технологии сериализации, возможность балансировки нагрузки. Разработан экспериментальный стенд, на основе которого были измерены и проведен сравнительный анализ временных задержек при передаче разного объема нагрузки. В случае передачи информации малого размера, по полученным значениям можно сделать вывод, что минимальная задержка вызова удаленной процедуры у фреймворка RPCX, у Apache Dubbo напротив – задержка максимальна. При изменении типа передачи с унарных вызовов на потоковую, задержка уменьшается.

КЛЮЧЕВЫЕ СЛОВА: микросервисная архитектура, gRPC, Apache Thrift, Apache Dubbo, RPCX.

Для цитирования: Бужин И.Г., Деревянкин А.Ю., Антонова В.М., Перевалов А.П., Миронов Ю.Б. Эффективность фреймворков для передачи информации в виртуализированной сети связи с микросервисной архитектурой // Научные технологии в космических исследованиях Земли. 2023. Т. 15. № 2. С. 23-32. doi: 10.36724/2409-5419-2023-15-2-23-32

Введение

Современные инфокоммуникационные сети включают в себя множество архитектурных элементов, в том числе виртуализированную сетевую инфраструктуру, и предполагают наличие таких требований, как масштабируемость, модульность, независимость от используемых платформ и инструментов разработки, использование стандартизированных интерфейсов для взаимодействия по стандартизированным протоколам. Использование монолитной архитектуры при реализации виртуализированной сетевой инфраструктуры ограничивает возможность модернизации системы, увеличивает ее программную сложность, затрудняет реализацию интерфейсов для управления и мониторинга. Таким образом, наблюдается переход от классической монолитной архитектуры построения сети к микросервисной. При такой реализации архитектуры возрастает количество устанавливаемых соединений в программных системах. В связи с этим возникает необходимость устанавливать требования к показателям соединений между микросервисами [1, 15]. В качестве таких показателей могли выступать задержка установленного соединения, количество запросов за интервал, эффективность балансировки нагрузки, скорость сжатия сообщения для передачи и т.д. Для обеспечения нужного уровня всех показателей необходимо эффективное использование инструментами для передачи данных в микросервисной архитектуре.

Одним из распространенных способов запуска микросервисов является использование контейнеров. Для управления контейнерами используются средства для оркестровки, например Kubernetes. Системы оркестровки включают в себя множество услуг, таких как мониторинг и конфигурация сети, балансировка нагрузки, планирование, DNS-службы и др. Внутри компании контейнеры взаимодействуют друг с другом посредством межсервисной связи [2, 13].

Принцип функционирования RPC

Использование RPC (от англ. remote procedure call (Удаленный вызов процедур)) в качестве межсервисного взаимодействия приносит некоторые преимущества. Одно из главных преимуществ заключается в абстрагировании разработчика от многих механизмов, связанных с коммуникацией, вместо этого разработчик может сосредоточиться над проблемами функциональности разрабатываемого приложения [2, 16].

Стоит отметить, что для ряда задач, использование RPC приведет к большим затратам, чем использование других технологий, например REST (от англ. Representational State Transfer — «передача репрезентативного состояния») или SOAP (от англ. Simple Object Access Protocol — простой протокол доступа к объектам). Поэтому стоит комбинировать средства для межсервисной коммуникации в программных системах.

В [3] подробно описан процесс установления соединения по протоколу RPC. Процесс можно разделить на следующую последовательность (рис. 1):

1. Приложение на стороне клиента вызывает метод, находящийся в клиентской заглушке (англ. client stub), передавая входные параметры.
2. Заглушка упаковывает имя метода и входные параметры в тело запроса и передает его в библиотеку среды выполнения (англ. run-time library).
3. Библиотека обрабатывает запрос и передает транспортной службе узла.
4. Клиент отправляет запрос на адрес сервера.
5. Библиотека среды восстанавливает сообщение, полученное из транспортной службы сервера.
6. Сообщение распаковывается и передается на серверную заглушку.
7. Серверная заглушка вызывает нужный метод, реализованный в серверном приложении.
8. После выполнения вызываемого метода, возвращаемое значение преобразуется в ответное сообщение заглушкой сервера.
9. Заглушка передает ответное сообщение библиотеке среды выполнения сервера.
- 10-13. После чего ответное сообщение передается клиентской заглушке таким же образом, как сообщение запроса было передано на серверную заглушку.
14. Клиентская заглушка преобразует ответное сообщение в возвращаемое значение вызываемого изначально метода и возвращает его клиентскому приложению.

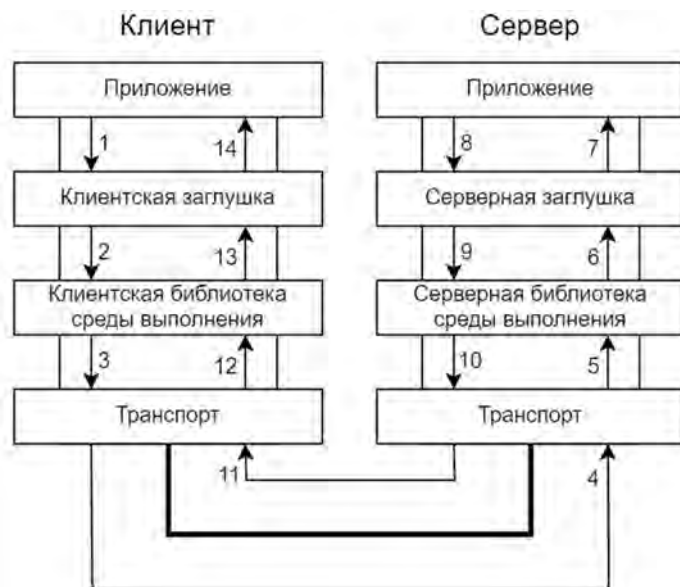


Рис. 1. Процесс установления соединения по протоколу RPC

Сравнительный анализ фреймворков для реализации RPC соединений

Существует множество фреймворков для реализации RPC соединений. В данной статье исследованы четыре RPC-фреймворка: «Apache Thrift», «gRPC», «RPCX» и «Apache Dubbo».

Одним из популярных фреймворков в наши дни является *gRPC*. Данное решение было предоставлено компанией Google в открытый доступ в 2015 году под лицензией Apache License 2.0. *gRPC* использует протокол HTTP/2 (англ. HyperText Transfer Protocol v2.0 – «протокол передачи гипертекста v2.0») для передачи данных и «Protocol Buffers» в качестве языка описания интерфейса. Фреймворк имеет встроенную поддержку установления безопасного соединения с использованием механизма аутентификации, а также средства для балансировки нагрузки на стороне клиента.

Технология *gRPC* позволяет определить четыре типа передачи [4]:

1. Унарные вызовы, при которых клиент делает запрос на сервер и получает обратно один ответ как при обычном вызове функции.

2. Серверные потоковые вызовы, в которых клиент делает запрос на сервер и получает обратно поток последовательно сообщений. Клиент считывает данные из возвращенного потока до тех пор, пока не останется сообщений с серверной части. Все полученные сообщения упорядочиваются.

3. Клиентские потоковые вызовы. В данном типе передачи, клиент отправляет поток сообщений на сервер, сервер в свою очередь, получив все сообщения, возвращает ответ клиенту в виде одного сообщения.

4. Двухнаправленные потоковые вызовы, в которых обе стороны обмениваются потоками сообщений. Потоки передаются независимо, поэтому клиент и сервер могут считывать и записывать данные в произвольном порядке.

Для передачи данных, *gRPC* использует двоичный протокол HTTP/2, который поддерживает асинхронную обработку запросов – при передаче сообщения не блокируют друг друга и не ждут в очереди обработки других. Для сериализации данных по умолчанию *gRPC* использует Protobuf, но также поддерживает другие форматы, например JSON (англ. JavaScript Object Notation).

Балансировку в *gRPC* можно разделить на два архитектурных типа: на стороне прокси (используя Load Balancer) и на стороне клиента. При отправке клиентом запроса на прокси, запрос пересылается на сервер с наименьшей загрузкой. При этом клиенты ничего не знают о внутренних серверах. Сам балансировщик отслеживает загрузку серверов с помощью специальных сообщений, получаемых от всех серверов. В случае балансировки на стороне клиента, клиент получает отчеты о загрузке внутренних серверов и реализует алгоритмы балансировки нагрузки [5].

Если говорить о плюсах данных типов, то в случае с прокси можно выделить отсутствие осведомленности о серверной части на стороне клиента, а в случае клиентской балансировки плюсом является высокая производительность из-за отсутствия дополнительных скачков загрузки. Из недостатков можно отметить присутствие дополнительного узла, что негативно сказывается на задержке в первом типе, и большое количество возложенных на клиента функций во втором типе. Вдобавок, при балансировке без прокси, клиент может отслеживать состояние сервера.

Рабочий процесс балансировки показан на рисунке 2. При запуске клиент получает информацию от распознавателя

имён (англ. Name Resolver) которая содержит список доступных IP-адресов с произвольными атрибутами и конфигурацией сервисов (1).

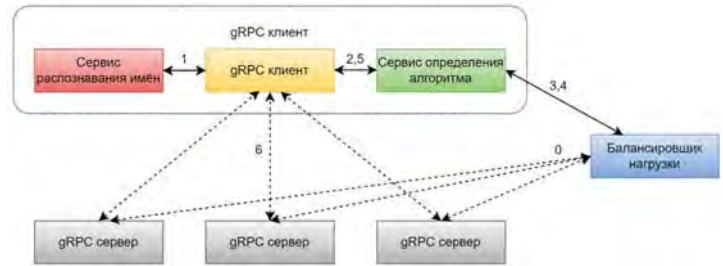


Рис. 2. Схема балансировки нагрузки *gRPC*

Атрибуты и конфигурация используются для определения алгоритма балансировки. По умолчанию в качестве распознавателя имён используется DNS служба. Затем клиент передаёт конфигурацию и атрибуты на сервис, отвечающий за выбор алгоритма балансировки (2). Как упоминалось ранее, можно использовать балансировщик как прокси-сервис. Балансировщик отслеживает состояние *gRPC*-серверов (0), и принимает все решения по балансировке запросов – для этого необходимо отправлять запросы на балансировщик (3,4). В конечном итоге, клиент получает информацию о том, на какой сервер осуществить *RPC*-вызов.

gRPC поддерживает три алгоритма балансировки: Pick First, Round Robin и *gRPC* Load Balancing. Основным алгоритмом по умолчанию является Pick First. После получения списка IP-адресов от распознавателя имён, балансировщик, начинает опрашивать сервисы из списка до тех пор, пока не установит соединение. Если соединение установлено, то оно помечается соответствующим флагом о готовности. Далее клиент подключается к первому в списке сервису.

В *gRPC* встроены следующие методы аутентификации [6]:

- Возможно использование SSL/TLS для аутентификации на сервере и шифрования соединения между клиентом и сервером;
- Аутентификация на основе JWT-токенов. Токены передаются в качестве метаданных авторизации по защищенному с помощью механизма SSL/TLS каналу.
- Поддержка ALTS (англ. Application Layer Transport Security). Данная система аутентификации и транспортного шифрования используется в случае запуска сервисов в GCP (англ. Google Cloud Platform).

Данные метода аутентификации подходят как для внутреннего взаимодействия между сервисами, так и для внешнего API.

Apache Dubbo – это высокопроизводительный *RPC*-фреймворк с открытым исходным кодом на основе Java. Изначально проект разрабатывался под руководством Alibaba Group, но в 2018 году перешел под управление некоммерческой организации Apache Software Foundation. В настоящее время поддерживается организацией Apache. *Apache Dubbo* используется более чем в 150 компаниях, включая Alibaba Group, China Telecom и другие, а реализация на Golang используется в Xiaomi Inc. *Dubbo* имеет реализации на языках Java, Golang, Erlang и Rust.

В качестве протокола передачи, Dubbo использует протокол Tripple, основанный на HTTP/2. Фреймворк также поддерживает опцию межязыкового взаимодействия – для этого необходимо использовать язык для описания интерфейсов IDL (англ. Interface Definition Language). В качестве IDL возможно использование Protobuf, Hessian и др. Hessian это двоичный протокол, разработанный Cauchy Technology на языке Java, используемый Dubbo по умолчанию. Для языка Golang официальной версии технологии описания интерфейса от разработчиков не предоставляется, но доступны сторонние реализации с открытым исходным кодом.



Рис. 3. Коммуникация между компонентами Dubbo

На рисунке 3 представлена схема коммуникации между компонентами Apache Dubbo при вызове потребителем услуги у поставщика. В качестве услуг выступают те процедуры, которые разработчик определил с помощью IDL. Для этого выполняются следующие шаги [7]:

0. Контейнер производит запуск поставщика.

1. Поставщик регистрирует свои услуги в регистрационном центре при запуске. В качестве регистрационных центров можно использовать Zookeeper, Nacos, etcd и Consul.

2. Потребитель фиксирует регистрационный центр при запуске.

3. Регистрационный центр возвращает список поставщиков потребителю; при изменении списка поставщиков, регистрационный центр оповестит об этом потребителя.

4. Основываясь на алгоритме балансировки нагрузки, потребитель выбирает поставщика и выполняет вызов.

5. При запуске, монитор фиксирует всех поставщиков и потребителей, которые зарегистрировались; потребитель и поставщик подсчитывают количество вызовов и каждую минуту отправляют статистику монитору.

Dubbo поддерживает верификацию по JWT-токенам. Поставщик генерирует токен и передает его в регистрационный центр, после чего потребитель может запросить токен в регистрационном центре перед вызовом службы и подтвердить свою подлинность у поставщика.

Для балансировки нагрузки Apache Dubbo использует, так называемую, технологию гибкой балансировки. Традиционно балансировка нагрузки основывается на устоявшихся алгоритмах таких как Round Robin, Least Connections, Sticky Sessions и др. Dubbo при балансировке оценивает динамиче-

ски пропускную способность между потребителем и поставщиком с помощью коэффициента использования услуг поставщика. При увеличении количества запросов (рис. 4), время отклика на вызываемую услугу увеличивается линейно (B и C) до определенной критической точки.

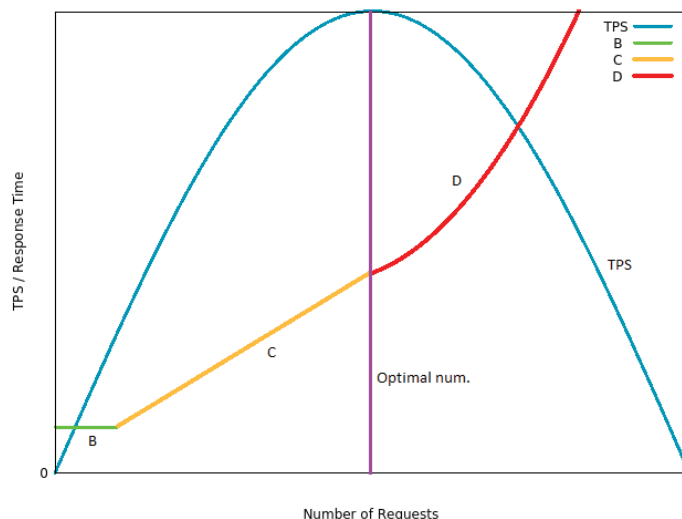


Рис. 4. Зависимость коэффициента использования услуг от количества запросов поставщикам при балансировке

Далее при увеличении количества запросов время отклика будет увеличиваться экспоненциально (D). Критическая точка является экстремумом кривой коэффициента использования услуг. Исходя из этого можно сделать вывод, что суть гибкой балансировки заключается в поддержании максимального значения коэффициента использования услуг, то есть оптимального количества запросов на один сервис [8].

RPCX это многофункциональный, быстрый и простой в использовании, подобный Apache Dubbo и Weibo Motan, RPC-фреймворк, за основу которого была взята стандартная библиотека RPC языка Golang.

Стандартно, для передачи байт данных, RPCX использует протоколы TCP или UDP – транспортные протоколы семиуровневой модели OSI. Фреймворк также поддерживает HTTP-вызовы на прикладном уровне, но сам разработчик, в виду производительности, не рекомендует их использовать. Также была добавлена поддержка протокола QUIC, описанного в RFC 9000. Для сериализации данных RPCX поддерживает множество технологий (Avro, JSON, Protobuf и др) и даёт возможность пользователю для написания собственного кода. По умолчанию RPCX использует формат MessagePack – это двоичная форма представления структур данных [8].

Схема взаимодействия клиента и сервера очень схожа со схемой Apache Dubbo. Незначительные отличия могут быть в связи с регистрационным центром в некоторых версиях. В качестве регистрационного центра фреймворк поддерживает Apache Zookeeper, etcd, Consul и mDNS.

Отдельно следует отметить возможность развертывания в режиме прокси, когда клиент взаимодействует с компонентами через отдельный сервис.

Возможно два варианта развертывания схемы в данном режиме (рис. 5): шлюз на отдельной машине и агент на локальной машине с клиентом. В первом случае шлюз отвечает за преобразования HTTP запросов в RPC вызовы и наоборот. Как вариант, можно развернуть несколько шлюзов и использовать Nginx для балансировки нагрузки между клиентами. Во втором случае роль агента схожа с ролью шлюза, но агент развертывается на локальной машине с клиентом в виде отдельной службы и взаимодействует с регистрационным центром и сервисом.



Рис. 5. Варианты развертывания прокси между клиентом и сервисом RPCX

Как было упомянуто ранее в качестве протокола передачи, RPCX использует протокол TCP. Конкретно в реализации на Golang, которая будет рассмотрена в данной статье, используется стандартная библиотека “net”. Поэтому для того, чтобы повысить защищенность соединения необходимо настроить TLS-сессию. Сделать это можно, сгенерировав ключи и сертификат с помощью библиотеки OpenSSL и подключив библиотеку «tls».

На прикладном уровне, как утверждает разработчик, поддерживается аутентификация с помощью токенов. Сама же реализация очень проста и суть её заключается в проверке двух строк через оператор «equal-to», но пользователь может изменить логику аутентификации самостоятельно.

Для балансировки нагрузки RPCX использует набор стандартных алгоритмов: Round Robin, Weight Round Robin, Random (без балансировки). Если пользователю предпочтительнее распределить нагрузку по качеству соединения, то реализован и такой метод, основанный на данных ring. Для крупномасштабных, в плане расположения серверов, задач существует реализация балансировки по географическим координатам – клиенту будут предложены услуги самого ближнего находящегося к нему сервера. Возможно написание реализации балансировки и самим пользователем.

В RPCX встроено множество дополнительных плагинов, таких как: широковещательная рассылка запросов на все сервисы, health check для поддержки состояния сессии, группировка услуг по определенным параметрам, мониторинг показателей сервисов с помощью Grafana и др. Пользователю доступна разработка плагинов самостоятельно.

Apache Thrift – это платформа для межязыковой сериализации и удаленного вызова процедур, разработанная некоммерческой организацией Apache Software Foundation. Фреймворк поддерживает более 20 языков программирования, среди которых есть C++, Java и Golang. Компания Meta совместно с Apache Software Foundation разработала собственную усовершенствованную версию фреймворка и открыла доступ в феврале 2014 года под названием Facebook Thrift.

Thrift также использует прикладной протокол HTTP/2 для передачи данных, но также возможна передача байт данных с помощью транспортного протокола TCP. По умолчанию, фреймворк использует собственное решение Apache Thrift IDL которое поддерживает три протокола сериализации данных [9].

В отличие от Dubbo и RPCX, Apache Thrift не имеет центра регистрации. Архитектура взаимодействия клиента и сервера платформы Thrift напоминает стандартную схему взаимодействия RPC (рис. 6) [9].

Внизу стека располагается транспорт, изолирующий верхние уровни от устройств. Транспорт позволяет читать и записывать потоки байт вне зависимости от производителя и прошивки устройств, поддерживая новые типы устройств и версии промежуточного программного обеспечения. В качестве транспорта при асинхронной передаче используется транспорт кадрирования (англ. Framed Transport) – к каждому сообщению добавляется четырёхбайтовый префикс с размером сообщения для более эффективной обработки. При синхронной передаче используется буферизированный транспорт (англ. Buffered Transport), который записывает данные переданных пакетов во внутренний буфер.

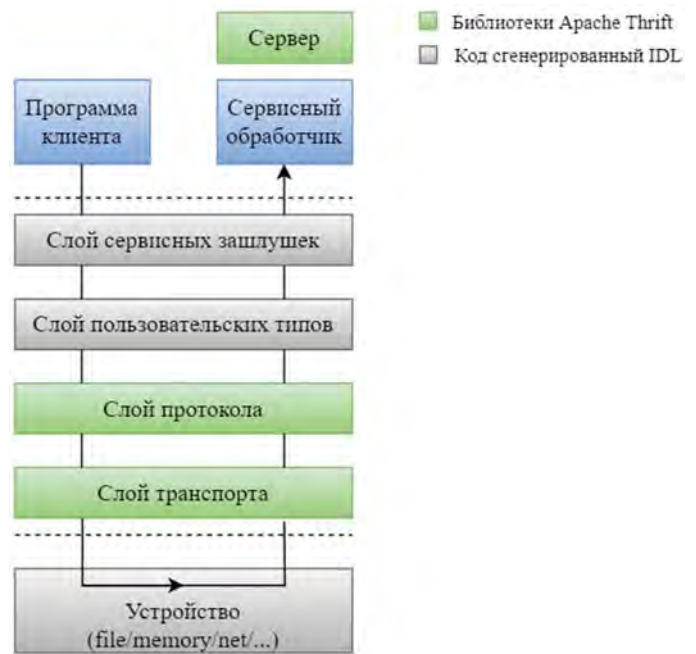


Рис. 6. Архитектура фреймворка Apache Thrift

«Protocol» – это слой сериализации типов. Apache Thrift IDL поддерживает в основном базовые типы данных, определенных в большинстве языках (int, string, float и др.), а также распространенные типы контейнеров: map, set и list [10].

Apache Thrift IDL поддерживает следующие протоколы сериализации: Compact Protocol, Binary Protocol и JSON Protocol. Binary Protocol - протокол перевода данных в поток байт. Compact Protocol кодирует данные более сложными типами кодировок, за счёт чего уменьшается размер передаваемых данных, но требуется больше ресурсов центрального процессора чем у Binary Protocol.

JSON Protocol преобразует входные данные в устоявшийся JSON формат, что дает более широкую совместимость и удобочитаемость, но потребляет больше всего системных ресурсов и увеличивает время передачи [9].

Слой “User types” определяет интерфейс использования типов. Пользователь в конфигурационном IDL файле имеет возможность определять собственные типы в виде структур. Структуры представляют собой набор полей, состоящих из базовых типов.

«Services stubs» предоставляет пользователю интерфейс для вызова удаленных процедур в виде сгенерированных заглушек.

Apache Thrift не предусматривает средств для защиты соединения на уровне фреймворка, поскольку многие используемые системы размещены в защищенных центрах обработки данных. Для установления безопасного соединения возможно настроить механизмы SSL/TLS, либо реализовать систему безопасности самостоятельно.

Для балансировки нагрузки также следует использовать сторонние сервисы.

В табл.1 представлено сравнение RPC-фреймворков по расписанным выше критериям.

Таблица 1

Сравнение RPC-фреймворков

| | <i>Apache Dubbo</i> | <i>RPCX</i> | <i>Apache Thrift</i> | <i>gRPC</i> |
|---|--|-----------------------------------|---|---|
| Центр регистрации | + | + | - | - |
| Встроенные средства безопасности на уровне фреймворка | + | - | - | + |
| Основные технологии сериализации | Hessian | MsgPack | Binary Protocol и Compact Protocol | Protobuf |
| Балансировка нагрузки | Помимо стандартных алгоритмов, имеет собственные решения | Реализованы стандартные алгоритмы | - | Реализованы некоторые стандартные алгоритмы |
| Поддерживаемые ЯП | Java, Golang, Erlang, Rust | Golang, Rust, Java | Поддерживает 28 языков программирования | Поддерживает 13 языков программирования |

Экспериментальное исследование

Для сравнения фреймворков по задержке были проведены тестовые измерения путём передачи данных между клиентом и сервером. В качестве языка программирования для написания приложений был выбран язык Golang. Основной причиной выбора стало наличие реализаций на данном языке у рассмотренных решений.

Измерения производились на вычислительной машине со следующими характеристиками:

- CPU: Intel(R) Core (TM) i5-10300H CPU @ 2.50GHz 2.50 GHz
- RAM: 16 GB
- Версия OS: Ubuntu 20.04.5 LTS, amd64
- Версия Golang: 1.19.4
- gRPC: 1.51.0
- RPCX: v1.7.11
- Apache Thrift: 0.17.0
- Apache Dubbo: v3.0.2

Клиент и сервер запускались в docker-контейнерах и передавали между собой полезную нагрузку. В роли средств мониторинга и визуализации метрик использовалась связка Grafana и Prometheus. Для средств оркестрации docker-контейнеров, с помощью инструмента для запуска локального кластера kind, был развернут Kubernetes кластер. Полученные данные были проанализированы и представлены в виде графиков и гистограмм, построенных с помощью программы gnuplot. На рис. 7 приведена примерная схема развернутого кластера для снятия тестовых измерений.

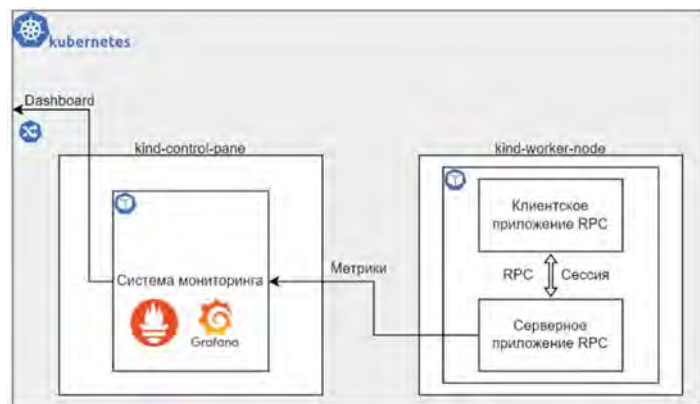


Рис. 7. Схема экспериментального кластера

Размер малых данных передаваемых в качестве полезной нагрузки можно считать пренебрежимо малым, при передаче же массивных данных, добавлялась произвольная полезная нагрузка размером 437 кБайт. Для измерения задержки каждого соединения использовалась встроенная в язык Go библиотека «time». Также стоит отметить, что вызов считается завершенным, когда сторона, открывшая соединение, его закрывает.

На рисунке 8 представлен результат исследования при передаче малых и больших данных между клиентом и сервером. В случае передачи информации малого размера, по полученным значениям можно сделать вывод, что минимальная задержка вызова удаленной процедуры у фреймворка RPCX, у Apache Dubbo напротив – задержка максимальна. Полученные результаты можно объяснить использованием технологий представления данных для передачи. RPCX сериализует данные с помощью MsgPack, который не упаковывает никакую дополнительную мета информацию в передаваемые сообщения, что дает высокую производительность, однако возникают сложности при передаче больших данных с большим количеством полей, поскольку приходится обрабатывать каждое поле структуры.

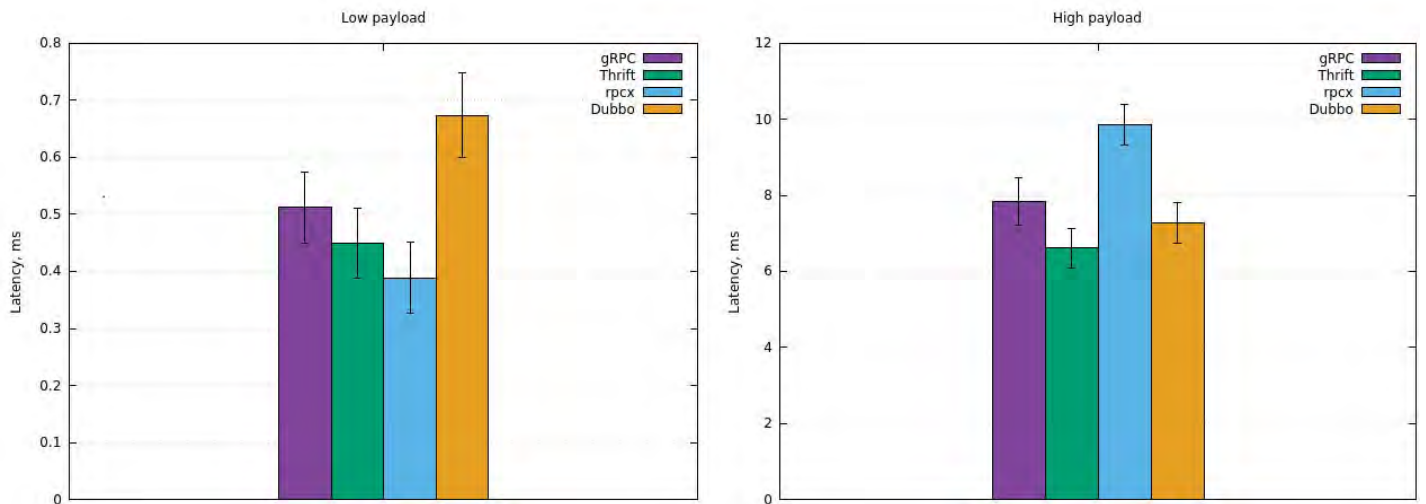


Рис. 8. Сравнение RPC-фреймворков при передаче малой и большой полезной нагрузки по задержке (95th percentile)

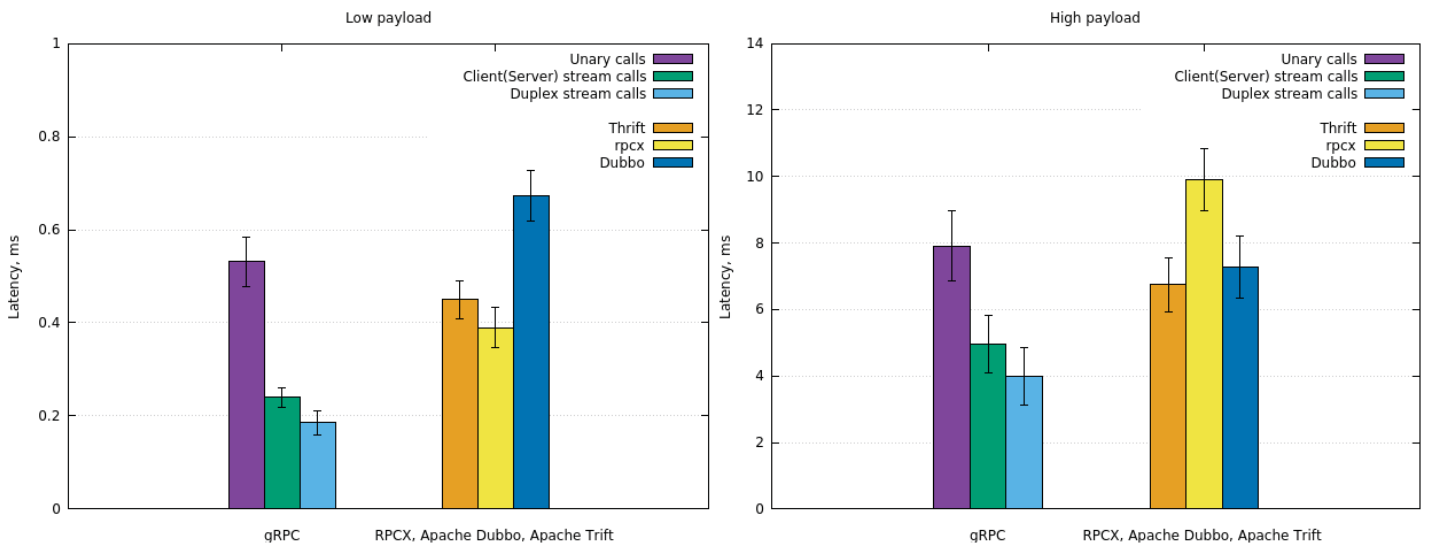


Рис. 9. Сравнение RPC-фреймворков при разных типах передач gRPC (95th percentile)

Метаинформация Thrift содержит много различных идентификаторов, что даёт большую задержку в передаче. Dubbo использует протокол Hessian, также который является двоичным. Большая задержка при передаче малых данных может говорить как о большом количестве сторонней дополнительной информации в сообщении, так и о недочётах в реализации на Golang. В тестировании использовалась версия Hessian из официального репозитория Apache Software Foundation.

Результаты Protobuf и gRPC следует выделить отдельно. Как было упомянуто ранее, gRPC имеет четыре типа передачи. На приведенном выше рисунке 8 был использован только тип передачи унарных вызовов, поэтому сравнение можно представить следующим образом (рис. 9). При изменении типа передачи с унарных вызовов на потоковую, задержка уменьшается. Этот факт можно объяснить следующим образом: при потоковой передаче, данные разбиваются на части на уровне фреймворка и передаются асинхронно в

разных горутинах [12] (англ. Goroutine). В случае двунаправленной передачи, полезная нагрузка вовсе передавалась в обе стороны по 437 КБайт.

Заключение

Таким образом, в результате сравнительного анализа RPC-фреймворков для передачи данных в микросервисной архитектуре можно сделать вывод, что при выборе средств для коммуникации сервисов необходимо находить компромисс между производительностью и функционалом технологии для решения задачи. Для большинства задач, завязанных на производительность и задержку системы, а также передачу массивных данных, следует рассмотреть вариант использования потоковых передач gRPC. Протокол Protobuf является одним из самых быстрых на обработку и компактных на передачу протоколов сериализации.

Решая простые задачи, не требующие высокой производительности, но требующие разнообразия функций инструмента рекомендуется рассмотреть фреймворк RPCX. Данный фреймворк показал свою простоту в реализации клиентской и серверной части, а широкий функционал позволил осуществить передачу метрик на систему мониторинга без использования сторонних библиотек. Для передачи массивных данных фреймворк RPCX не подходит.

Для построения сложных систем, требующих возможности расширить функциональность инструмента, стоит сделать выбор в сторону решения от Apache Dubbo. Помимо уже имеющегося набора функций, фреймворк является достаточно гибким для реализации и внедрения собственных решений. Проблемы возможны при изучении официальной документации, поскольку фреймворк изначально разрабатывался китайской компанией и имеет небольшую часть описаний на английском языке.

В больших и сложных системах, требующих высокой точности описания инструмента, возможности для расширения и в то же время высокой производительности предлагается использовать фреймворк Apache Thrift. Из-за большого количества документации данным инструментом можно овладеть в совершенстве за относительно короткий промежуток времени, а также возможно расширить функционал. Двоичные протоколы сериализации являются одними из самых производительных, что обеспечивает большую скорость при передаче.

Литература

1. Zhizhou Zhang, Murali Krishna Ramanathan, Prithvi Raj, Abhishek Parwal, Timothy Sherwood, Milind Chabbi. CRISP: Critical Path Analysis of Large-Scale Microservice Architectures // USENIX Annual Technical Conference, 2022, Carlsbad, CA, USA.
2. Zhipeng Jia, Emmett Witchel. Nightcore: Efficient and Scalable Serverless Computing for Latency-Sensitive, Interactive Microservices // ASPLOS '21, April 19-23, 2021, Virtual, USA.
3. Принцип работы RPC // Официальная документация Microsoft. [Электронный ресурс]: <https://learn.microsoft.com/ru-ru/windows/win32/rpc/how-rpc-works>.
4. Introduction to gRPC // Официальная документация gRPC. [Электронный ресурс]: <https://grpc.io/docs/what-is-grpc/introduction/>.
5. gRPC Load Balancing // Официальная документация gRPC. [Электронный ресурс]: <https://grpc.io/blog/grpc-load-balancing/>.
6. Michal Stefanic. Developing the guidelines for migration from RESTful microservices to gRPC // Masaryk University, Faculty of Informatics, Brno, 2021.
7. Architecture of Apache Dubbo // Официальная документация Apache Dubbo. [Электронный ресурс]: <https://dubbo.apache.org/en/docs/v2.7/user/preface/architecture/>.
8. Flexible load balancing // Официальная документация Apache Dubbo. [Электронный ресурс]: https://dubbo.apache.org/zh/docs3-v2/golang-sdk/concept/service_management/adaptive_lb/.
9. Randy Abernethy. Programmer's guide to Apache Trift // Manning Publications Co, 2019.
10. Introduction to RPCX // Официальная документация RPCX. [Электронный ресурс]: <https://doc.rpccx.io/>.
11. Thrift types // Официальная документация Apache Thrift. [Электронный ресурс]: <https://thrift.apache.org/docs/types.html>.
12. Goroutines // Официальная документация Golang. [Электронный ресурс]: <https://go.dev/tour/concurrency>.
13. Thurlow R. RFC 5531: RPC: Remote procedure call protocol specification version 2. 2009.
14. He X., Yang X. Authentication and authorization of end user in microservice architecture // Journal of Physics: Conference Series. IOP Publishing, 2017. Т. 910. №1. С. 012060.
15. Safaryan O. et al. Information system development for restricting access to software tool built on microservice architecture // E3S Web of Conferences. EDP Sciences, 2020. Т. 224. С. 01041.
16. El Kholly M., El Fatatry A. Framework for interaction between databases and microservice architecture // IT Professional. 2019. Т. 21. №. 5. С. 57-63.
17. Mochalov V. P. et al. Methods and models of resource allocation service in load balancing clusters for data centers. 2022.
18. Мочалов В.П. и др. Инфокоммуникационные технологии // Инфокоммуникационные технологии. 2021. Т. 19. №2. С. 163-172.
19. Буранов М.А., Карташевский В.Г., Мутханна А.С. Анализ параметров функционирования программно-конфигурируемой сети на основе протокола OpenFlow // Электросвязь. 2022. № 4. С. 2-7. DOI 10.34832/ELSV.2022.29.4.001. EDN KMHZKH.
20. Stepanov M.S., Stepanov S.N., Ndayikunda J. et al. The Increasing of Resource Sharing Efficiency in Network Slicing Implementation // Communications in Computer and Information Science. 2022. Vol. 1552. P. 18-35. DOI 10.1007/978-3-030-97110-6-2. EDN ZSXJTR.
21. Vilalta R. et al. GRPC-based SDN control and telemetry for soft-failure detection of spectral/spacial superchannels // 45th European Conference on Optical Communication (ECOC 2019). IET, 2019. С. 1-4.



THE EFFECTIVENESS OF FRAMEWORKS FOR TRANSMITTING INFORMATION IN A VIRTUALIZED COMMUNICATION NETWORK WITH A MICROSERVICE ARCHITECTURE

IGOR G. BUZHIN,

Moscow, Russia, i.g.buzhin@mtuci.ru

ALEKSEY YU. DEREVYANKIN,

Moscow, Russia, alexeyderevyankin@yahoo.com

VERONIKA M. ANTONOVA,

Moscow, Russia, v.m.antonova@mtuci.ru

ALEKSEY P. PEREVALOV,

Moscow, Russia, a.p.perevalov@mtuci.ru

YURIY B. MIRONOV,

Moscow, Russia, i.b.mironov@mtuci.ru

KEYWORDS: *microservice architecture, gRPC, Apache Thrift, Apache Dubbo, RPCX.*

ABSTRACT

Introduction: Different information system designs are moving from a classical monolithic network architecture to a microservice one. Therefore, there is a need to set requirements to the performance of interconnection between microservices, which are implemented using various frameworks. **The aim of this study** is to make a comparative analysis of frameworks for data transmission in a microservice architecture according to several criteria as well as to develop recommendations for effective selection of tools for microservice communication. **The results** of the study include a comparative analysis of RPC frameworks by the fol-

lowing criteria: the availability of a registration centre, the availability of built-in framework-level security features, the main serialization technologies, the ability to balance the load. An experimental stand was developed; it was used to measure time delays and to make their comparative analysis while transmitting different data workload. When small amounts of information are transferred, the values obtained indicate that the RPCX framework has the lowest latency for a remote procedure call, while Apache Dubbo, on the contrary, has the highest latency. When the transfer type switches from unary calls to streaming, the latency decreases.

REFERENCES

1. Zhizhou Zhang, Murali Krishna Ramanathan, Prithvi Raj, Abhishek Parwal, Timothy Sherwood, Milind Chabbi. CRISP: Critical Path Analysis of Large-Scale Microservice Architectures. *USENIX Annual Technical Conference, 2022*, Carlsbad, CA, USA.
2. Zhipeng Jia, Emmett Witchel. Nightcore: Efficient and Scalable Serverless Computing for Latency-Sensitive, Interactive Microservices. *ASPLOS '21*, April 19-23, 2021, Virtual, USA.
3. The principle of RPC operation // Official Microsoft documentation. [Electronic resource]: <https://learn.microsoft.com/ru-ru/windows/win32/rpc/how-rpc-works>.
4. Introduction to gRPC // Official gRPC documentation. [Electronic resource]: <https://grpc.io/docs/what-is-grpc/introduction/>.
5. gRPC Load Balancing // Official gRPC documentation. [Electronic resource]: <https://grpc.io/blog/grpc-load-balancing/>
6. Michal Stefanic. Developing the guidelines for migration from RESTful microservices to gRPC. *Masaryk University, Faculty of Informatics*, Brno, 2021.
7. Architecture of Apache Dubbo // Официальная документация Apache Dubbo. [Electronic resource]: <https://dubbo.apache.org/en/docs/v2.7/user/preface/architecture/>.
8. Flexible load balancing // Official Apache Dubbo documentation. [Electronic resource]: https://dubbo.apache.org/zh/docs3-v2/golang-sdk/concept/service_management/adaptive_lb/.
9. Randy Abernethy. Programmer's guide to Apache Trift. Manning Publications Co, 2019.
10. Introduction to RPCX // Official RPCX documentation. [Electronic resource]: <https://doc.rpcx.io/>.
11. Thrift types // Official Apache Thrift documentation. [Electronic resource]: <https://thrift.apache.org/docs/types.html>.

12. Goroutines. Official documentation of Golang. [Electronic resource]: <https://go.dev/tour/concurrency>.
13. Thurlow R. RFC 5531: RPC: Remote procedure call protocol specification version 2. 2009.
14. He X., Yang X. Authentication and authorization of end user in microservice architecture. *Journal of Physics: Conference Series*. IOP Publishing, 2017. Vol. 910. No. 1. P. 012060.
15. Safaryan O. et al. Information system development for restricting access to software tool built on microservice architecture. *E3S Web of Conferences*. EDP Sciences, 2020. Vol. 224. P. 01041.
16. El Kholy M., El Fatatry A. Framework for interaction between databases and microservice architecture. *IT Professional*. 2019. Vol. 21. No. 5, pp. 57-63.
17. Mochalov V.P. et al. Methods and models of resource allocation service in load balancing clusters for data centers. 2022.
18. Mochalov V.P. et al. Infocommunication technologies. *Infocommunication technologies Founders: Volga State University of Telecommunications and Informatics, Academy of Telecommunications and Informatics*. 2021. Vol. 19. No. 2, pp. 163-172.
19. Buranova M.A., Kartashevsky V.G., Muthanna A.S. Analysis of the parameters of the functioning of a software-configurable network based on the OpenFlow protocol. *Telecommunications*. 2022. No. 4, pp. 2-7. DOI 10.34832/ELSV.2022.29.4.001.
20. Stepanov S.N. Stepanov J. Ndayikunda et al. The Increasing of Resource Sharing Efficiency in Network Slicing Implementation. *Communications in Computer and Information Science*. 2022. Vol. 1552, pp. 18-35. DOI 10.1007/978-3-030-97110-6_2.
21. Vilalta R. et al. GRPC-based SDN control and telemetry for soft-failure detection of spectral/spacial superchannels. *45th European Conference on Optical Communication (ECOC 2019)*. IET, 2019, pp. 1-4.

INFORMATION ABOUT AUTHORS:

Igor G. Buzhin, PhD, Associate Professor of the Department "Fixed-line networks and Systems", Moscow Technical University of Communications and Informatics, Moscow, Russia

Aleksey Yu. Derevyankin, Student, Moscow Technical University of Communications and Informatics, Moscow, Russia

Veronika M. Antonova, PhD, docent, Head of the Department "Fixed-line networks and Systems", Moscow Technical University of Communications and Informatics, Moscow, Russia

Aleksey P. Perevalov, graduate student, Moscow Technical University of Communications and Informatics, Moscow, Russia

Yuriy B. Mironov, PhD, Dean of the Faculty of "Networks and Communication Systems", Moscow Technical University of Communications and Informatics, Moscow, Russia

For citation: Buzhin I.G., Derevyankin A. Yu., Antonova V.M., Perevalov A.P., Mironov Yu.B. The effectiveness of frameworks for transmitting information in a virtualized communication network with a microservice architecture. H&ES Reserch. 2023. Vol. 15. No 2. P. 23-32. doi: 10.36724/2409-5419-2023-15-2-23-32 (In Rus)

ORGANIZERS:

IRIS ASSOCIATION (INSTITUTE OF RADIO AND INFORMATION SYSTEMS, VIENNA, AUSTRIA)
RUSSIA SECTION TEM/GRS/ITSS JOINT CHAPTER

INTERNATIONAL CONFERENCE

**«2023 International Conference «Engineering
Management of Communication and Technology»
(EMCTECH)**

IEEE Conference

16 – 18 October 2023, Vienna, Austria

Conference will produce a publication.

All accepted and presented Papers following the conference will be submitted for inclusion into IEEE Xplore and will be submitted also for indexing in Scopus and Web of Science data bases

The papers which are discussed at the conference can be divided into the following chapters:

CHAPTER 1. TECHNOLOGY ADVANCEMENTS IN IOT DEVICES & ARTIFICIAL INTELLIGENCE

CHAPTER 2. TRANSPORT AND COLLECTIVE SYSTEMS: SMART CONTROL TECHNOLOGY IN TRANSPORTATION, BIOMEDICAL, FARMING AND CYBER PHYSICAL SYSTEMS (new opportunities using technology in biomedical, farming, transportation, and cyber physical systems)

CHAPTER 3. BROADCAST TECHNOLOGIES ADVANCEMENTS – RADIO, IP, CELLULAR, ON DEMAND, INTERACTIVE

CHAPTER 4. TECHNOLOGY ADVANCEMENTS IN WIRE AND OPTICAL COMMUNICATION AND CONTROL SYSTEMS

CHAPTER 5. DIGITALIZATION PROCESS AND SECURITY MANAGEMENT IN DIGITAL SOCIETY AND INDUSTRY 4.0

CHAPTER 6. DIGITAL TRANSFORMATION AND DATA RISK MANAGEMENT IN ICT/TELECOMMUNICATION

CHAPTER 7. DEVELOPING PERSONAL SKILLS FOR LEADING INNOVATION INITIATIVES

CHAPTER 8. ENGINEERING TECHNOLOGY LEADING TO SOCIAL, POLITICAL AND ECONOMICAL CHANGE

Materials are available in English

<http://media-publisher.eu/conference-emctech/call-for-papers/>



doi: 10.36724/2409-5419-2023-15-2-33-40

СРАВНЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ АЛГОРИТМОВ КЛАССИФИКАЦИИ В РАМКАХ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

УЙМИН

Антон Григорьевич¹

НИКИТИН

Олег Рафаилович²

Сведения об авторах:

¹ Старший преподаватель кафедры кафедры безопасности информационных технологий ФГАОУ ВО "РГУ нефти и газа (НИУ) имени И.М. Губкина", Москва, Россия
 Область научных интересов: информационная безопасность; мониторинг информационных ресурсов; сбор и обработка информации

² Д.т.н., профессор, заведующий кафедрой радиотехники и радиосистем. Владимирский Государственный Университет имени Александра Григорьевича и Николая Григорьевича Столетовых (ВлГУ), г. Владимир, Россия.
 Область научных интересов: информационная безопасность; мониторинг информационных ресурсов; сбор и обработка информации

АННОТАЦИЯ

Введение: Аутентификация пользователя в настоящее время является стандартной процедурой для доступа к корпоративной или общедоступной сетевой инфраструктуре. Преимуществом биометрической аутентификации является уникальная и однозначная идентификация личности в системе. **Методы:** Для мониторинга поведения пользователей использовались контролируемые методы машинного обучения, позволяющие идентифицировать законных пользователей. После тестирования всех пользователей, использующих классификаторы, уровень проверки был достигнут на уровне 98%. **Результаты** могут быть использованы в корпоративных проектах и организации конкурсов. Работа ведется в рамках платформы RemoteTopology. На открытой веб-странице пользователь открывает несколько сеансов протоколов RDP, VNC, Telnet, SSH. Данные сеанса собираются расширением браузера и передаются в базу данных. На втором этапе был проведен эксперимент по обучению и тестированию каждого пользователя с использованием определенных выше классификаторов. Если характеристики, которые пользователь демонстрирует в текущий момент времени, совпадают с теми, которые были выявлены при обучении модели, пользователь продолжает работу, в противном случае система блокирует работу пользователя и требует повторной аутентификации. Модель должна обеспечивать постоянное определение пользовательских характеристик на основе динамики мыши. Характеристики собираются и упаковываются на стороне клиента в расширение браузера, затем передаются на сервер и сохраняются в базе данных. После этого каждому надежному действию присваивается значение, а единственный блок работы не является единственным пользователем. Единый блок не является незаконным или незаконным пользователем для блокировки работы. Также можно отметить, что для сценариев 1, 2 и 3 с использованием кривой FAR, FRR, EER и ROC: сценарий 1 имел самые низкие значения EER: RF EER: 0,010%.

КЛЮЧЕВЫЕ СЛОВА: *пользователь, данные, обучения, аутентификация, легитимный.*

Для цитирования: Уймин А.Г., Никитин О.Р. Сравнение производительности алгоритмов классификации в рамках сетевой инфраструктуры // Научные технологии в космических исследованиях Земли. 2023. Т. 15. № 2. С. 33-40. doi: 10.36724/2409-5419-2023-15-2-33-40

Введение

Аутентификация пользователей является, в настоящее время стандартной процедурой при доступе в сетевую инфраструктуру предприятия или открытого доступа [1]. Аутентификация делится на три класса: на основе знания какого-либо разделяемого секрета, на основе обладания каким-либо уникальным объектом (токеном) и на основе биометрии индивида. Аутентификация на основе знаний характеризуется степенью конфиденциальности информации, и может быть легко скомпрометирована. Аутентификация на основе обладания объектом характеризуется контролем за объектом и может подвергнуться хищению или копированию. Аутентификация на основе биометрии зависит от физиологических и или поведенческих характеристик индивида, т.е. являются его неотъемлемой частью.

Достоинством биометрической аутентификации является уникальная однозначная идентификация индивида в системе. В нашей работе будет рассматриваться только поведенческая биометрия, в виду возможности посредством нее организации непрерывной аутентификации пользователя в системе, на протяжении всего сеанса работы [2-4]. В настоящее время получили большое распространение корпоративные порталы, на основе web-технологий. В рамках проекта RemoteTopology [5-6] реализованы основные компоненты корпоративного портала по администрированию сетевой инфраструктуры. Разработано браузерное расширение, обеспечивающее сбор данных на стороне пользователя.

В данной работе основной задачей становится определение производительности алгоритмов машинного обучения в зависимости от временных интервалов сбора данных для идентификации пользователя и анализ областей окна браузера, с которыми работает пользователь для его идентификации и аутентификации на основе данных манипулятора типа мышь, при заданном уровне ошибки.

Обзор литературы

Ниже приведен обзор литературы, в котором рассматриваются аналогичные задачи, в том числе определение модели движения манипулятора, для идентификации и аутентификации пользователя. В соответствии с нашей целью, мы изучили несколько исследовательских работ для того, чтобы найти модель движения мыши и идентифицировать подлинных пользователей.

В работе [7] авторы предлагают новую одномерную сверхточную архитектуру использованием двух наборов данных. Они оценили модель, используя три сценария: (i) ПРОСТЫЕ модели, обученные с нуля с использованием обучающих данных из набора данных Balabit; (ii) модели TRANSFER1, использующие обучение передаче, где модели были предварительно обучены на наборе данных DFL; и (iii) Модели TRANSFER2, которые были получены с помощью обучения передаче, а затем веса были сформированы с использованием обучающих данных из набора данных Balabit. Результаты для количества блоков (300): PLAIN = 0,63, TRANSFER1 = 0,50 и TRANSFER2 = 0,66.

Это были результаты для количества блоков (всех): PLAIN = 0,55, TRANSFER1 = 0,34 и TRANSFER2 = 0,62. В этом исследовании использовался общедоступный набор данных Balabit; он содержит данные мыши только от 10 пользователей, которых может быть недостаточно для создания надежной и безопасной модели пользователя, основанной на динамике мыши.

В работе [8] авторы предложили систему эмпирического биометрического исследования для идентификации пользователей с использованием различных нейронных сетей в онлайн-игре League of Legends. Результаты их экспериментов показали, как различные нейронные сети ведут себя с биометрическими данными и базами данных League of Legends. RBF и байесовские сети показали, что можно улучшить результаты, собирая образцы с большей частотой, несмотря на стоимость обработки.

В заключении авторы заявляют, что в будущей работе можно использовать стратегию, в которой анализируются различия между выборками ранней игры, середины игры и поздней игры; этот подход рассматривает профиль пользователя на каждом уровне, поскольку один и тот же игрок проводит игру от начала до конца. Объем собранных данных был недостаточным, чтобы позволить экспериментам более точно проверить, не атакует ли пользователь сам в рамках совместного использования учетных записей.

В работе [9] авторы предложили схему аутентификации пользователя, основанную на динамике мыши. Они собрали данные о поведении мыши у 48 пользователей и применили нечеткую классификацию, основанную на алгоритме обучения для многомерного анализа данных. Они провели оценку и достигли уровня ложного принятия (FAR) 0% и уровня ложного отклонения (FRR) 0,36%. Для их экспериментов требовалось более 2000 событий мыши, чтобы классифицировать пользователя как законного.

В работе [10] авторы представили структуру для проверки пользователей с использованием действий мыши. Структура была разделена на три части: получение, обучение и проверка. Первым шагом является захват действий пользователя из действий мыши пользователей. Затем классифицируется каждый тип событий и сохраняется их в базе данных. На третьем этапе заключается в отправке каждого события в избранный классификатор на основе типа действия. Классификатор имеет два уровня: уровень прогнозирования и уровень принятия решений. Исследователи провели тесты многоклассового классификатора с использованием RF-классификатора. Авторы собрали данные у 25 добровольцев. Они получили одинаковую частоту ошибок (EER) в 1,01% на основе 30 событий.

В работе [11] авторы рассматривают форму поведенческой биометрии, основанную на динамике мыши, которую можно использовать в различных приложениях безопасности. Разработан способ моделирования поведенческих характеристик на основе данных, захваченных искусственными нейронными сетями. Помимо этого, авторы представляют дизайн и реализацию детектора, который охватывает все этапы потоков биометрических данных. Они провели эксперимент, в котором приняли участие 5000 человек, и обнаружили FAR 2.4649% и FRR 2.4614%.



В планах у них расширить размер факторов пользователя и мыши для достижения более высокой производительности

В работе [12] авторы проверяют гипотезу о способе идентификации людей с помощью статистики, рассчитанной для комбинации записанных положений мыши и взгляда. Показанный им подход и эксперименты в этих исследованиях дали некоторые основания полагать, что разработка такого решения возможна. Снятие метрики динамики мыши и взгляда отличается дизайном, методом извлечения признаков. Результаты показывают, что он может быть использован как для авторизации (средний EER 11,2%, F1-score 90,6%, лучший результат EER 4%, лучший F1-score 99%), так и для идентификации некоторого числа пользователей (средний EER 18%, точность 53%, лучшая точность 96%).

Поэтому данный анализ показал, что применение поведенческой биометрической идентификации как единственного механизма безопасности в настоящее время практически невозможно и требует дальнейшего совершенствования. Анализ показал, что последующие шаги исследования включают: поиск других особенностей идентификации и оптимизацию метода для отдельных участников; а также проверку других сценариев эксперимента, которые запланированы как будущая работа.

В работе [13] авторы демонстрируют, что модель CNNs для биометрической аутентификации на основе динамики нажатия клавиш может значительно повысить надежность паролей против атак грубой силы. Заблокировать вход 100% нелегальных пользователей можно даже если пароль пользователя был украден. Если обучающие данные используются для обучения паролей подозреваемых пользователей, то аккаунт легального человека будет надежно защищен от взлома. Гарантированно! Большинство легальных пользователей имеют 13% FRR. Любой человек может повторно ввести пароль, если его/ее заблокировали для входа в систему.

Кроме того, в случае изменения структуры обучающих данных так чтобы модель CNN была менее чувствительной к отбрасыванию легальных пользователей и FRP нелегалов улучшились до 6%. Точность идентификации модели CNN увеличилась почти на 97%. Также они рассмотрели более реалистичный сценарий, в котором данные об использовании клавиш пароля большинства нелегальных пользователей были исключены из обучения. По мнению CNN, модель безопасности по-прежнему может защитить 72% нелегальных пользователей, а точность идентификации CNN модели составляет 80%. Таким образом, понимая важность требований к производительности вычислений при большом объеме данных и количестве тренировок, авторы объединили параллельные вычисления на GPU в нашей CNN-модели и получили ускорение примерно в 4,45 раза. Это делает предложенный подход очень практичным и осуществимым.

В работе [14] авторы описывают способ выработать параметры для снятия данных с компьютерной мыши, рассматривают требования для создания DataSet, определяют эффективность анализа и извлечения основных признаков из необработанных данных. Рассмотрены модели DL для CA и AD, позволяющие верифицировать пользователя, произвести их качественное сравнение. В результате работы определено, что существующие методы, связанные с CA и AD описывают

в основном лабораторные исследования, и носят характер подтверждения гипотез. В рассмотренных исследованиях описаны использованные параметры, по разработке программного обеспечения для снятия данных о действиях мыши. Исследования показывают, что инструменты сбора незначительно влияют на качество получаемых данных, при условии предобработки данных с использованием алгоритмов выделения ключевых признаков.

Большинство исследований рассматривает наборы данных полученных, либо из свободных источников, либо из групп добровольцев в диапазоне от 10 до 60 человек. Необходимо отметить, что количество, превышающее 10 можно считать достаточным для определения репрезентативной выборки. Определено, что наибольшее значение на результат дали признаки, описывающие перемещение мыши между двумя местоположениями экрана. Рассмотрены модели DL для CA и AD, позволяющих верифицировать пользователя, произведено их качественное сравнение. Практическая значимость: проведенное исследование позволяет судить о возможности реализации решения по непрерывной онлайн-аутентификации и систем обнаружения аномалий для постоянного подтверждения личности пользователя в рамках разработанной ранее системы проведения дистанционных чемпионатов RemoteTopology.

В работе [15] авторы представили первый сравнительный анализ NuMldb, новой общедоступной базы данных с более 5 ГБ различных мобильных данных, собранных по неконтролируемому сценарию. При этом для каждой модальности была разработана своя LSTM RNN с тройной потерей. По словам авторов исследования они показали, что наиболее эффективным источником являются фиксированные текстовые данные о нажатии клавиш для сенсорного экрана и магнитометра с датчиками фонового излучения. Однако сила различения системы значительно повышается при синтезе, обычно достигая диапазона 4-9% EER в течение примерно 3 с взаимодействия.

Постановка задачи

Биометрическая система позволит с высоким процентом достоверности определить подмену пользователя. Таким образом есть возможность выделить легитимного и не легитимного пользователя на основе данных, полученных при работе с манипулятором [16]. В нашем исследовании для мониторинга поведения пользователей использовались контролируемые методы машинного обучения для возможности выделения легитимных пользователи [17].

В качестве источника данных нами используются данные, полученные в рамках обучения студентов ВУЗ по дисциплине «Сети и системы передачи информации» возрастная категория 18-24 года гендерное соотношение 60% муж. 40% жен. А также Чемпионата по «Информационной безопасности», проходившего в рамках международного чемпионата BRICS Future Skills Challenge 2022 в рамках дистанционной работы участников из 8 стран. Возрастная категория 18-37 года гендерное соотношение 92% муж. 8% жен. Для обеспечения высокой точности метода, необходимо обрабатывать большое количество параметров манипулятора [18].

При этом проблемой будет являться получаемый пользователем опыт. Пользователь систематически улучшает навыки работы с мышью, повышая/изменяя скорость движения и скорость перемещения манипулятора и т.д.

Модель должна обеспечивать постоянное определение характеристик пользователя на основе динамики работы мыши. Характеристики собираются и упаковываются на стороне клиента в браузерном расширении, затем передаются на сервер и хранятся в базе данных. Если характеристики, которые пользователь демонстрирует в текущий момент времени совпадают с теми, которые были выделены при обучении модели пользователь продолжает работу, в противном случае система блокирует работу пользователя и требует повторной аутентификации. Работа модели описывается схемой на рисунке 1.



Рис. 1. Схема работы системы

1 Этап сбора. На данном этапе собираются данные пользователя. Сбор данных осуществляется расширением браузера в пределах окна браузера. Данные сеанса каждого сеанса обрабатываются расширением браузера. Расширение собирает информацию о движениях мыши по осям X, Y, а также о том на каком url находится пользователь, собирает эти данные в стандартном объекте JavaScript, затем раз в 4 секунды происходит отправка данных в формате JSON на удаленный сервер. Данные хранятся на сервере. Данные записываются в СУБД PostgreSQL. После получения сервером достаточного количества данных, о определенном пользователе, происходит их обработка, а именно вычисление скорости, ускорения и преобразования url в категориальный атрибут, затем данные записываются в новую таблицу (которая создается индивидуально по id пользователя).

2 Фаза извлечения признаков.

Собранные данные, средствами расширения браузера подвергаются обработке, из них мы выделяем шесть основных признаков для формирования набора данных:

- Метка времени: определяется временем с начала сеанса, запись браузерным расширением.
- Статус кнопки: статус кнопки мыши, применяется условие нажатия левой кнопки мыши, правой кнопки мыши, колеса мыши. В настоящий момент не учитывается скорость прокрутки колеса.
- Состояние кнопки мыши: определяется дополнительным атрибутом, таким как нажатие, отпускание, зажатие клавиши.
- Ось X: координата X курсора на экране.

- Ось Y: координата Y курсора на экране.
- Положение области XY: мы определяем экран браузера как полотно, состоящее из 4 областей. Каждая выделенная область рассматривается как отдельное прямоугольное полотно. Для определения областей в рамках окна применяется объект window [19]. Пример показан на рисунке 2.

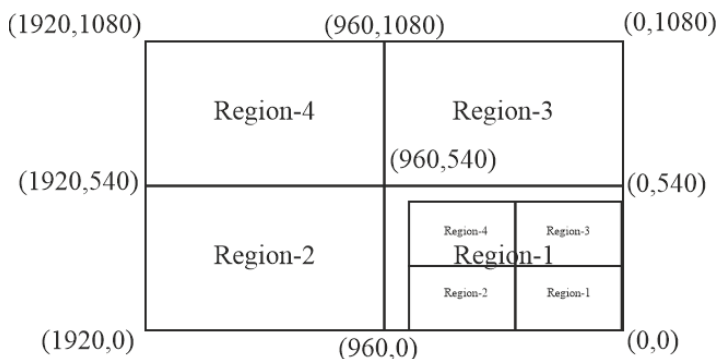


Рис. 2. Области экрана

3 Этап подготовки данных: на этапе обучения все данные пользователей сгруппированы в блоки в рамках серверной части инфраструктуры. После этого Данные были разбиты на две категории. первая категория (80% данных) использовалась для обучения, а вторая категория (20% данных) использовалась для тестирования производительности модели. Для каждого эксперимента процент обучающих и оценочных наборов оставался неизменным, чтобы избежать смещения классификатора.

В дальнейшем данное разделение должно учитываться при непрерывной онлайн аутентификации, т.е. модель замещает старые учебный данные от вновь полученные, прогрессируя в след за пользователем в владении пользователем мышью. Выбор фазы классификатора подробно описан в работе [14], что позволяет определить легитимен ли доступ пользователя в системе. Нами применяются пять алгоритмов классификаций: Random Forest, Decision Tree, KNN, Naïve Bayes and Principal Component Analysis (PCA).

Эффективность методов определяется с использованием трех общих показателей: частота ложного принятия (FAR), частота ложного отклонения (FRR) и равная частота ошибок (EER). FRR – это вероятность того, что легитимный пользователь, не сможет получить доступ к системе. EER – это пороговое значение между частотой ложного принятия и частотой ложного отклонения пользователя. Необходимо получить классификатор со структурой его кривых рабочих характеристик приемника (ROC) так как они определяют успешность прогнозирования модели в рабочих точках возможных пороговых значений. Кривая ROC отображает истинную положительную скорость (TPR) в сравнении с ложноположительной скоростью (FPR).

Для целей оценки производительности использовались следующие выражения: TP: истинно положительный, TN: истинно отрицательный, FP: ложноположительный, FN: ложноотрицательный, FAR: коэффициент ложного принятия, FRR: коэффициент ложного отклонения и EER: равная частота ошибок:



$$ACC = \frac{TP + TN}{TP + TN + FP + FN}$$

$$TPR = \frac{TP}{TP + FN}$$

$$TNR = \frac{TN}{TN + FP}$$

$$FPR = \frac{FP}{FP + FN}$$

$$FNR = \frac{FN}{FN + TP}$$

$$FAR = \frac{\text{Number of accepted imposters}}{\text{Total number of imposters}}$$

$$FRR = \frac{\text{Number of rejected genuines}}{\text{Total number of genuines}}$$

$$EER = \frac{FAR + FRR}{2}$$

Нами применяются пять алгоритмов классификаций: Random Forest, Decision Tree, KNN, Naïve Bayes and Principal Component Analysis (PCA). Перед классификацией данные делятся на обучающие и тестовые. 80% данных используются для обучения модели. 20% данных для в качестве тестовых данных. Выборка данных производится случайным образом. Обработка данных данных пяти сессий по 15 секунд и пяти сессий по пять секунд, что позволяет получить баланс между объемом данных и скоростью выявления неавторизованного пользователя. Данные временные интервалы подобраны эмпирическим путем в ходе эксперимента.

4. Этап обучения: процесс обучения начнётся со считывания характеристик всех пользователей из обучающего набора данных и последующей загрузки их классификаторы для обучения модели. Этот шаг определяет паттерн поведения пользователя.

5. Этап тестирования данных: после завершения этапа обучения модель была протестирована на новых данных, которые никогда не использовались для обучения, чтобы определить, является ли пользователь подлинным пользователем или самозванцем.

Эксперимент и анализ результатов

Эксперимент проводился в два этапа: этап проверки и этап аутентификации. Этап проверки: на данном этапе все классификаторы сначала обучаются с использованием данных, которые содержат только подлинные действия легитимного пользователя. Работа ведется в рамках платформы RemoteTopology. В рамках открытой web страницы пользователь открывает несколько сеансов протоколов RDP, VNC, Telnet, SSH. Данные о сеансах собираются расширением браузера и передаются в базу данных. На втором этапе был проведен эксперимент путем обучения и тестирования для

каждого пользователя с использованием классификаторов, определенных выше. Целью этапа проверки было проверить, связаны ли данные мыши с данным пользователем. После тестирования всех пользователей с использованием классификаторов был достигнут показатель 98% проверки. Этап аутентификации: на этом этапе каждый пользователи разделяются на два блока: легитимные пользователи и не легитимные пользователи. Действия нелегитимных пользователей подменяют работы легитимных пользователей в системе, путем смены участников за рабочим местом. После чего каждому достоверному действию присваивается единичное значение, а не достоверному нулевое. Классификаторы отвечают за определение вероятности того, что пользователь принадлежит к блоку легитимных или не легитимных пользователей. Результаты работы в сценариях.

Таблица 1

Оценка СА — Сценарий 1 (Действия с учетом движений мыши): FAR, FRR и EER

| Классификатор | KNN | DT | RF | CNN |
|---------------|-------|-------|-------|-------|
| FAR | 0,014 | 0,016 | 0,010 | 0,046 |
| FRR | 0,196 | 0,64 | 0,072 | 0,965 |
| ERR | 0,105 | 0,328 | 0,041 | 0,506 |

Таблица 2

Оценка СА – Сценарий 2: (Действия с учетом движений мыши и однократных нажатий): FAR, FRR и EER

| Классификатор | KNN | DT | RF | CNN |
|---------------|-------|-------|-------|-------|
| FAR | 0,032 | 0,016 | 0,011 | 0,048 |
| FRR | 0,475 | 0,256 | 0,143 | 0,869 |
| ERR | 0,254 | 0,136 | 0,077 | 0,459 |

Таблица 3

Оценка СА – Сценарий 3: (Действия с учетом движений мыши и многократных нажатий): FAR, FRR и EER

| Классификатор | KNN | DT | RF | CNN |
|---------------|-------|-------|-------|-------|
| FAR | 0,028 | 0,306 | 0,031 | 0,054 |
| FRR | 0,786 | 0,488 | 0,563 | 0,974 |
| ERR | 0,407 | 0,397 | 0,297 | 0,514 |

Данные эксперименты позволили сформировать нагрузку для системы. Это позволило сравнить производительность алгоритмов в рамках предложенной модели. Выбранные нами 20% (экспериментальные данные) были обработаны в рамках модели классификации и позволили сравнить точность работы алгоритмов.

Таблица 4

Процент региона для каждого пользователя

| User | 5 сессий по 15 секунд | | | | 5 сессий по 5 секунд | | | |
|---------|-----------------------|-------|-------|-------|----------------------|-------|-------|-------|
| | R-1 | R-2 | R-3 | R-4 | R-1 | R-2 | R-3 | R-4 |
| User-1 | 56,01 | 0,86 | 41,99 | 6,91 | 57,43 | 4,42 | 47,02 | 5,37 |
| User-2 | 62,98 | 5,18 | 13,47 | 1,41 | 60,17 | 3,50 | 17,56 | 3,86 |
| User-3 | 60,39 | 2,04 | 18,95 | 2,28 | 62,28 | 5,18 | 38,70 | 6,88 |
| User-4 | 71,65 | 7,50 | 39,31 | 3,56 | 69,91 | 1,06 | 30,69 | 10,64 |
| User-5 | 98,80 | 4,85 | 20,46 | 2,82 | 85,92 | 2,36 | 48,82 | 10,43 |
| User-6 | 69,64 | 0,32 | 16,69 | 1,88 | 52,09 | 5,48 | 30,36 | 0,30 |
| User-7 | 90,02 | 6,02 | 43,75 | 7,92 | 99,39 | 7,67 | 28,46 | 4,66 |
| User-8 | 81,80 | 1,22 | 34,47 | 10,70 | 91,78 | 5,30 | 10,74 | 0,70 |
| User-9 | 70,90 | 9,30 | 19,54 | 4,13 | 82,99 | 3,15 | 35,25 | 1,98 |
| User-10 | 87,89 | 0,08 | 11,32 | 4,38 | 67,10 | 9,91 | 29,27 | 7,96 |
| User-11 | 84,19 | 8,88 | 12,13 | 10,20 | 61,16 | 9,26 | 20,39 | 6,17 |
| User-12 | 68,33 | 6,97 | 34,04 | 0,06 | 90,92 | 9,97 | 26,78 | 9,04 |
| User-13 | 99,22 | 0,51 | 17,91 | 2,50 | 72,18 | 8,14 | 18,69 | 4,01 |
| User-14 | 50,16 | 2,97 | 25,18 | 8,22 | 90,04 | 1,98 | 30,61 | 2,12 |
| User-15 | 70,57 | 8,20 | 15,88 | 7,70 | 57,99 | 5,39 | 14,64 | 9,86 |
| User-16 | 77,82 | 1,17 | 10,11 | 5,16 | 93,04 | 1,57 | 49,14 | 9,56 |
| User-17 | 59,95 | 3,40 | 26,66 | 2,73 | 97,63 | 8,32 | 29,18 | 1,74 |
| User-18 | 88,09 | 7,08 | 11,87 | 2,59 | 93,18 | 1,81 | 36,37 | 4,72 |
| User-19 | 51,78 | 10,69 | 17,94 | 10,77 | 63,38 | 8,50 | 11,77 | 6,01 |
| User-20 | 66,39 | 3,50 | 11,90 | 2,53 | 61,71 | 7,44 | 12,04 | 5,83 |
| User-21 | 71,21 | 10,25 | 40,24 | 2,76 | 86,55 | 2,14 | 20,81 | 0,13 |
| User-22 | 65,99 | 1,32 | 43,39 | 10,85 | 71,51 | 8,10 | 34,38 | 3,17 |
| User-23 | 56,33 | 9,98 | 33,52 | 1,91 | 51,55 | 1,96 | 49,88 | 4,87 |
| User-24 | 84,31 | 2,31 | 15,80 | 3,61 | 82,14 | 3,16 | 17,35 | 9,69 |
| User-25 | 96,67 | 8,60 | 23,64 | 10,64 | 84,29 | 1,58 | 34,18 | 8,44 |
| User-26 | 58,28 | 8,02 | 15,02 | 2,26 | 83,30 | 10,03 | 28,42 | 1,06 |
| User-27 | 63,57 | 7,58 | 33,34 | 6,79 | 70,47 | 6,78 | 10,51 | 3,37 |
| User-28 | 66,30 | 10,68 | 34,55 | 6,34 | 67,05 | 10,90 | 26,73 | 10,89 |
| User-29 | 95,01 | 1,32 | 26,50 | 2,06 | 60,25 | 2,32 | 28,20 | 8,28 |
| User-30 | 77,53 | 10,99 | 48,10 | 3,20 | 80,21 | 2,49 | 44,87 | 5,12 |

На основе этих данных можно построить гистограмму (рис. 3), позволяющую определить какой регион наиболее часто использует пользователь.

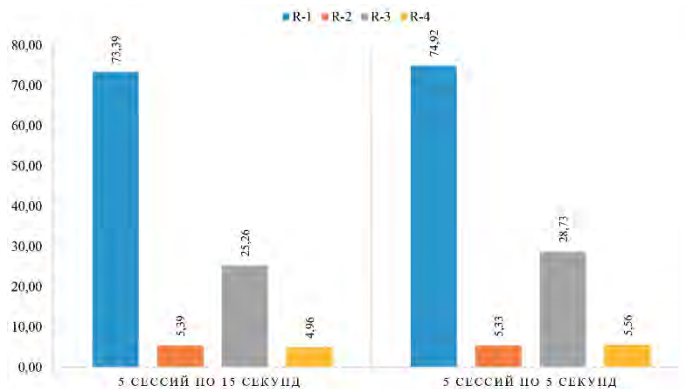


Рис. 3. Средний процент использования региона пользователями

Ниже приведено сравнение с аналогичными исследованиями других ученых, рассматриваемых нами методов (табл. 5).

Таблица 5

| Автор со ссылкой | Результаты исследований других авторов | Средний результат нашего исследования |
|---|--|---------------------------------------|
| | ERR | ERR |
| A. E. Ahmed, I. Traore [10] | 1,01 | 0,0215 |
| Kasprowski, Pawel & Harezlak, Katarzyna [12] авторизация | 11,2 | |
| Kasprowski, Pawel & Harezlak, Katarzyna [12] идентификация | 18 | |
| Giuseppe Stragapede, Ruben Vera-Rodriguez, Ruben Tolosana, Aythami Morales, Alejandro Acien, Gaël Le Lan [15] | 4-9% | |

Результаты исследования и выводы

В ходе проведенного обзора источников и проведенного эксперимента можно выделить преимущества random forest над другими четырьмя алгоритмами в сессиях 10 секунд, что позволяет применять его в рамках проектов корпоративного обучения и организации соревнований. Так же можно отметить, что для сценариев 1, 2 и 3 с использованием FAR, FRR, EER и кривой ROC: сценарий 1 имел самые низкие значения EER: KNN EER: 0,014%, DT EER: 0,016%, RF EER: 0,010% и CNN EER: 0,046% по сравнению со сценариями 2 и 3. Результаты по всем сценариям представлены в таблицах 1-3. Можно отметить, что совместное применение данных технологий позволит получить высокую скорость работы решения при малой доле ошибок.



Литература

1. *Pisani P.H.* et al. Adaptive biometric systems: Review and perspectives // ACM Computing Surveys (CSUR). 2019. Т. 52. №.5. С. 1-38.
2. *Chong P., Elovici Y., Binder A.* User authentication based on mouse dynamics using deep neural networks: A comprehensive study // IEEE Transactions on Information Forensics and Security. 2019. Т. 15. С. 1086-1101.
3. *Siddiqui N., Pryor L., Dave R.* User authentication schemes using machine learning methods – a review // Proceedings of International Conference on Communication and Computational Technologies. Springer, Singapore, 2021. С. 703-723.
4. *Antal M., Egyed-Zsigmond E.* Intrusion detection using mouse dynamics // IET Biometrics. 2019. Т. 8. №. 5. С. 285-294.
5. Свидетельство о государственной регистрации программы для ЭВМ № 2021619990 Российская Федерация. RemoteTopology-модуль авторизации: № 2021613424; заявл. 09.03.2021; опубл. 21.06.2021 / А. Г. Уймин, С. В. Любкин.
6. *Уймин А.Г.* Интеллектуальный анализ динамики трехпозиционного графического манипулятора типа "мышь" как элемента поведенческой биометрии // Системы управления и информационные технологии. 2022. № 2(88). С. 92-96. DOI 10.36622/VSTU.2022.88.2.018.
7. *Antal M., Egyed-Zsigmond E.* Intrusion detection using mouse dynamics. IET Biom. 2019, 8, pp. 285-294.
8. *da Silva V.R.; Costa-Abreu M.D.* An empirical biometric-based study for user identification with different neural networks in the online game League of Legends. In Proceedings of the 2018 International Joint Conference on Neural Networks (IJCNN), Rio de Janeiro, Brazil, 8-13 July 2018; pp. 1-6.
9. *Nakkabi Y., Traoré I., Ahmed A.A.E.* Improving mouse dynamics biometric performance using variance reduction via extractors with separate features. IEEE Trans. Syst. Man Cybern. Part A: Syst. Hum. 40(6), pp. 1345-1353.
10. *Ahmed A.E., Traore I.* A New Biometric Technology Based on Mouse Dynamics // IEEE transactions on Dependable and Secure Computing, vol. 4, no. 3, pp. 165-179, July-Sept. 2007.
11. *Awad A., Liu Y.* Cognitive biometrics for user authentication // Biometric-Based Physical and Cybersecurity Systems. Springer, Cham, 2019. С. 387-399.
12. *Kasprowski Pawel, Harezlak Katarzyna.* Biometric Identification Using Gaze and Mouse Dynamics During Game Playing: 14th International Conference, BDAS 2018, Held at the 24th IFIP World Computer Congress, WCC 2018, Poznan, Poland, September 18-20, 2018, Proceedings. 10.1007/978-3-319-99987-6_38.
13. *Lin C.H., Liu J.C., Lee K.Y.* On neural networks for biometric authentication based on keystroke dynamics // Sensors and materials. 2018. Т. 30. №. 3. С. 385-396.
14. *Уймин А.Г., Морозов И.М.* Сравнительный анализ инструментов непрерывной онлайн-аутентификации и систем обнаружения аномалий для постоянного подтверждения личности пользователя // Т-Comm: Телекоммуникации и транспорт. 2022. Т. 16. № 5. С. 48-55. DOI 10.36724/2072-8735-2022-16-5-48-55
15. *Giuseppe Stragapede, Ruben Vera-Rodriguez, Ruben Tolosana, Aythami Morales, Alejandro Acien, Gaël Le Lan.* Mobile behavioral biometrics for passive authentication, Pattern Recognition Letters. Vol. 157, 2022, pp. 35-41, ISSN 0167-8655, <https://doi.org/10.1016/j.patrec.2022.03.014>.
16. *Уймин А.Г.* Эмпирическая оценка методов машинного обучения в задачах онлайн-аутентификации // Вестник компьютерных и информационных технологий. 2022. Т. 19. № 8(218). С. 49-57. DOI 10.14489/vkit.2022.08, pp. 049-057.
17. *Almalki S., Chatterjee P., Roy K.* Continuous authentication using mouse clickstream data analysis // International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage. Springer, Cham, 2019. С. 76-85.
18. *Lu X., Feng Z., Xia J.* An Efficient Man-Machine Recognition Method Based On Mouse Trajectory Feature De-redundancy // Annual Computer Security Applications Conference. 2021. С. 365-374.
19. Описание объекта window // MDN web docs URL: <https://developer.mozilla.org/ru/docs/Web/API/Window>.

COMPARISON OF CLASSIFICATION ALGORITHMS PERFORMANCE WITHIN NETWORK INFRASTRUCTURE

ANTON G. UIMIN

St. Petersburg, Russia

OLEG R. NIKITIN

St. Petersburg, Russia

ABSTRACT

Introduction: User authentication is now a standard procedure for access to corporate or public network infrastructure. The advantage of biometric authentication is the unique and unambiguous identification of an individual in the system. Supervised machine learning techniques were used to monitor user behavior to identify legitimate users. After testing all users using the classifiers, the verification rate was achieved at 98%. **The results** can be used in corporate projects and organizing contests. The work is conducted within the RemoteTopology platform. On the open web page, the user opens several RDP protocol sessions. VNC, Telnet, SSH. Session data is collected by the browser extension and transmitted to the database. In the second stage, an experiment was

REFERENCES

1. Pisani P.H. et al. Adaptive biometric systems: Review and perspectives. *ACM Computing Surveys (CSUR)*. 2019. Vol. 52. No. 5, pp. 1-38.
2. Chong P., Elovici Y., Binder A. User authentication based on mouse dynamics using deep neural networks: A comprehensive study. *IEEE Transactions on Information Forensics and Security*. 2019. Vol. 15, pp. 1086-1101.
3. Siddiqui N., Pryor L., Dave R. User authentication schemes using machine learning methods-a review. *Proceedings of International Conference on Communication and Computational Technologies*. Springer, Singapore, 2021, pp. 703-723.
4. Antal M., Egyed-Zsigmond E. Intrusion detection using mouse dynamics. *IET Biometrics*. 2019. Vol. 8. No. 5, pp. 285-294.
5. Uimin A.G., Lyubkin S.V. Certificate of state registration of the computer program No. 2021619990 Russian Federation. RemoteTopology-Authorization Module : No. 2021613424 : App. 03/09/2021 : publ. 06/21/2021.
6. Uimin A.G. Intellectual analysis of the dynamics of a three-position graphic manipulator of the "mouse" type as an element of behavioral biometrics. *Control systems and information technologies*. 2022. No. 2(88), pp. 92-96. DOI 10.36622/VSTU.2022.88.2.018.7. Antal, M.; Egyed-Zsigmond, E. Intrusion detection using mouse dynamics. *IET Biom*. 2019, 8, pp. 285-294.
8. da Silva, V.R.; Costa-Abreu, M.D. An empirical biometric-based study for user identification with different neural networks in the online game League of Legends. *In Proceedings of the 2018 International Joint Conference on Neural Networks (IJCNN)*, Rio de Janeiro, Brazil, 8-13 July 2018, pp. 1-6.
9. Nakkabi Y., Traore I., Ahmed A.A.E. Improving mouse dynamics biometric performance using variance reduction via extractors with separate features. *IEEE Trans. Syst. Man Cybern. Part A: Syst. Hum.* 40(6), pp. 1345-1353.
10. Ahmed A.E., Traore I. A New Biometric Technology Based on Mouse Dynamics. *IEEE transactions on Dependable and Secure Computing*, vol. 4,

INFORMATION ABOUT AUTHORS:

Anton G. Uimin, Senior Lecturer of the Department of Information Technology Security Department of the Federal State Autonomous Educational Institution of Higher Education Russian State University of Oil and Gas (NRU) named after I.M. Gubkin, Research interests: information security; monitoring of information resources; collection and processing of information, Moscow, Russia

Oleg R. Nikitin, Doctor of Technical Sciences, Professor, Head of the Department of Radio Engineering and Radio Systems. Vladimir State University named after Alexander Grigorievich and Nikolai Grigorievich Stoletovs (VISU). Research interests: information security; monitoring of information resources; collection and processing of information, Vladimir, Russia

KEYWORDS: user, data, learning, authentication, legitimate.

conducted to train and test each user using the classifiers defined above. If the characteristics that the user exhibits at the current time match those identified by the model training, the user continues to work, otherwise the system locks the user and requires re-authentication. The model must provide constant detection of user characteristics based on mouse dynamics. Characteristics are collected and packaged on the client side in a browser extension, then transmitted to the server and stored in a database. Each reliable action is then assigned a value, and a single block of work is not a single user. A single block is not an illegal or illegal user to block work. It can also be noted that for scenarios 1, 2 and 3 using the FAR, FRR, EER and ROC curve: scenario 1 had the lowest EER values: RF EER: 0.010%.

no. 3, pp. 165-179, July-Sept. 2007.

11. Awad A., Liu Y. Cognitive biometrics for user authentication. *Biometric-Based Physical and Cybersecurity Systems*. Springer, Cham, 2019, pp. 387-399.

12. Kasprowski, Pawel & Harezlak, Katarzyna. (2018). Biometric Identification Using Gaze and Mouse Dynamics During Game Playing. *14th International Conference, BDAS 2018, Held at the 24th IFIP World Computer Congress, WCC 2018*, Poznan, Poland, September 18-20, 2018, Proceedings. 10.1007/978-3-319-99987-6_38.

13. Lin C. H., Liu J. C., Lee K. Y. On neural networks for biometric authentication based on keystroke dynamics. *Sensors and materials*. 2018. Vol. 30. No. 3, pp. 385-396.

14. Uimin A.G., Morozov I.M. Comparative analysis of continuous online authentication tools and anomaly detection systems for permanent confirmation of the user's identity. *T-Comm*. 2022. Vol. 16. No. 5. S. 48-55. DOI 10.36724/2072-8735-2022-16-5-48-55

15. Giuseppe Stragapede, Ruben Vera-Rodriguez, Ruben Tolosana, Aythami Morales, Alejandro Acien, Gael Le Lan, Mobile behavioral biometrics for passive authentication, *Pattern Recognition Letters*. Vol. 157, 2022, pp. 35-41, ISSN 0167-8655, <https://doi.org/10.1016/j.patrec.2022.03.014>.

16. Uimin A.G. Empirical evaluation of machine learning methods in online authentication problems. *Bulletin of computer and information technologies*. 2022. Vol. 19. No. 8(218), pp. 49-57. DOI 10.14489/vkit.2022.08.pp.049-057

17. Almalki S., Chatterjee P., Roy K. Continuous authentication using mouse clickstream data analysis. *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*. Springer, Cham, 2019, pp. 76-85.

18. Lu X., Feng Z., Xia J. An Efficient Man-Machine Recognition Method Based On Mouse Trajectory Feature De-redundancy. *Annual Computer Security Applications Conference*. 2021, pp. 365-374.

19. Description of the window object. MDN web docs URL: <https://developer.mozilla.org/ru/docs/Web/API/Window>



doi: 10.36724/2409-5419-2023-15-2-41-48

ИНТЕГРАЦИЯ СИСТЕМ БИЗНЕС-АНАЛИТИКИ С СИСТЕМАМИ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ НА ТРАНСПОРТЕ

МАРКЕВИЧ

Даниил Владимирович¹

ХАРЛАНОВА

Валерия Владиславовна²

ХОМОНЕНКО

Анатолий Дмитриевич³

АННОТАЦИЯ

Введение: в настоящее время большой практический интерес представляет решение различных транспортных задач с применением информационных технологий. Для работы с базами данных, содержащих в себе огромные массивы информации, их структуризации, тщательного анализа и принятия оптимальных решений, исследователи и аналитики активно используют различные системы, такие как системы управления базами данных (СУБД) или системы бизнес-аналитики. Несмотря на это, до сих пор не так широко применяется интеграция таких систем, способная повысить качество принимаемых решений. **Цель исследования:** состоит в отработке технологии интеграции между системой бизнес-аналитики и СУБД, позволяющей эффективно работать с огромным объемом данных при решении транспортных задач. **Методы и средства:** интеграция рассматриваемых систем реализована с помощью СУБД PostgreSQL 11 и аналитической платформы Loginom Community. Результаты: выполнен полный цикл интеграции систем, включающий в себя создание и заполнение базы данных в системе PostgreSQL 11, а также её подключение к аналитической платформе Loginom Community для структуризации данных, их анализа и дальнейшего принятия решений. **Практическая значимость:** главной отличительной чертой реализованной технологии является полная совместимость двух систем, изначально отвечающих за разные задачи: базы данных, располагающей обширной экосистемой доступных средств, и платформы, предоставляющей возможности глубокой аналитики для принятия оптимальных управленческих решений. Представлены причины и преимущества интеграции указанных систем, а также их применения при решении конкретных транспортных задач. **Обсуждение:** при решении задачи обеспечения интеграции рассмотрено практическое применение СУБД и системы бизнес-аналитики. С помощью PostgreSQL 11 сформированы две базы данных, которые интегрированы с аналитической платформой Loginom Community. Дальнейшие исследования целесообразно продолжить в направлениях практического использования интеграции для аналитики больших массивов баз данных, а также в интересах повышения качества принятия управленческих решений в транспортных задачах.

Сведения об авторах:

¹магистрант кафедры информационные и вычислительные системы Петербургского государственного университета путей сообщения Императора Александра I, г. Санкт-Петербург, Россия, dmarkevich811@mail.ru

²магистрант кафедры информационные и вычислительные системы Петербургского государственного университета путей сообщения Императора Александра I, г. Санкт-Петербург, Россия, lerya107@yandex.ru

³д.т.н., профессор, профессор кафедры информационные и вычислительные системы Петербургского государственного университета путей сообщения Императора Александра I, г. Санкт-Петербург, Россия, khomon@mail.ru

КЛЮЧЕВЫЕ СЛОВА: система бизнес-аналитики, система управления базами данных, интеграция инструментальных систем, PostgreSQL, Loginom Community, роль интеграции и цифровизации в железнодорожной области.

Для цитирования: Маркевич Д.В., Харланова В.В., Хомоненко А.Д. Интеграция систем бизнес-аналитики с системами управления базами данных на транспорте // Научные исследования в космических исследованиях Земли. 2023. Т. 15. № 2. С. 41-48. doi: 10.36724/2409-5419-2023-15-2-41-48

1. Введение

Одной из важнейших задач нашего времени является развитие транспортных технологий. Игнорировать информационные системы, не использовать их на транспорте (в частности, на железной дороге) – значит упускать возможность оптимизировать ресурсы, инвестиции, затраты и, соответственно, получать выгоды [1].

В статье предлагается разработка прототипа эффективной экосистемы взаимодействия СУБД PostgreSQL 11 и аналитической платформы Loginom Community, идея которой заключается в том, что пользователь интегрированной системы сможет эффективно решать задачи хранения информации и ее аналитической обработке.

В качестве примера рассмотрена технология создания экосистемы взаимодействия баз данных для эффективного контроля за фирменным подвижным составом Октябрьской железной дороги в течение X дня с использованием СУБД PostgreSQL 11 и аналитической платформы Loginom Community.

2. Актуальность применения информационных технологий в логистике

Индустрия логистики значительно выигрывает от достижений в области информационных технологий. Однако улучшения, которые технологии привносят в сектор логистики, от улучшения связи до оптимизации маршрутов доставки, на этом не заканчиваются. При использовании логистической интеграции, транспортные компании могут расширить свое портфолио и предложить своим клиентам больше услуг [2].

В последние годы возможность интегрировать несколько инструментальных систем обеспечивает повышение эффективности решения транспортных и логистических задач. Благодаря интеграции API обмен данными происходит быстро и безопасно, что позволяет обеим сторонам оперативно действовать в случае возникновения проблем [3, 4].

Такая система использует программное обеспечение и технологии, среди прочего, для помощи в управлении автопарком, а также используется для мониторинга данных о пассажирах или грузах в движении и предоставления информации о автопарке в режиме реального времени. Это упрощает общий процесс транспортировки за счет использования комплексного решения для обеспечения видимости и контроля, которое позволяет планировать и управлять перевозочным процессом, а также выбирать наиболее экономичный способ.

3. Формирование баз данных с применением СУБД PostgreSQL

Одной из наиболее успешных доступных баз данных с открытым исходным кодом в настоящее время считается PostgreSQL. Сейчас это одна из самых продвинутая система с широким спектром функций, которые бросают вызов даже многим базам данных с закрытым исходным кодом [5, 6].

Так как PostgreSQL является надежной, безопасной и расширяемой базой данных, а также располагает обширной экосистемой доступных средств, разработчики используют PostgreSQL в разнообразных сценариях.

Это программное обеспечение совместимо со всеми основными операционными системами, включая Linux, Windows и Macintosh, а также поддерживает текст, изображения, звуки и видео. Благодаря этому база данных пользуется популярностью у пользователей и компаний с различными потребностями [7, 8]. В статье рассматривается взаимодействие двух баз данных, сформированных с помощью PostgreSQL: RailwayStation и RailwayStation_data.

В базе данных RailwayStation сосредоточены динамические данные железнодорожного перемещения действующего фирменного подвижного состава Октябрьской железной дороги (заказы, билеты, пассажиры), которые ежедневно дополняются и обновляются.

В базе данных RailwayStation_data располагаются сведения, касающиеся основных характеристик рассматриваемого подвижного состава, посадочных мест, станций и стандартными рейсами. Эти данные можно назвать статичными, так как они практически всегда остаются постоянными.

В формируемой базе данных RailwayStation_data задействованы следующие таблицы:

1) таблица подвижного состава, задача которой – хранение основных данных действующего фирменного подвижного состава ОЖД (всего 48 единиц);

2) таблица станций, задача которой – хранение основных данных тех станций, по которым движется фирменный подвижной состав ОЖД;

3) таблица посадочных мест, задача которой – хранение основных данных всех посадочных местах фирменного подвижного состава ОЖД;

4) таблица рейсов, задача которой – хранение основных данных рейсов, проходящих в течение X дня;

Таблицы в базе данных связываются между собой путём создания ключей (табл. 1).

Таблица 1

Установка связей между таблицами в базе данных RailwayStation_data

| Пояснение | Отображение |
|--|--|
| Присваивание первичного ключа колонке <i>railway_station_id</i> | CREATE TABLE Railway_Stations (railway_station_id INT PRIMARY KEY GENERATED ALWAYS AS IDENTITY, railway_station_code INT, railway_station_name VARCHAR(80), city VARCHAR(80)); |
| Присваивание первичного ключа колонке <i>train_id</i> | CREATE TABLE Rolling_Stock (train_id INT PRIMARY KEY GENERATED ALWAYS AS IDENTITY, train_code VARCHAR(20), train_name VARCHAR(30), vagon_quantity INT, travel_time VARCHAR(10)); |
| В таблице колонка <i>train_id</i> имеет тип <i>varchar</i> , так как в базе данных для наглядности сведения приведены в виде диапазона | CREATE TABLE Seats(train_id VARCHAR(20), vagon_number VARCHAR(20), seat_number VARCHAR(20), fare_conditions VARCHAR(20)); |

Таблица 3

| Пояснение | Отображение |
|---|--|
| Присваивание первичного ключа колонке <i>race_id</i> , а также ограничение внешнего ключа колонки <i>train_id</i> таблицы <i>Races</i> через ссылку на таблицу <i>Rolling_Stock</i> | CREATE TABLE Races (race_id INT PRIMARY KEY GENERATED ALWAYS AS IDENTITY, scheduled_departure VARCHAR(10), scheduled_arrival VARCHAR(10), departure_station VARCHAR(30), arrival_station VARCHAR(30), train_id INT REFERENCES Rolling_Stock(train_id)); |

В формируемой базе данных RailwayStation будут задействованы следующие таблицы:

1. Таблица заказов, задача которой – хранение данных всех заказов (индивидуальный номер заказа, дата и цена).

Для удобства распределения заказов между различными типами поездов, все номера генерируются в различных диапазонах в зависимости от подвижного состава (табл. 2).

Таблица 2

Выделенные диапазоны по типам подвижного состава

| Тип подвижного состава | Выделенные диапазоны |
|------------------------|----------------------|
| Гранд Экспресс | 0 – 1000 |
| Карелия | 1001 – 2000 |
| Красная стрела | 2001 – 3000 |
| Мегаполис | 3001 – 4000 |
| Невский экспресс | 4001 – 5000 |
| Николаевский экспресс | 5001 – 6000 |
| Сапсан | 6000 – 25000 |
| Северная пальмира | 25001 – 26000 |
| Черноморец | 26001 – 27000 |
| Экспресс | 27001 – 28000 |

2. Таблица билетов, задача которой – хранение персональных данных пассажиров и отображение индивидуального номера каждого билета. Значение ‘order_number’ связано с таблицей заказов так, что по одному заказу может быть выделено сразу несколько билетов (в том случае, если один человек заказывает билеты на нескольких);

3. Связующая таблица данных о билетах и рейсах, задача которой – соотношение каждого взятого билета к выбранному рейсу дополнительно с указанием класса и цены;

4. Таблица посадочных талонов, задача которой – хранение основных данных, указанных на посадочных талонах каждого пассажира. Таблица является связующей, так как принимает значения из вышеприведенных таблиц.

Таблицы в базе данных связываются между собой путём создания ключей (табл. 3).

Таким образом, SQL позволяет определять ограничения для столбцов и таблиц, а сами ограничения дают контроль над данными в таблицах. Если пользователь пытается сохранить данные в столбце, который нарушает ограничение, возникает ошибка. Это применимо, даже если значение получено из определения значения по умолчанию.

Установка связей между таблицами в базе данных
RailwayStation_data

| Пояснение | Отображение |
|--|--|
| Присваивание первичного ключа колонке <i>order_id</i> | CREATE TABLE Bookings (order_id INT PRIMARY KEY GENERATED ALWAYS AS IDENTITY, order_number INT, booking_date DATE, total_price INT); |
| Присваивание первичного ключа колонке <i>ticket_id</i> | CREATE TABLE Tickets (ticket_id INT PRIMARY KEY GENERATED ALWAYS AS IDENTITY, ticket_number BIGINT, order_number INT, passenger_name VARCHAR(80), contact_data VARCHAR(20)); |
| Ограничение внешнего ключа колонки <i>ticket_id</i> таблицы <i>Ticket_Races</i> через ссылку на таблицу <i>Tickets</i> , а также колонки <i>race_id</i> через ссылку на таблицу <i>Races</i> | CREATE TABLE Ticket_Races (ticket_id BIGINT REFERENCES Tickets(ticket_id), race_id INT REFERENCES Races(race_id), fare_conditions VARCHAR(150), price INT); |
| Ограничение внешнего ключа колонки <i>ticket_id</i> таблицы <i>Ticket_Races</i> через ссылку на таблицу <i>Tickets</i> , а также колонки <i>race_id</i> через ссылку на таблицу <i>Races</i> | CREATE TABLE Boarding_Passes (ticket_id INT REFERENCES Tickets(ticket_id), race_id INT REFERENCES Races(race_id), seat_number INT); |

3. Интеграция баз данных в аналитическую платформу Loginom Community

После формирования двух баз данных, необходимо их вывести на аналитическую платформу Loginom Community для дальнейшего решения задач. Выбор платформы обусловлен тем, что компания Postgres Professional и Loginom Company заключили соглашение о технологическом партнерстве, направленном на обеспечение совместимости продуктов [9, 10].

Данное сотрудничество позволит предлагать заказчикам комплексное решение по хранению, обработке и анализу данных, включающее функционал как аналитической low-code платформы Loginom, так и СУБД Postgres Pro – флагманского продукта компании Postgres Professional.

Logicom Community – это аналитическая платформа, которая предоставляет возможности глубокой аналитики и позволяет принимать управленческие решения на основе точной и достоверной информации [12].

В качестве ключевых возможностей выделяют проведение сложных расчетов, консолидацию данных, очистку данных, прогнозирование и оптимизацию данных, интеграцию с любыми хранилищами данных (базами данных, отдельные файлы, учетные системы, социальные сети, веб-сервисы), комбинацию из структурного и объектно-ориентированного подходов к моделированию [13, 14].

Перед тем как использовать в сценариях узлы взаимодействия в пакете необходимо создать подключение к источнику данных. Подключение содержит в себе необходимые параметры для соединения с источником данных, такие как пароль/логин, расположение источника и др. Созданное подключение в дальнейшем может использоваться в пакете многократно [15, 16].

Для работы с базой данных, предварительно необходимо создать Подключение соответствующего типа, в зависимости от того к какой базе нужно подключиться. Созданное подключение необходимо поместить в сценарий, для этого необходимо создать узел, выходными данными которого являются параметры подключения к источнику данных [17].

Подключение можно создать двумя способами:

- перетащить нужное подключение из дерева в область подключений;
- дважды кликнуть по выбранному подключению в дереве.

В области подключений появится новое подключение, и откроется диалог редактирования параметров подключения. После того, как требуемые параметры будут заданы, подключение может быть протестировано.

Для работы с таблицами в базе данных в среде Loginom Community необходимо настроить параметры подключения (рис. 1).

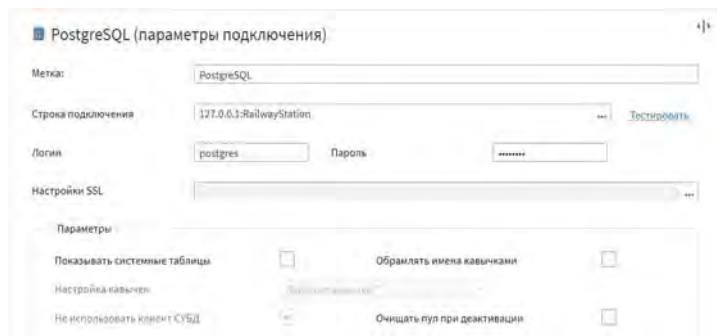


Рис. 1. Подключение базы данных RailwayStation в PostgreSQL к среде Loginom Community

Loginom полностью построен на основе веб-технологий. Веб-интерфейс обладает рядом существенных преимуществ:

- браузеры функционируют на любых ОС (Windows, MacOS, Linux и др.) и множестве устройств;
- минимизируются усилия по администрированию, так как отсутствует необходимость инсталляции и настройки рабочих мест.

Платформа обладает пользовательским интерфейсом, не требующим для работы специальной подготовки. Loginom имеет поддержку технологий анализа: от простой логики до машинного обучения.

В результате настройки подключения баз данных к среде Loginom Community, окно «Подключения» выглядит следующим образом (рис. 2).

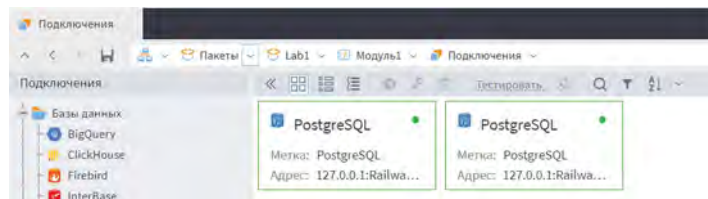


Рис. 2. Окно «Подключения» после интеграции баз данных в PostgreSQL в среду Loginom Community

Для реализации эффективного отслеживания ключевых сведений отдельного действующего фирменного поезда Октябрьской железной дороги, разработан следующий алгоритм:

- добавление таблиц, разработанных в системе PostgreSQL, в среду Loginom Community;
- разделение всех таблиц на две группы: со статическими данными (характеристики действующего подвижного состава, станций, количества и классов посадочных мест) и динамическими данными (количество заказов, билетов, талонов и рейсов);
- сортировка строк таблиц в соответствии с настроенными диапазонами значений (либо *train_id* в таблицах со статическими данными, либо *race_id* или *order_number* в таблицах с динамическими данными);
- слияние или соединений данных, собранных с разных таблиц для дальнейшего получения наглядных данных и впоследствии эффективной работы с ними;
- настройка и вывод результатов в удобную для восприятия форму Excel-документа.

Для реализации алгоритма сформирован следующий сценарий в среде Loginom Community (рис. 3).

Для оценки эффективности выполнения сценария рассмотрим его работу на примере случайно выбранного подвижного состава – к примеру, Экспресса. Для этого необходимо настроить компоненты всех элементов сортировки в сценарии (табл. 4).

Таблица 4

Настройка компонентов сценария «Экспресс»

| Параметр | Условие |
|---------------------|----------------------------------|
| <i>train_id</i> | 47 <= order_number <= 48 |
| <i>order_number</i> | 27 001 <= order_number <= 28 000 |
| <i>race_id</i> | 47 <= order_number <= 48 |

В результате настройки параметров нами получены результаты всех данных, касающихся подвижного состава Экспресса, в виде трех таблиц в формате Excel-документа. Для демонстрации формата вывода приведена таблица, включающая в себя данные о заказах, билетах и пассажирах, взятые за X день (рис. 4). Кроме этих данных, также можно настроить вывод необходимых сведений о рейсах и поездах, которые будут в движении в X день.

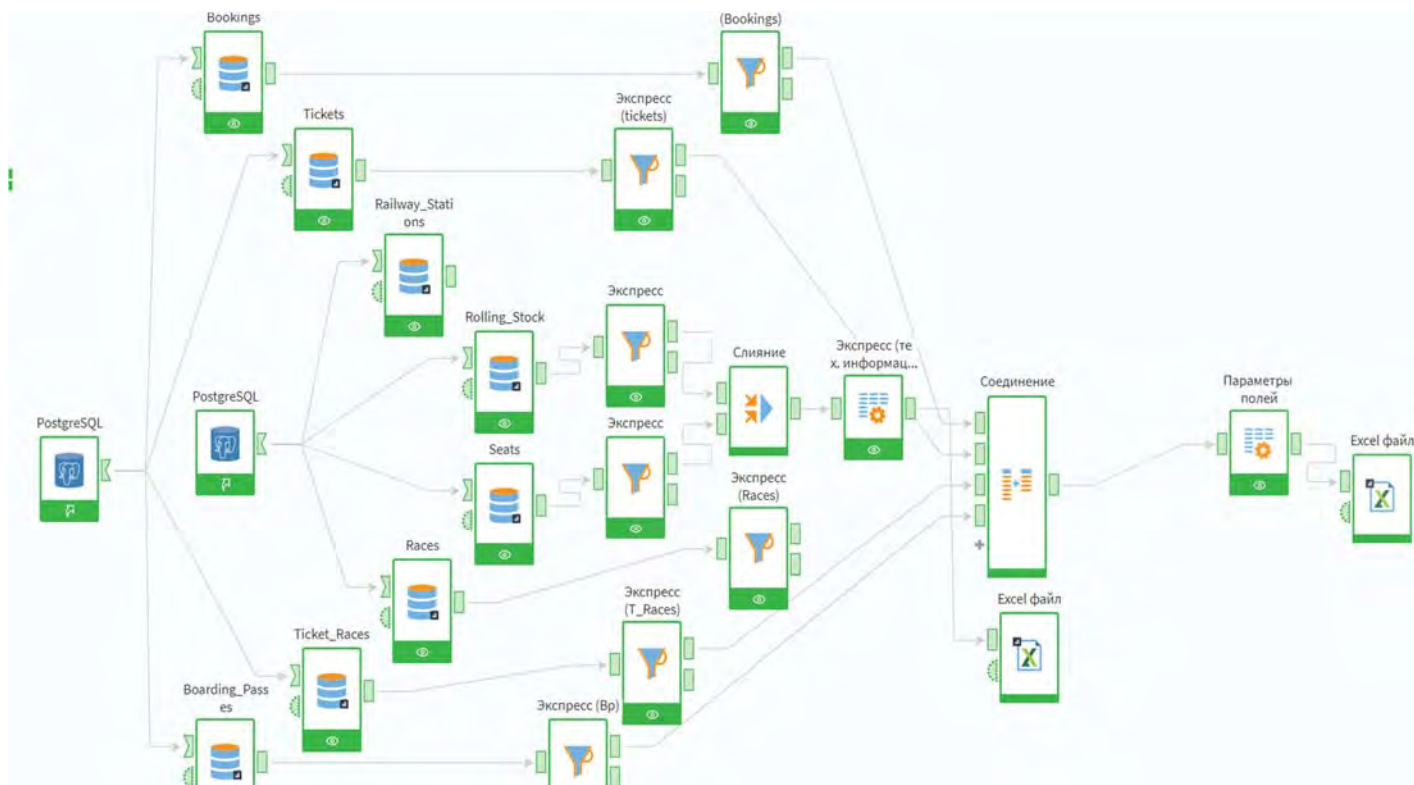


Рис. 3. Сценарий проекта

| # | A | B | C | D | E | F | G | H |
|---|-----------|------------|--------------------|--------------------------|--------------|-----------------|-------|-----------|
| 1 | order_nun | booking_d | ticket_number | passenger_name | contact_data | fare_conditions | price | seat_numl |
| 2 | 27 666 | 10.10.2022 | 74 532 723 148 678 | Константинова Арина Мирс | +79626777532 | Вагон Плацкарт | 1 300 | 11 |
| 3 | 27 008 | 10.10.2022 | 74 778 034 566 765 | Макаров Иван Константино | +79224185630 | Вагон Купе | 1 950 | 13 |
| 4 | 27 994 | 10.10.2022 | 74 261 338 554 080 | Демьянова Анна Тимофееви | +79218667598 | Вагон Плацкарт | 1 300 | 17 |
| 5 | 27 876 | 10.10.2022 | 74 635 686 753 565 | Гусева Камила Никитична | +79313445245 | Вагон Купе | 1 950 | 12 |
| 6 | 27 345 | 10.10.2022 | 74 251 466 545 654 | Селезнева Виктория Дании | +79313445245 | Вагон Купе | 1 950 | 6 |

Рис. 4. Данные о заказах, билетах и пассажирах, взятые за X день

При рассмотрении взаимодействия СУБД PostgreSQL 11 и аналитической платформы Loginom Community предложено решение эффективного хранения и обработки информации о перемещении действующего фирменного подвижного состава Октябрьской железной дороги в течение одного случайного дня. Благодаря реализации взаимодействия, пользователь интегрированной системы способен эффективно отслеживать ключевые сведения отдельно выбранного действующего фирменного поезда Октябрьской железной дороги.

Таким образом, благодаря интеграции СУБД и аналитической платформы Loginom Community становятся доступными решения разнообразного спектра задач. Применение платформы Loginom делает продвинутую аналитику доступной бизнес-пользователям. Визуальный конструктор позволяет настроить все процессы анализа: интеграцию, подготовку данных, моделирование и визуализацию. Loginom сокращает время от тестирования гипотезы до создания работающего бизнес-процесса [15].

Интеграция инструментальных систем и сбалансированное распределение функций управления движением поездов позволяет создать и реализовать комплекс по управлению перевозочным процессом нового уровня, способный к разрешению конфликтов и оптимизации графика с учетом изменений в реальном времени.

4. Заключение

Развитие транспортной инфраструктуры играет важную роль для устойчивого развития России и вхождения ее в международную систему хозяйства. Надежность работы всех коммуникаций во многом зависит от оперативной и достоверной оценки пространственно-временных параметров природно-техногенных условий и процессов. При этом важно знать существующее состояние объекта, динамику ситуации и возможные направления ее развития.

Применение новых отечественных СУБД и аналитических платформ позволяет Российской Федерации решать транспортные задачи с применением независимых универсальных технологий. PostgreSQL уже завоевал прекрасную репутацию мощного и многофункционального решения для реляционных данных, причём СУБД отличается превосходной реализацией основных реляционных функций, не ограничивая себя рамками традиционных СУБД. ОАО «РЖД» подписало трехлетнее соглашение, предоставляющее возможность неограниченного использования лицензий СУБД Postgres Pro, что позволит компании активно развивать цифровые сервисы, в основе которых лежат постоянно растущие объемы данных, продолжить реализацию политики импортозамещения, направленную на достижение технологической независимости.

Благодаря таким шагам, в транспортную отрасль внедряются важнейшие базовые технологии в решение задачи построения «умного» железнодорожного комплекса, находящегося на передовых позициях в транспортных системах регионов.

Дальнейшие исследования целесообразно продолжить в направлениях практической реализации подходов к интеграции современных инструментальных средств, в том числе рассмотренных систем с пакетами математических расчетов, организации параллельных вычислений и системами программирования высокого уровня для повышения удобства и эффективности решения сложных научно-технических задач по аналогии с тем, как это описано в [18-20].

Литература

1. *Илюхина С.С.* Информационные технологии в логистике транспортного узла // *Инновации и инвестиции*. 2020. № 2. С. 256-258.
2. *Негреева В.В., Замятина А.А., Шпакович Д.К., Шаронова А.Д.* Использование цифровых технологий в логистике. Научный журнал НИУ ИТМО. Серия «Экономика и экологический менеджмент». 2020. С. 94-99.
3. *Ding Y., Jin M., Li S., Feng D.* Smart logistics based on the internet of things technology: an overview. *International Journal of Logistics Research and Applications*, 2021, vol. 24, pp. 323-345.
4. *Tang C., Veelenturf L.* The strategic role of logistics in the industry 4.0 era. *Transportation Research Part E: Logistics and Transportation Review*, 2019, vol. 129, pp. 1-11.
5. *Ferrari L., Pirozzi E.* Learn PostgreSQL: Build and manage high-performance database solutions using PostgreSQL 12 and 13. Birmingham: Packt Publishing, 2020. 616 p.
6. *Juba S., Volkov A.* Learning PostgreSQL 11: A beginner's guide to building high-performance PostgreSQL database solutions. Birmingham: Packt Publishing, 2019. 528 p.

7. *Данилов А.Д., Терехов Д.В.* Сравнительный анализ СУБД для выбора операционной базы данных // *Системы управления и информационные технологии*. 2019. № 3(77). С. 56-63.

8. *Демахин И.А.* Сравнительный анализ систем управления базами данных с открытым исходным кодом. Россия молодая. 2022. С. 31513.1–31513.7

9. *Ткаченко А.Л., Мельников А.А., Кузнецова В.И.* Прикладные решения на базе Loginom. *Дневник науки*. 2021. № 5.

10. *Невекин Д.А., Прокопенко Н.Ю.* Разработка библиотеки очистки данных для систем бизнес-аналитики на базе АП Loginom. *X Всероссийский фестиваль науки*. 2020. № 2. С. 358-361.

11. *Невекин Д.А., Прокопенко Н.Ю.* Разработка системы поддержки принятия решений на базе аналитической платформы Loginom для эффективного управления маркетинговыми кампаниями. *Вестник Сыктывкарского университета. Серия 1. Математика. Механика. Информатика*, 2020. № 2(35). С. 37-44.

12. *Морарь Е.В., Рыжковский П.А.* О возможности применения аналитической платформы Loginom для анализа данных торговой компании. *Информационный бюллетень омского научно-образовательного центра ОмГТУ и ИМ СО РАН в области математики и информатики*, 2020. № 1. С. 71-73.

13. *Староверов С.В., Иванова И.А., Перунова В.Э., Чижова Н.А.* Эффективность алгоритмов выбора товара для потребителя в системе Loginom. *Современные технологии в науке и образовании*, 2020. С. 214-219.

14. *Бабурин А.Н.* Особенности построения ансамблей моделей для обработки разнородных социологических данных в среде Loginom // *Актуальные проблемы современной науки: взгляд молодых*. 2019. С. 597-600.

15. *Ткаченко А.Л., Махорин Д.П., Кузнецова В.И.* Интеллектуальный анализ динамики курса золота с помощью программы Loginom // *Заметки ученого*. 2021. № 9 (57).

16. *Евсюков В.В., Капустин А.В., Ильина Ю.А.* Аналитическая платформа Loginom – универсальный инструмент углубленной аналитики. *Вестник тульского филиала финуниверситета*. 2020. № 1. С. 291-292.

17. *Тришин Д.В., Прокопенко Н.Ю.* Разработка библиотеки прогнозирования в Loginom // *X Всероссийский фестиваль науки*. 2020. С. 354-357.

18. *Ермаков С.Г., Забродин А.В., Красновидов А.В., Хомоненко А.Д.* О взаимодействии Simulink-моделей сложных и интеллектуальных систем с программами на языках высокого уровня. *Телекоммуникации и транспорт*. 2022. № 12. С. 23-31.

19. *Adadurov S., Khomonenko A., Krasnovidov A.* Comparison of Control Systems Based on PID Controllers and Based on Fuzzy Logic Using MatLab and Simulink. *Lecture Notes in Networks and Systems*, 2021, vol. 229, pp. 224-237.

20. *Krasnovidov A.V., Khomonenko A.D.* Integration of MatLab and R with high-level languages using C# and Microsoft Visual Studio as an example/ *Conference Paper. Journal of Physics: Conference Series*, 2021, 2131(2), 022096.



INTEGRATION OF BUSINESS INTELLIGENCE SYSTEMS WITH DATABASE MANAGEMENT SYSTEMS IN TRANSPORT

DANIIL MARKEVICH
St-Petersburg, Russia

VALERIA KHARLANOVA
St-Petersburg, Russia

ANATOLY KHOMONENKO
St-Petersburg, Russia

KEYWORDS: *business intelligence system, database management system, tool systems integration, PostgreSQL, Loginom Community, the role of integration and digitalization in the railway field.*

ABSTRACT

Introduction: at present, the solution of various transport problems using information technologies is of great practical interest. To work with databases containing huge amounts of information, their structuring, thorough analysis and making optimal decisions, researchers and analysts actively use various systems, such as database management systems (DBMS) or business intelligence systems. Despite this, the integration of such systems, which can improve the quality of decisions, is still not widely used. **Purpose:** is to develop the integration technology between the business intelligence system and the DBMS, which allows you to work effectively with a huge amount of data when solving transport tasks. **Methods:** The integration of the systems under consideration is implemented using the PostgreSQL 11 DBMS and the Loginom Community analytical platform. **Results:** a full cycle of system integration has been completed, including the creation and filling of a database in the PostgreSQL 11 system, as well as its connection to

the Loginom Community analytical platform for data structuring, analysis and further decision-making. **Practical relevance:** the main distinguishing feature of the implemented technology is the full compatibility of two systems initially responsible for different tasks: a database with an extensive ecosystem of available tools, and a platform that provides deep analytics capabilities for making optimal management decisions. The reasons and advantages of the integration of the above systems, as well as their application in solving specific transport problems, are presented. **Discussion:** when solving the problem of ensuring integration, the practical application of a DBMS and a business intelligence system is considered. Using PostgreSQL 11, two databases are formed, which are integrated with the Loginom Community analytical platform. It is advisable to continue further research in the areas of practical use of integration for the analytics of large database arrays, as well as in the interests of improving the quality of managerial decision-making in transport problems.

REFERENCES

1. Ilyukhina S.S. Information technologies in logistics of a transport hub. *Innovacii i investicii* [Innovation and investment]. 2020. No. 2, pp. 256-258. (In Rus)
2. Negreeva V.V., Zamyatina A. A., Shpakovich D. K., Sharonova A.D. The use of digital technologies in logistics. *Nauchnyy zhurnal NIU ITMO. Seriya "Jekonomika i jekologicheskij menedzhment"* [Scientific Journal of NIU ITMO. The series "Economics and Environmental Management"]. 2020, pp. 94-99. (In Rus)
3. Ding Y., Jin M., Li S., Feng D. Smart logistics based on the internet of things technology: an overview. *International Journal of Logistics Research and Applications*, 2021, vol. 24, pp. 323-345.
4. Tang C., Veelenturf L. The strategic role of logistics in the industry 4.0 era. *Transportation Research Part E: Logistics and Transportation Review*, 2019, vol. 129, pp. 1-11.
5. Ferrari L., Pirozzi E. Learn PostgreSQL: Build and manage high-performance database solutions using PostgreSQL 12 and 13. Birmingham: Packt Publishing, 2020. 616 p.
6. Juba S., Volkov A. Learning PostgreSQL 11: A beginner's guide to building high-performance PostgreSQL database solutions. Birmingham: Packt Publishing, 2019. 528 p.
7. Danilov A.D., Terekhov D.V. Comparative analysis of a DBMS for choosing an operational database. *Sistemy upravlenija i informacionnye tehnologii* [Management systems and information technologies]. 2019. No. 3(77), pp. 56-63. (In Rus)
8. Demakhin I.A. Comparative analysis of open source database management systems. *Molodaya Rossiya* [Young Russia]. 2022, pp. 31513.1-31513.7. (In Rus)
9. Tkachenko A.L., Melnikov A.A., Kuznetsova V.I. Applied solutions based on Loginom. *Dnevnik nauki* [Diary of Science]. 2021. No. 5. (In Rus)
10. Nevekin D.A., Prokopenko N.Y. Development of a data purification library for business intelligence systems based on Loginom. *X All-Russian Science Festival*. 2020. No. 2, pp. 358-361. (In Rus)
11. Nevekin D.A., Prokopenko N.Y. Development of a decision support system based on the Loginom analytical platform for effective management of marketing campaigns. *Vestnik Syktyvkar'skogo universiteta. Seriya 1. Matematika. Mehanika. Informatika* [Bulletin of Syktyvkar University. Series 1. Mathematics. Mechanics. Informatics], 2020. No. 2(35), pp. 37-44. (In Rus)
12. Morar E.V., Ryzhkovsky P.A. On the possibility of using the Loginom analytical platform for analyzing trading company data. *Informacionnyj bjulleten' omskogo nauchno-obrazovatel'nogo centra OmGTU i IM SO RAN v oblasti matematiki i informatiki* [Newsletter of the Omsk Scientific and Educational Center of OmSTU and IM SB RAS in the field of mathematics and computer science], 2020. No. 1, pp. 71-73. (In Rus)

13. Staroverov S.V., Ivanova I.A., Perunova V.E., Chizhova N.A. Efficiency of algorithms for choosing goods for consumers in the Loginom system. *Sovremennye tehnologii v nauke i obrazovanii* [Modern technologies in science and education], 2020, pp. 214-219. (In Rus)
14. Baburin A.N. Features of constructing ensembles of models for processing heterogeneous sociological data in the Loginom environment. *Aktual'nye problemy sovremennoj nauki: vzgljad molodyh* [Actual problems of modern science: the view of the young]. 2019, pp. 597-600. (In Rus)
15. Tkachenko A.L., Makhorin D. P., Kuznetsova V.I. Intellectual analysis of the dynamics of the gold exchange rate using the Loginom program. *Zametki uchenogo* [Notes of the scientist]. 2021. No. 9 (57).
16. Evsyukov V.V., Kapustin A.V., Ilyina Y.A. Loginom analytical platform is a universal tool for in-depth analytics. *Vestnik tul'skogo filiala finuniversiteta* [Bulletin of the Tula branch of the Financial University]. 2020. No. 1, pp. 291-292. (In Rus)
17. Trishin D.V., Prokopenko N.Y. Development of the forecasting library in Loginom. *X All-Russian Science Festival*. 2020, pp. 354-357. (In Rus)
18. Ermakov S.G., Zabrodin A.V., Krasnovidov A.V., Homonenko A.D. The interaction of Simulink models of complex and intelligent systems with programs in high-level languages. *Telekommunikacii i transport* [Telecommunications and Transport]. 2022. No. 12, pp. 23-31. (In Rus)
19. Adadurov S., Khomonenko A., Krasnovidov A. Comparison of Control Systems Based on PID Controllers and Based on Fuzzy Logic Using MatLab and Simulink. *Lecture Notes in Networks and Systems*, 2021, vol. 229, pp. 224-237.
20. Krasnovidov A.V., Khomonenko A.D. Integration of MatLab and R with high-level languages using C# and Microsoft Visual Studio as an example. *Conference Paper. Journal of Physics: Conference Series*, 2021, 2131(2), 022096.

INFORMATION ABOUT AUTHORS:

Daniil V. Markevich, Master's student at the Department of Information and Computing systems of Emperor Alexander I St. Petersburg state transport university, St. Petersburg, Russia, dmarkevich811@mail.ru

Valeria V. Kharlanova, Master's student at the Department of Information and Computing systems of Emperor Alexander I St. Petersburg state transport university, St. Petersburg, Russia, lerya107@yandex.ru

Anatoly D. Khomonenko, Grand PhD, Professor, Professor of the Department of Information and Computing systems of Emperor Alexander I St. Petersburg state transport university, St. Petersburg, Russia, khomon@mail.ru

For citation: Markevich D.V., Kharlanova V.V., Khomonenko A.D. Integration of business intelligence systems with database management systems in transport. *H&ES Reserch*. 2023. Vol. 15. No 2. P. 41-48. doi: 10.36724/2409-5419-2023-15-2-41-48 (In Rus)



doi: 10.36724/2409-5419-2023-15-2-49-56

ИДЕНТИФИКАЦИЯ УГРОЗ СРЕДСТВАМИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И ВЫБОР ЗАЩИТЫ МЕТОДАМИ МАШИННОГО ОБУЧЕНИЯ

ВОРОНИН

Евгений Алексеевич¹

КОЗЛОВ

Сергей Витальевич²

КУБАНКОВ

Александр Николаевич³

АННОТАЦИЯ

Введение: В сфере разработки и производства бортовых информационно-коммуникационных систем и комплексов отмечается устойчивая тенденция к интенсивному внедрению новых интеллектуальных технологий, обеспечивающих поддержку их функционирования в рамках единого информационного пространства. Такое направление открывает широкие возможности повышения эффективности применения средств мобильности различного назначения (перевозка грузов, персонала служб в условиях чрезвычайных ситуаций и др.). Вместе с тем с ростом технологического уровня средств мобильности, а также их бортовых систем и комплексов информационного взаимодействия одновременно расширяются горизонты новых угроз и потенциальных опасностей, определяющих экономическую безопасность как основу гарантированного развития этой отрасли с минимальными рисками на основе применения перспективных интеллектуальных технологий. **Рассматриваются задачи:** выявления источников и характера угроз методами наивного Байеса и Байесовских сетей доверия для обеспечения безопасности при разработке, производстве и эксплуатации бортовых систем; выбора оптимального набора операций и мероприятий организационного и технологического характера с учетом ожидаемых затрат или максимуму безопасности при ограничениях допустимых расходов. Предлагается решать их методами машинного обучения и эволюционных алгоритмов оптимизации.

Сведения об авторах:

¹ д.т.н., в.н.с., ведущий научный сотрудник, Федеральный исследовательский центр "Информатика и управление" РАН, Москва, Россия, e.voronin1@gmail.com

² к.т.н., с.н.с., руководитель отделения, Федеральный исследовательский центр "Информатика и управление" РАН, Москва, Россия, sv_kozlov@mail.ru

³ д.в.н., профессор, заведующий кафедрой, Московский технический университет связи и информатики, Москва, Россия, a.n.kubankov@mtuci.ru

КЛЮЧЕВЫЕ СЛОВА: Сфера производства интеллектуальных бортовых систем, безопасность, вероятностные модели безопасности, байесовские сети доверия, угрозы безопасности, машинное обучение, EM алгоритм максимального правдоподобия.

Для цитирования: Воронин Е.А., Козлов С.В., Кубанков А.Н. Идентификация угроз средствами обеспечения безопасности и выбор защиты методами машинного обучения // Научные технологии в космических исследованиях Земли. 2023. Т. 15. № 2. С. 49-56. doi: 10.36724/2409-5419-2023-15-2-49-56

Введение

Выбор и обоснование средств и мероприятий по обеспечению экономической безопасности сложная и многоэтапная задача [1, 2]. Она может быть решена при наличии необходимой информации о организации и структуре защищаемых систем, эмпирическая информация достаточно больших объемов и достоверности. Цифровая экономика и информационное пространство может быть построено на современных распределенных и доступных информационных ресурсах с возможностью представления и получения необходимых знаний. Они извлекаются и обрабатываются из информационных ресурсов данных методами машинного обучения. Для решения этой, важной задачи следует определить необходимые знания (свойства и закономерности) и технологии их обработки.

В существующих руководствах и методиках обеспечения безопасности эта задача решается в два этапа [1-4]. В начале выявляются угрозы путем оценки индикаторов безопасности. На втором выбираются необходимые меры противодействия. При этом оптимизация набора защитных мероприятий, в классическом её смысле не ставится и осуществляется на интуитивном или эмпирическом уровне т.к. количество индикаторов достигает десятков и сотен единиц и нет критерия оптимизации, а практика свертки индикаторов не удовлетворяют условиям устойчивости и достаточной достоверности оптимизации. Угрозы экономической безопасности можно разделить на явные и скрытые, прямые и косвенные. Косвенными угрозами называются некоторые признаки явных или скрытых, будущих угроз. Угрозы имеет ряд косвенных признаков, предшествующих ей, и определяются, как аномалии. По выявленным аномалиям формируются и оцениваются свидетельства, которые передаются для дальнейшего анализа в соответствующую систему управления безопасностью (рис. 1).



Рис. 1. Структура системы идентификации угроз и обеспечения безопасности

Известно, что во многих случаях явные угрозы легче и дешевле предупредить. Поэтому в маркетинге, управлении бизнесом, медицине и военном деле применяется анализ поведенческих данных, позволяющий находить причинно-следственные связи между событиями и экономическими факторами [5]. Такой анализ поведенческих данных к обеспечению экономической и других видов безопасности, в условиях массовой цифровизации, актуален и может быть эффективным при использовании методов машинного обучения.

Цель исследования. Разработка методов идентификации причинно-следственных связей угроз безопасности, поиска оптимального набора защитных мероприятий и технологий машинного обучения.

Методы. Показатели безопасности принято определять отраслевым стандартом или нормативным документом. Но такие стандарты и методики оценки отсутствуют, а руководства и учебники по безопасности предлагают методики основаны на наборах индикаторов состояния или их свертке в один нормируемый параметр. Число таких индикаторов от десяти и больше сотни [1-4]. Но сравнение этих векторов с эмпирическими весами не информативно и субъективно и не может быть нормируемым показателем безопасности.

Известно, что безопасность защищаемых объектов определяется угрозами ей и способностью его противостоять им.

Поэтому выбран и предлагается вероятностный показатель [6]:

$$P_s = (1 - P_u) + P_u \cdot P_o, \quad (1)$$

где: P_s – вероятность безопасного состояния, P_u – вероятность угрозы безопасности, P_o – вероятность успешного отражения или противодействия угрозе.

Этот критерий безопасности представляет возможность построения алгебры безопасности систем со сложной схемой событий, структурой и схемой угроз.

К примеру, если имеется n – е количество угроз, то безопасность субъекта вычисляется по формуле

$$P_s = \prod_{i=1}^n P_{si} = \prod_{i=1}^n [(1 - P_{ui}) + P_{ui} \cdot P_{oi}], \quad (2)$$

где: P_{si} – вероятность безопасности при i -й угрозе, P_{ui} – вероятность i -й угрозы, P_{oi} – вероятность успешного противодействия i -й угрозе.

Главные достоинства этого критерия безопасности в том, что он учитывает угрозы и возможности их отражения, является нормируемым, подходит для сложной схемы событий и мероприятий, имеет четкое, функциональное объяснение, учитывает опасность угроз и возможности противодействия им. Основное свойство системы безопасности успешно противодействовать угрозам отражается P_o – вероятностью успешного противодействия угрозе. Она, во многих случаях, может быть параметром оптимизации безопасности.

Не трудно заметить, что уровень безопасности, в экономическом смысле, определяется ожидаемым ущербом от нарушения безопасности и затратами противодействие угрозам. Очевидно, что существует определенное, минимальное, равновесное значение их суммы, дающее оптимальное значение безопасности, т.е.

$$opt(P_s) \rightarrow \min(U + Z_o), \quad (3)$$

где: U – потери от реализованных угроз при заданном уровне безопасности, Z_o – затраты на обеспечение заданного уровня безопасности.



Эта сумма полностью отвечает требованиям к экономическому критерию безопасности и предлагается в качестве показателя оптимальности.

При известных вероятностях P_u и P_o ожидаемые потери от реализованных угроз вычисляются по формуле

$$U = P_u \cdot (1 - P_o) \cdot d, \quad (4)$$

где: d – возможные экономические потери от угроз.

Затраты на противодействие угрозам $Z_o = Z(P_o, \{x_i, i=1...N\})$ – вычисляются, как функция от вероятности успешного противодействия угрозам или P_o определяется затратами на мероприятие по ее обеспечению.

Главной особенностью оптимизации безопасности является то, что оптимальное решение строится путем комбинаторной оптимизации и дискретных переменных, т.е. путем выбора набора мероприятий или операций, имеющих установленные значения стоимости и определяющих вероятность успешного противодействия угрозам. Такой набор, в математическом определении, представляется вектором с бинарными компонентами, принимающими значения из множества $\{0, 1\}$ т.е., как набор категориальных переменных.

Исходя из этого подхода, алгоритм расчета экономически оптимального уровня безопасности представляется в виде

$$opt(P_S) \rightarrow \arg \min_{\{x_i, i=1...N\}} [d \cdot P_u (1 - P_o(x_i, i=1...N)) + Z(x_i, i=1...N)], \quad (5)$$

где: $Z(x_i, i=1...N)$ – функция категориальных переменных от скалярного произведения вектора мероприятий на вектор их стоимости

$$Z(x_i, i=1...N) = \sum_{i=1}^N c_i \cdot x_i = c_1 x_1 + c_2 x_2 + c_3 x_3 + \dots + c_N x_N, \quad (6)$$

c_i – затраты на i -е мероприятие по обеспечению безопасности.

На практике, могут быть случаи, когда потери от ожидаемых угроз не представляется определить в валюте. Это будет в здравоохранении, обороне, природопользовании и т.п. При этом экономический критерий оптимизации не подходит т.к. не все сводится к деньгам. Тогда поставленная задача решается путем максимизации вероятностного показателя безопасности при ограничениях затрат на операции и мероприятия противодействия угрозам, а формально, алгоритм оптимизации будет иметь вид

$$opt(P_S) \rightarrow \arg \max_{\{x_i, i=1...N\}} [(1 - P_u) + P_u P_o], \quad (7)$$

при

$$Z(x_i, i=1...N) \leq Z_{\max}, \quad (8)$$

где Z_{\max} – ограничение на затраты по противодействию угрозам.

Вектор набора мероприятий $\{x_i, i=1...N\}$ определяет успешность обеспечения безопасности с вероятностью

$P_o(x_1, x_2, x_3, \dots, x_N)$. Это, в свою очередь, порождает задачу определения и оценки этой функции вероятности. Метод ее решения будет изложен дальше в предлагаемой работе

Так как вектор оптимального управления представляется в виде набора $X = \{x_i, i=1...N\}$ с переменными категориального типа, решение задачи может быть осуществлено методами эволюционных алгоритмов комбинаторной оптимизации с использованием алгоритмов отжига или генетической модификации [7,8,12] и критериев эффективности по формулам (5) или (8).

Реализуются эти алгоритмы последовательностью действий:

- Создается одномерный массив всех возможных средств и мероприятий, предназначенных для противодействия возможным или ожидаемым угрозам безопасности;
- Элементы этого массива нумеруются и располагаются в строго фиксированном порядке;
- Этому массиву создается соответствующий его размерности бинарный вектор, каждому элементу, которого, соответствует позиция элемента из созданного массива;
- Далее, случайным образом, формируется образец этого вектора из соответствующих элементов заданного массива.

Процесс выбора оптимального решения реализуется путем генерации и отбора образцов этого вектора с помощью генетического алгоритма или алгоритма отжига.

Если число элементов массива возможных мероприятий равно m то число вариантов решений равно

$$N_v = 2^m - 1. \quad (9)$$

При этом, для формирования варианта вектора решений достаточно будет выбрать случайное, целое число от 1 до N и представить его в двоичном коде. В нем 1 будет соответствовать наличию соответствующего элемента заданного массива, как компоненты вектора решений, а 0 – отсутствие.

Наблюдаемые и латентные угрозы, из-за некоторой неопределенности, имеют случайный характер и их значимость должна оцениваться в виде вероятностной меры по предлагаемому критерию безопасности (1).

Поэтому, для выявления угроз и оценки их вероятностей необходимо построить вероятностное пространство возможных и угрожающих состояний внешней среды у защищаемой системы и найти функцию вероятности $P(x_1, x_2, \dots, x_n)$. Это реализуется методами математической статистики на необходимом большом объеме статистических данных.

В дальнейшем, путем маргинализации по некоторым переменным представляется возможность построить необходимую схему событий и найти соответствующие частные распределения для возможных угроз безопасности. Но такой, прямой подход имеет ряд недостатков:

- требует большой объем исходных данных,
- сложен в вычислениях,
- не отражает причинно-следственных или логических связей между переменными.

Угрозы или факторы угроз могут быть как непрерывными случайными параметрами, так и дискретными, случайными событиями. На непрерывных факторах можно построить дискретное вероятностное пространство угроз если определить их путем введения критических, угрожающих значений фазовых состояний и оценки вероятностей событий достижения или превышения этих уровней.

Известно, если переменные, характеризующие состояние внешней среды, имеют бинарный характер, то для уверенной оценки их вероятностей состояний достаточным будет объем наблюдений больше $N \approx 10 \cdot 2^n$, где n – число переменных [9].

При даже не очень большом числе переменных это будет большой объем данных и затрат на их получение и построение функции вероятности $P(x_1, x_2 \dots x_n)$.

Это подтверждается тем, что неопределенность угроз безопасности определяется этой функцией вероятностей и вычисляется, как энтропия совместного распределения случайных величин

$$H(x_1, x_2, \dots, x_n) = - \sum_{x_1, x_2, \dots, x_n} P(x_1, x_2, \dots, x_n) \log_2 P(x_1, x_2, \dots, x_n). \quad (10)$$

Не трудно заметить, что это будет большая величина и для ее снятия потребуются большие объемы наблюдений и времени. Поэтому необходимо найти метод снижения этой неопределенности.

Для этого рассмотрим формулы совместной энтропии для двух переменных

$$H(x_1 | x_2) = H(x_1, x_2) - H(x_2), \quad (11)$$

$$H(x_1, x_2) = H(x_1 | x_2) + H(x_2). \quad (12)$$

Не трудно заметить в них способ снижения исходной энтропии путем перехода к условным вероятностям и для этого воспользуемся цепным правилом разложения многомерного, совместного распределения на условные распределения

$$P(x_1, x_2, x_3 \dots x_n) = P(x_1)P(x_2 | x_1) \times \dots \times P(x_n | x_1, x_2, x_3 \dots x_{n-1}) \quad (13)$$

Существует $n!$ таких разложений и из них можно найти наиболее простые путем исключения отсутствующих условных вероятностных и логических связей между переменными. Таким путем мы получим Байесовскую сеть и возможности Байесовского анализа [9-12]. Это существенно упростит и облегчит выявление и прогнозирование угроз безопасности.

При таком подходе маргинальные вероятности вычисляются, как Байесовская оценка вероятности гипотезы по формуле [12,13].

$$P(h_i | x_1, x_2 \dots x_n) = \frac{P(x_1, x_2 \dots x_n | h_i) P_a(h_i)}{P(x_1, x_2 \dots x_n)}, \quad (14)$$

где: $P(h_i | x_1, x_2 \dots x_n)$ – вероятность i – й гипотезы, $P(x_1, x_2 \dots x_n | h_i)$ – правдоподобие i – й гипотезы, $P(x_1, x_2 \dots x_n)$ – вероятность

наблюдаемых событий, $P_a(h_i)$ – априорная вероятность i – й гипотезы.

Если в качестве гипотезы определить вероятность угрозы, то формула ее апостериорной вероятности будет иметь вид

$$P(u_i | x_1, x_2 \dots x_n) = \frac{P(x_1, x_2 \dots x_n | h_i) P_a(u_i)}{P(x_1, x_2 \dots x_n)}. \quad (15)$$

Априорные вероятности гипотез удобно определять из наблюдений с использованием бета-распределения [10,11,12].

Апостериорную вероятность, как правило, вычисляют методом Монте-Карло или наивного Байеса [11,12,13], считая наблюдаемые события x_j – независимыми, т.е.

$$P(x_1, x_2 \dots x_n | h_i) \sim P(x_1 | h_i) P(x_2 | h_i) \dots P(x_n | h_i). \quad (16)$$

Метод наивного Байеса широко применяют при выявлении аномалий в задачах оценки информационной безопасности [9], но в задачах экономической безопасности, экологической безопасности и медико-биологической безопасности это допущение о независимости факторов имеет ограниченное применение. Его, как правило применяют на стадии предварительного выявления возможных угроз или свидетельств о них. Кроме того, он не позволяет проводить причинно-следственный анализ событий и оценивать наличие и вероятности латентных факторов возможных угроз.

Эффективной технологией расширения Байесовского анализа являются Байесовские сети доверия [12-16]. Байесовская сеть доверия, графическим образом, представляет функцию вероятности $P(x_1, x_2, \dots, x_n)$ в виде направленного ациклического графа с узлами видов состояний, свидетельств и таблиц условных вероятностей связей между узлами по цепному правилу

$$P(x_1, x_2, \dots, x_n) = P(x_1) P(x_2 | x_1) P(x_3 | x_1, x_2) \dots P(x_n | x_1, \dots, x_{n-1}). \quad (17)$$

Где $P(x_i) \rightarrow (P(x_i = 1), P(x_i = 0))$ – вектор состояния угрозы x_i ,

$${}^a P(x_2 | x_1) \rightarrow \begin{array}{|c|cc|} \hline & P(x_1 = 1) & P(x_1 = 0) \\ \hline P(x_2 = 1) & 0.8 & 0.3 \\ P(x_2 = 0) & 0.2 & 0.7 \\ \hline \end{array} \quad \text{– табли}$$

условных вероятностей.

В аналогичной, табличной форме представляются остальные вектора состояний и условные вероятности [9].

Вектора вероятностей состояний и условные вероятности связей между узлами графа рассчитываются частотным методом по результатам наблюдения и известным формулам из математической статистики.

Значимые узлы и связи этого графа определяются, вычисляются и строятся методами машинного обучения по таблицам не размеченных данных и алгоритму Чоу (Chow) и Лю (Liu) [15, 17] путем вычисления и упорядочивания по величине перекрестной энтропии

$$I(x_i, x_j) = \sum_{x_i, x_j} P(x_i, x_j) \log\left(\frac{P(x_i, x_j)}{P(x_i)P(x_j)}\right). \quad (18)$$

Оптимальной структурой Байесовской сети будет структура максимального веса

$$W(x_1, x_2, \dots, x_n) = \max_{j=1}^{n-1} \sum_{i=1}^{j-1} I(x_i, x_j). \quad (19)$$

Непрерывное обучение и доучивание (корректировка) Байесовской сети на практике реализуется в виде системы машинного обучения, поддерживающей актуальность данных о состоянии защищаемой системы и ее внешнего окружения.

Данные сохраняются в виде таблиц, отражающих события в жизненном цикле защищаемой системы. Для Байесовской машины вывода они требуют специальной разметки, как это делается в случаях использования нейронных сетей и логистической регрессии [11-14].

Пример построения Байесовской сети доверия в экономической безопасности с векторами вероятностей состояний в вершинах и таблиц (матриц) условных вероятностей в узлах графа представлен на рисунке 2.

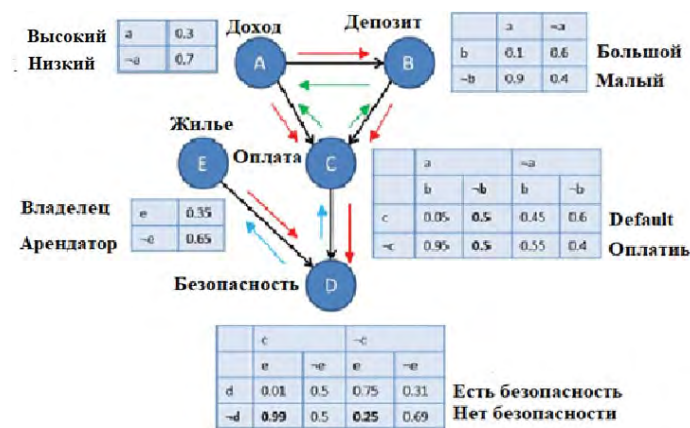


Рис. 2. Пример структуры Байесовской сети доверия в экономической безопасности

Пересчет, в соответствии с алгоритмом распространения вероятности Дж. Перла [18], производится по направлениям, указанным красными стрелками, таблицам исходных состояний (свидетельств) и таблицам условных вероятностей, сверху в низ, позволяет рассчитать вероятность безопасного состояния D. Обратный пересчет по направлению зеленых стрелок, при известной вероятности безопасного состояния D, позволяет уточнить вероятности свидетельств A, C, E, A и B.

Этот алгоритм распространения вероятности позволяет реализовать EM (Expectation - Maximisation) эффективного алгоритма построения вероятностных моделей, т.е. алгоритм обучения и уточнения структуры Байесовской сети при отсутствии на начальном этапе ее построения достаточного количества обучающих данных [12,14].

Предлагаемый вероятностный критерий безопасности позволяет использовать Байесовскую сеть и логистическую

регрессию для оценки вероятностей угроз и противодействия угрозам.

Байесовская сеть доверия обладает важными преимуществами по сравнению с классическими методами теории вероятностей при выявлении, идентификации и оценке значимости угроз [9]:

- представляет компактную по данным и объемам памяти вероятностную модель,
- более эффективная по времени вычислений,
- проще в получении и понимании информации,
- удобнее и проще в обучении на различных формах данных и при создании на основе экспертных данных.

Важнейшим этапом выявления и идентификации угроз является оценка успешности противодействия им имеющимися средствами и мероприятиями по обеспечению безопасности.

На практике такие оценки проводятся методами натуральных испытаний, имитационного и статистического моделирования. Данные, полученные по результатам этих мероприятий, обрабатываются методами математической регрессии и классификации.

Общепринятой является методика статистических испытаний и оценки искомых вероятностей успешных противодействий угрозам методами математической статистики. Это проводится по каждому виду угроз и соответствующих им мер и средств противодействия. Если же учесть ещё и комбинации угроз и мер противодействия, то задача становится объемной и математически трудноразрешимой. По этим причинам предпринимаются попытки найти наиболее простой и понятный метод ее решения.

В результате, предложено заменить метод статистического описания событий на метод классификации событий с оценкой вероятностей успешности и неуспешности мер защиты от угроз.

Одним из самых распространенных и удобных в применении является метод оценки логарифма шансов или логистической регрессии [13,14,15].

В частности, логистическая регрессия известный метод машинного обучения, применяемый при оценке информационной безопасности [9].

Для оценки вероятности успешного противодействия угрозам строится выборка размеченных данных. Экспертным путем, выбираются структура и тип угроз, параметры состояния защищаемой системы, набор предполагаемых мероприятий по противодействию им в виде строк записей соответствующей таблиц. Эти данные размечаются признаком успешности противодействия в виде единицы и неуспешности в виде ноля в специальной колонке таблицы. Из построенной и заполненной таблицы формируются и выделяются: бинарный вектор возможных угроз $\{u_i, i = 1 \dots N_u\}$, вектор показателей фазового состояния системы $\{y_j, j = 1 \dots N_y\}$ и бинарный вектор мероприятий и средств противодействия угрозам $\{x_k, k = 1 \dots N_k\}$. Где: N_u – число угроз, N_y – число фазовых состояний, N_k – число возможных мероприятий по противодействию угрозам.

На этих векторах строится расширенное пространство состояний классификации методом логистической регрессии

$$V = \{v_l, l = 1 \dots N_v\} = \{u_1, u_2, \dots, u_{N_u}, y_1, y_2, \dots, y_{N_y}, x_1, x_2, \dots, x_{N_x}\}, \quad (20)$$

где: $N_v = N_u + N_y + N_x$.

Вероятность успешного противодействия угрозам находится, из определения логистической регрессии, по формулам

$$P_o(V) = \frac{1}{1 + e^{-Q}}, \quad (21)$$

$$Q = b_s + \theta^T V, \quad (22)$$

где: θ^T – искомый, транспонированный вектор весовых коэффициентов регрессии, V – вектор из пространства регрессии, b_s – параметр смещения.

Алгоритм машинное обучение в логистической регрессии реализуется путем подбора вектора коэффициентов регрессии на обучающей выборке методом максимального правдоподобия функционала вероятности событий по схеме Бернулли

$$\theta^T = \arg \max_{\theta} \prod_{i=1}^{N_o} P_o \{s = s^{(i)} | v = v^{(i)}\}, \quad (23)$$

где: $P_o(s | v) = P_o(\theta^T V)^s \cdot (1 - P_o(\theta^T V))^{1-s}$ – распределение Бернулли от $P_o(Q_i)$, $s \in \{0, 1\}$, $s = 0$ – реализация угрозы, $s = 1$ – успешное отражение ее.

Вероятности начальных свидетельств возможных угроз вычисляются методом максимального правдоподобия апостериорной вероятности (10) по данным из размеченной таблицы наблюдаемых событий из жизненного цикла защищаемой системы с отметкой угрожающих событий $V = \{v_l, l = 1 \dots N_v\} = \{u_1, u_2, \dots, u_{N_u}\}$ и набора значений $\{s^{(i)}, v^{(i)}, i = 1 \dots N_v\}$ полученных по результатам реальных наблюдений и/или методом Монте-Карло [12, 15, 17].

Метод логистической регрессии позволяет решить задачу оценки успешности противодействия угрозам, но не пригоден для причинно-следственного анализа угроз, для которого, наиболее подходящими, будет использования Байесовских сетей доверия.

Методы и численные алгоритмы решения этих задач широко представлены в специальной литературе. Они реализованы в виде библиотек и модулей на Python, Scala, Julia и R [16, 19, 20].

Заключение

1. Для достижения высокой эффективности обеспечения безопасности в сфере разработки, производства и эксплуатации интеллектуальных бортовых систем и комплексов необходимо выявлять и прогнозировать внутренние и внешние угрозы.

2. Вероятностный критерий безопасности позволяет математически формализовать и решить задачу оптимального управления ею.

3. Принцип минимума суммарных затрат является необходимым и достаточным критерием оптимального управления безопасностью.

4. Байесовские сети позволяют значительно снизить объемы необходимых, статистических наблюдений и затраты на построение вероятностной модели угроз за счет исключения маловероятных событий и причинно-следственных связей между ними.

5. Байесовские сети доверия, в сочетании с алгоритмом машинного обучения, являются эффективным средством и технологией выявления, идентификации и прогнозирования угроз.

6. Метод классификации с помощью логистической регрессии позволяет оценить эффективность набора средств и операций по обеспечению противодействия внешним угрозам экономической безопасности с учетом внутреннего состояния защищаемого субъекта.

7. Многомерный вектор категориальных переменных, вычисленных методами эволюционных вычислений типа генетического отбора или алгоритма отжига является единственно возможным и достаточным решением задачи оптимизации безопасности.

8. Язык программирования Python с библиотеками Scikit-learn и TensorFlow, а для высоконагруженных и распределенных корпоративных или отраслевых систем, Scala или Julia являются достаточными средствами решения задачи оптимизации безопасности.

Литература

1. *Северцев Н.А., Бецов А.В.* Моделирование безопасности динамических систем: Научное издание. М.: ТЭИС, 2015.
2. *Косьяков А., Свит У.* и др. Системная инженерия. Принципы и практика. Перевод с английского. М.: ДМК Пресс, 2017.
3. *Гунина И.А., Посаженикова Ю.Н.* Система управления экономической безопасностью предприятия. ЭКОНОМИНФО. 2018. Т.15. № 1.
4. *Унижаев Н.В.* Управление экономической безопасностью организации. «ЛитРес: Самиздат», 2018, 345 с.
5. *Бьюиссон Ф.* Анализ поведенческих данных на R и Python / пер. с англ. А.В. Логунова. М.: ДМК Пресс 2022. 368 с.
6. *Воронин Е.А., Нгуен К.Т.* Выбор и обоснование критерия оценки и нормирования безопасности мероприятий и систем различного назначения. Научные технологии. 2018. Т.19. №4. С. 17-19.
7. *Дэн Саймон.* Алгоритмы эволюционной оптимизации / пер. англ. А.В. Логунова. М.: ДМК Пресс, 2020. 1002 с.
8. *Скобцов Ю.А., Сперанский Д.В.* Эволюционные вычисления. М.: Национальный открытый университет «ИНТУИТ», 2014.
9. *Луис Энрике Сукар.* Вероятностные и графовые модели. Принципы и приложения / пер. с английского А.В. Снастина. М.: ДМК Пресс, 2021. 338 с.
10. *Чюо К., Фримэн Д.* Машинное обучение и безопасность / пер. с англ. А.В. Снастина. М.: ДМК Пресс, 2020. 388 с.
11. *Voronin E.A., Kozlov S.V., Kubankov A.N.* Integrated control of economic security by machine learning in information in the information space of the digital economy // В сборнике: 2021 Systems of Signals Generating and Processing in the Field of on Board Communications, Conference Proceedings. 2021. С. 9416115.



12. *Voronin E.A., Kozlov S.V., Kubankov A.N.* Methodology for assessing the level of threats based on a limited set of data while ensuring the safety of on-board systems // В сборнике: 2022 Systems of Signals Generating and Processing in the Field of on Board Communications, SOSG 2022 - Conference Proceedings. 2022.

13. *Мэрфи К.П.* Вероятностное машинное обучение: введение / пер. с англ. А.А. Слинкина. М.: ДМК Пресс 2022. 940 с.

14. *Грас Д.* Data Science. Наука о данных с нуля: Пер. с англ. 2-е изд., перераб. и доп. СПб.: БХВ-Петербург, 2021. 416 с.

15. *Флах П.* Наука и искусство построения алгоритмов, которые извлекают знания из данных / пер. с англ. А.А. Слинкина. М.: ДМК Пресс, 2015. 400 с.

16. *Луис Энрике Сукар.* Вероятностные графовые модели. Принципы и приложения / пер. с англ. А.В. Снастина. М.: ДМК Пресс, 2021. 338 с.

17. *Ави Пфеффер.* Вероятностное программирование на практике / пер. с англ. А.А. Слинкина. М.: ДМК Пресс, 2017. 462 с.

18. *Chow C.K., Liu C.N.* Approximating discrete probability distributions with dependence trees // IEEE Trans. Inf. Theory 14, pp. 462-467, 1968.

19. *Pearl J.* Fusion, Propagation and structuring in belief networks. Artif. Intell. 29, pp. 241-288, 1986.

20. *Жерон Орельен.* Прикладное машинное обучение с помощью Scikit-Learn и TensorFlow: концепции, инструменты и техники для создания интеллектуальных систем: Пер. с англ. СПб.: ООО «Альфа-книга», 2018. 688 с.

21. *Рашка Себастьян, Мирджалили Вахид.* Python и машинное обучение: машинное и глубокое обучение с использованием Python, Scikit-learn и TensorFlow 2, 3-е изд.: Пер. с англ. СПб.: ООО «Диалектика», 2020. 848 с.

THREATS IDENTIFICATION BY SECURITY AND PROTECTION SELECTION BY MACHINE LEARNING METHODS

EVGENY A. VORONIN

Moscow, Russia

SERGEY V. KOZLOV

Moscow, Russia

ALEXANDER N. KUBANKOV

Moscow, Russia

ABSTRACT

Introduction. In the field of development and production of on-board information and communication systems and complexes, there is a steady trend towards the intensive introduction of new intelligent technologies that provide support for their operation within a single information space. This direction opens up wide opportunities for increasing the efficiency of using mobility aids for various purposes (transportation of goods, service personnel in emergency situations, etc.). At the same time, with the growth of the technological level of mobility aids, as well as their on-board systems and information interaction complexes, the horizons of new threats and poten-

KEYWORDS: *intelligent airborne systems industry, security, probabilistic security models, Bayesian belief networks, security threats, machine learning, maximum likelihood EM algorithm.*

tial dangers are simultaneously expanding, defining economic security as the basis for guaranteed development of this industry with minimal risks based on the use of promising intelligent technologies. **The following tasks are considered:** identifying the sources and nature of threats using the methods of naive Bayes and Bayesian trust networks to ensure security in the development, production and operation of on-board systems; selection of the optimal set of operations and measures of an organizational and technological nature, taking into account the expected costs or maximum security with restrictions on allowable costs. It is proposed to solve them by methods of machine learning and evolutionary optimization algorithms.

REFERENCES

1. Severtsev N.A., Betskov A.V. Modeling the safety of dynamic systems: Scientific publication. Moscow: TEIS 2015
2. Kosyakov A., Sweet U. et al. System engineering. Principles and practice. Translation from English. Moscow: DMK Press, 2017.
3. Gunina I.A., Posazhennikova Yu.N. System for managing the economic security of an enterprise. *ECONOMINFO*. 2018. Vol. No. 1.
4. Unizhaev N.V. Management of the economic security of the organization. "LitRes: Samizdat", 2018, 345 p.
5. Buisson F. Behavioral data analysis in R and Python / per. from English. A.V. Logunov. Moscow: DMK Press 2022. 368 p.
6. Voronin E.A., Nguyen K.T. Selection and substantiation of the criterion for assessing and standardizing the safety of measures and systems for various purposes. *Science-intensive technologies*. 2018. Vol.19. No. 4, pp. 17-19.
7. Dan Simon Algorithms for evolutionary optimization / translation from English. A.V. Logunov. Moscow: DMK Press, 2020. 1002 p.
8. Skobtsov Yu.A., Speransky D.V. Evolutionary calculations. Moscow: National Open University "INTUIT", 2014.
9. Luis Enrique Sucar. Probabilistic and graph models. Principles and applications / translation from English by A.V.Snastina. Moscow: DMK Press, 2021. 338 p.
10. Chio K., Freeman D. Machine learning and security / translation from eng. A.V. Snap. -M.: DMK Press, 2020. 388 p.
11. Voronin E.A., Kozlov S.V., Kubankov A.N. Integrated control of economic security by machine learning in information in the information space of the digital economy. *In the collection: 2021 Systems of Signals Generating and Processing in the Field of on Board Communications, Conference Proceedings*. 2021, pp. 9416115.
12. Voronin E.A., Kozlov S.V., Kubankov A.N. Methodology for as-sessing the level of threats based on a limited set of data while ensur-ing the safety of on-board systems. *In the collection: 2022 Systems of Signals Generating and Processing in the Field of on Board Communications, SOSG 2022 - Conference Proceedings*. 2022.
13. Murphy K.P. Probabilistic machine learning: an introduction / translation from English. A.A. Slinkin. Moscow: DMK Press 2022. 940 p.
14. Grace D. Data Science. Data science from scratch: Per. from English. 2nd ed., revised. And extra. St. Petersburg: BHV-Petersburg, 2021. 416 p.
15. Flach P. Science and art of constructing algorithms that extract knowledge from data / translation from English. A.A. Slinkin. Moscow: DMK Press, 2015. 400 p.
16. Luis Enrique Sucar. Probabilistic graph models. Principles and applications / translation from English. A.V. Snastina. Moscow: DMK Press, 2021. 338 p.
17. Avi Pfeffer. Probabilistic programming in practice / translation from English. A.A. Slinkin. Moscow: DMK Press, 2017. 462 p.
18. Chow C.K., Liu C.N. Approximating discrete probability distributions with dependence trees. *IEEE Trans. inf. Theory* 14, 462-467, 1968.
19. Pearl, J. Fusion, propagation and structuring in belief networks. *Artif. nIntel.* 29, pp. 241-288, 1986.
20. Geron, Aurelien Applied Machine Learning with Scikit-Learn and TensorFlw: Concepts, Tools and Techniques for Building Intelligent Systems. Translation from English. St. Petersburg: Alfa-kniga LLC, 2018. 688 p.
21. Raska Sebastian, Mirjalili Vahid. Python and Machine Learning: Machine and Deep Learning with Python, Scikit-learn, and TensorFlow 2, 3rd ed.: translation from English.SPb.: Dialectika LLC, 2020. 848 p.

INFORMATION ABOUT AUTHORS:

¹ Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, Moscow, Russia, e.voronin1@gmail.com

² Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, Moscow, Russia sv_kozlov@mail.ru

³ Moscow Technical University of Communications and Informatics, Moscow, Russia a.n.kubankov@mtuci.ru

For citation: Voronin E.A., Kozlov S.V., Kubankov A.N. Threats identification by security and protection selection by machine learning methods. H&ES Reserch. 2023. Vol. 15. No. 2. P. 49-56. doi: 10.36724/2409-5419-2023-15-2-49-56 (In Rus)



III КОНГРЕСС "СФЕРА"

XVI Международной навигационный форум и III конгресс "Сфера" состоятся 13 апреля 2023 года в Москве на территории ЦВК "Экспоцентр" на одной площадке с Российской неделей высоких технологий и экспозицией "Навитех-2023".

На пленарной сессии конгресса "Сфера возможностей. Сфера развития. Сфера влияния" Госкорпорацию "Роскосмос" представят генеральный директор, д.т.н. Борисов Юрий Иванович и исполнительный директор по перспективным программам и науке Блошенко Александр Витальевич. Госкорпорация "Роскосмос" обеспечивает реализацию государственной политики в области космической деятельности и ее нормативно-правовое регулирование, а также размещает заказы на разработку, производство и поставку космической техники и объектов космической инфраструктуры. В функции государственной корпорации также входит развитие международного сотрудничества в космической сфере и создание условий для использования результатов космической деятельности в социально-экономическом развитии России.

Национальную технологическую инициативу (НТИ) представит Песков Дмитрий Николаевич, специальный представитель Президента Российской Федерации по вопросам цифрового и технологического развития, генеральный директор АНО "Платформа НТИ". Национальная технологическая инициатива (НТИ) представляет собой объединение представителей бизнеса и экспертных сообществ. Она создана для поддержки перспективных направлений технологического бизнеса в России и увеличения в стране числа инновационных компаний, которые могут стать основой мировой экономики на период до 2035 г. Правительство РФ оказывает поддержку НТИ в рамках выпущенного в 2016 г. постановления "О реализации Национальной технологической инициативы".

На пленарной сессии выступит Первый заместитель председателя Комитета Государственной Думы по экономической политике, ответственный секретарь Бюро Высшего совета Партии "ЕДИНАЯ РОССИЯ", председатель Ко-

миссии Бюро Высшего совета Партии "ЕДИНАЯ РОССИЯ" по опережающему социально-экономическому и научно-технологическому развитию Кравченко Денис Борисович.

НТИ "Автонет" представит Гурко Александр Олегович, соруководитель рабочей группы НТИ "Автонет", председатель совета НП "ГЛОНАСС". Автонет – это рынок НТИ по развитию услуг, систем и современных транспортных средств на основе интеллектуальных платформ, сетей и инфраструктуры в логистике людей и вещей, эффективный инструмент на основе государственно-частного партнерства по поиску, отбору и выращиванию перспективных проектов в успешные высокотехнологические бизнесы мирового масштаба с целью обеспечения устойчивого роста национального ВВП, создания высококвалифицированных рабочих мест, обеспечения суверенитета в критически важных технологиях, укрепление национальной безопасности.

На мероприятии обсудят реализацию федерального проекта "Комплексное развитие космических информационных технологий "Сфера", использование телекоммуникационных, навигационных и геоинформационных технологий, а также продемонстрируют инновационные разработки отечественной ракетно-космической отрасли.

13 апреля 2023 г. участники Навигационного форума и Конгресса "Сфера" подведут итоги развития отрасли за 2022 год. Ведущие эксперты выступят с докладами о реализации проекта "Сфера", представители министерств и ведомств обсудят актуальные и планируемые к запуску профильные государственные программы поддержки навигационной и космической индустрии, руководители ключевых компаний рынка поделятся опытом и расскажут об имеющихся наработках и планах развития.

В 2022 г. на мероприятии зарегистрировалось более 1500 человек из шести стран мира. 75 спикеров выступили со своими докладами, а ключевые игроки рынка телекоммуникационных, навигационных и смежных технологий представили свои разработки.

Форум и конгресс проходят под эгидой Государственной корпорации по космической деятельности "Роскосмос".

Организатор Навигационного форума: Ассоциация "ГЛОНАСС/ГНСС-Форум"

Экспертные партнеры: НП "ГЛОНАСС" и НТИ "Автонет"

Стратегический партнер: АО "Организация "АГАТ"

Официальные партнеры: АО "ЦНИИмаш"

Партнеры: АО "Спутниковая система "Гонец", АО "ОКБ "Факел", SpaceTeam

Оператор события: агентство деловых коммуникаций "ПрофКонференции".

Организатор выставки "Связь-2023" и экспозиции "Навитех": АО "Экспоцентр" под патронатом Торгово-промышленной палаты Российской Федерации.

Российская неделя высоких технологий проходит при поддержке Министерства промышленности и торговли Российской Федерации, Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, Комитета по науке и высшему образованию Государственной Думы Федерального собрания Российской Федерации, Роскомнадзора и Министерства науки и высшего образования Российской Федерации.



Подробная информация на сайтах:
www.glonass-forum.ru; www.navitech-expo.ru

SMART CITY & REGION: ТЕХНОЛОГИИ, БЕЗОПАСНОСТЬ, ЭКОЛОГИЯ

2 марта 2023 г. в павильоне "Умный город" на ВДНХ в Москве при поддержке Министерства строительства и жилищно-коммунального хозяйства РФ состоялся X Федеральный форум по цифровизации городской среды "Smart City & Region: технологии, безопасность, экология", организованный Информационной группой ComNews.

Мероприятие проходило в гибридном формате и собрало в общей сложности 580 участников.

Также форум состоялся при поддержке Департамента информационных технологий города Москвы, Министерства цифрового развития и связи Кузбасса, Департамента цифрового развития города Севастополя, Правительства Забайкальского края, Администрации Костромской области, Администрации городов Курск, Мичуринск Тамбовской области и Курчатова Курской области и Франко-российской торгово-промышленной палаты.

Мероприятие поддержали профильные союзы, партнерства и ассоциации: АНО "Национальные приоритеты", Проект "Цифровая экономика", АНО "Цифровая экономика", АНО "Консорциум "Телекоммуникационные Технологии" (АНО ТТ), Некоммерческое Партнерство РУССОФТ, Ассоциация участников отрасли центров обработки данных (ЦОД), Ассоциация Содружество Волоконная оптика, Ассоциация Разработчиков Программных Продуктов "Отечественный софт" (АРПП "Отечественный софт"), Ассоциация больших данных (АБД), Общероссийское межотраслевое объединение работодателей "Российский Союз строителей", Общество цифровых управленцев яИТы, Университет ИТМО и Международная академия связи (МАС).

Генеральным партнером форума выступило ООО "ОТ-ЗВУК", официальными партнерами – Компания ТрансТелеКом (ТТК) и ПАО "Мобильные ТелеСистемы", партнерами сессии - АО "ИскраУралТЕЛ", ГК "ТРИАЛИНК", ООО "ВидеоМатрикс", Группа компаний ЦРТ, AT Consulting Восток и ООО "РЭЙДИКС".

В рамках форума прошла выставка отраслевых инновационных разработок и решений. Генеральными участниками выставки стали компании ENGY и ООО "Валамис" в составе Консорциума Интегра-С. Также приняли участие в качестве экспонентов компании: АО "ИскраУралТЕЛ", ГК "ТРИАЛИНК" и ООО "ОТЗВУК".

Пленарную сессию "От "Умного города" к "Умному региону" провел модератор Леонид Коник, генеральный директор – главный редактор, ООО "КомНьюс Груп".

Открыл форум с приветственным словом Константин Михайлик, заместитель министра, Министерство строительства и жилищно-коммунального хозяйства Российской Федерации. В своём обращении Константин Михайлик отметил: "Города и, самое главное, люди предъявляют все более высокие требования к качеству городской сре-

ды, поэтому решения не могут стоять на месте, их необходимо постоянно развивать". Замглавы Минстроя России призвал активнее применять уже апробированные в рамках проекта "Умный город" практики. В настоящее время в реализации проекта участвуют более 200 городов. "Любое решение для города интересно, когда оно широко тиражируется. Очень важно, чтобы эти решения были максимально удобны, экономичны и эффективны", – подчеркнул Константин Михайлик. Минстрой России готов оказывать регионам методическую и информационную поддержку.

Перед началом дискуссии установочный доклад "О реализации проекта от "Умного города" к "Умному региону" в Пермском крае" представил Алексей Черников, заместитель Председателя, Правительство Пермского края

В пленарной дискуссии приняли участие: Дарья Долгих, заместитель директора по направлению "Умный город", ФАУ "Проектная дирекция Минстроя России", Анатолий Курманов, заместитель руководителя рабочей группы Минстроя России по реализации проекта "Умный город", Дмитрий Онтоев, советник руководителя, Департамент информационных технологий города Москвы, Александра Осипова, директор, Департамент цифрового развития города Севастополя, Алексей Черников, заместитель Председателя, Правительство Пермского края, Кирилл Киреев, заместитель директора по развитию, АНО "Цифровая экономика", Роман Астанков, генеральный директор, ООО "Отзвук", Сергей Козерод, директор по развитию бизнеса на корпоративном и государственном рынке, АО "Компания ТрансТелеКом", Антон Салов, руководитель стратегии интернета вещей, ПАО "МТС".

В рамках сессии с докладом на тему: "Роль подсистемы оповещения АПК БГ в современных условиях. Актуальные вопросы" выступил Роман Астанков, генеральный директор, ООО "Отзвук".

Модератором сессии 1, посвященной поиску оптимальных источников финансирования "умных городов" и их элементов, стал также Леонид Коник, генеральный директор – главный редактор, ООО "КомНьюс Груп".

Партнером сессии стала компания AT Consulting Восток.

Свои доклады представили: Адель Славутин, директор, АНО "Центр компетенций Умный город" с темой: "Центр компетенций "Умный город", как продуктовый аутсорс офис, обеспечивающий оценку, тестирование и внедрение решений с привлечением средств поддержки"; Евгений Катаев, руководитель Центра информационного развития Пермского края, Министерство информационного развития и связи Пермского края, с темой: "Возможности привлечения финансирования по проекту "Умный город"; Владимир Высоцкий, генеральный директор, AT Consulting Восток с темой: "Больше нельзя меньше"; Анна Батуева, управляющий директор по юридическому сопровождению проектов, Национальный центр государственно-частного

партнерства с темой: "ГЧП для "Умных городов": текущее состояние, проблемы и перспективы"; Мария Озернова, руководитель сервиса "Городские запросы", ГБУ "Агентство инноваций Москвы" с темой: "Инновации в городской среде на практике: от планирования до внедрения. Грантовая поддержка технологического бизнеса", Андрей Казаков, генеральный директор, АО "ТКС" (подведомственная организация Администрации города Сарова) с докладом "Практический кейс г. Сарова по финансированию эксплуатации решений "Умного города" и Георгий Пчелинцев, партнер практики в области интеллектуальной собственности, информационных технологий и телекоммуникаций, Nextons с темой: "Правовые перспективы реализации ИТ проектов по модели ГЧП и концессий".

Тема сессии 2: "Инновационные технологии и решения для цифровизации городской инфраструктуры". Провел сессию Сергей Митягин, директор Института дизайна и урбанистики, Университет ИТМО.

Партнерами сессии выступили АО "ИскраУралТЕЛ" и ГК "ТРИАЛИНК".

Открыл сессию доклад Алексея Алексева, заместителя генерального директора, АО "ИскраУралТЕЛ": "Цифровая трансформация регионального и муниципального управления". Алексей Алексеев рассказал об опыте внедрения цифровых платформ проектов Безопасный город и Умный город. Было отмечено, эти проекты имеют базис для организационной и технологической унификации как на уровне муниципального образования, так на уровне субъекта РФ. Этот подход позволяет оптимизировать как количество создаваемых сервисов для функциональных пользователей систем, так затраты ресурсы (бюджетные, временные) на их создание. В его основе взято объектно-ориентированное проектирование с последующей реализацией в платформе конструирования бизнес-процессов. В качестве примера был представлен проект создания Комплексной информационной системы обеспечения безопасности жизнедеятельности и городского управления Кемеровской области.

Также с докладами выступили: Валерия Костюковская, заместитель председателя, Правительство Санкт-Петербурга Жилищный комитет с темой: "Методика оценки цифровой зрелости в исполнительных органах власти"; Андрей Шахраманьян, совладелец "СОДИС ЛАБ", член рабочей группы, Агентство стратегических инициатив (АСИ) с темой: "Цифровизация строительства и эксплуатации зданий"; Константин Созанский, технический руководитель направления "Марс-Мониторинг", ГК "ТРИАЛИНК" с темой: "Особенности современной цифровой трансформации процесса сбора, анализа и передачи измерений и сырых данных", Сергей Козерод, директор по развитию бизнеса на корпоративном и государственном рынке, АО "Компания ТрансТелеКом" с темой: "Комплексное инфраструктурное решение для многоквартирных домов". Сергей Козерод выступил со словами: "Большинство жилого фонда в РФ составляют многоквартирные дома, для обеспечения которых современными услугами сейчас применяется целый "зоопарк" решений от различных компаний, зачастую дублирующих друг друга и плохо совместимых

между собой. Единственный разумный выход из этой ситуации – это комплексное инфраструктурное решение, которое устроит как застройщиков и управляющие компании, так и собственников жилья, обеспечив единые системы безопасности и управления ЖКХ, высокоскоростной интернет и цифровое ТВ с высокими стандартами качества. Специалистами ТТК такие проекты уже реализованы в ряде городов, включая Томск, Новосибирск и Кемерово, показав свою эффективность и надежность. Отмечу, что такой подход подразумевает долгосрочное партнерство, а не одноразовые проекты "сделал и забыл".

Продолжила сессию Валерия Кузьминова, управляющая, визионер технологических трендов в сфере "Умных городов", ООО "Валамис" с докладом на тему: "Цифровые двойники городов: от концепции до промышленной эксплуатации" и Максим Чернов, заместитель директора по федеральному проекту "Информационная Инфраструктура", направление "Безопасная открытая инфраструктура", АНО "Цифровая экономика" с темой: "Телекоммуникационная инфраструктура для "Умных городов".

Сессию 3 "Интеллектуальное видеонаблюдение и видеоаналитика в интересах органов власти, бизнеса и общества. Интеллектуальные транспортные системы (ИТС) и беспилотный транспорт как элемент "Умного города" провел Антон Кураш, руководитель проекта Vision, ComNews.

Партнерами сессии выступили Группа компаний ЦРТ и ООО "РЭЙДИКС".

С докладами приняли участие: Андрей Хорошев, первый заместитель министра, Министерство информационного развития и связи Пермского края с темой: "Опыт реализации и эффекты от внедрения единой системы видеонаблюдения в Пермском крае";

Александра Осипова, директор, Департамент цифрового развития города Севастополя с темой: "Интеллектуальное видеонаблюдение в интересах органов власти, бизнеса и общества"; Андрей Хрулев, директор по бизнес-развитию направления биометрических систем, группа компаний ЦРТ с темой: "Интеллектуальное видеонаблюдение для обеспечения безопасности и комфорта горожан". Андрей Хрулев отметил: "Решения на базе компьютерного зрения, биометрии, речевых технологий доказали эффективность для создания комфортной и безопасной городской среды. Система компьютерного зрения "Визирь" используется уже в 270 проектах – на 150 объектах транспорта, более 20 – спорта, в 15 проектах "Безопасный город". Мы готовы масштабировать лучшие решения в регионах, в синергии развивая современные цифровые сервисы".

Продолжил сессию доклад Фариды Нигматуллиной, генерального директора, ООО "ВидеоМатрикс" с темой: "Видеоаналитика для диагностики цифрового биоритма города на благо органов власти, бизнеса, общества сегодня и завтра". "По опыту Videomatrix современная видеоаналитика на искусственном интеллекте и машинном зрении способна решить огромное количество задач. Обкатанная в ряде случаев до точности в 99,9% в промышленности, она становится все более доступной и для муниципалитетов на благо города, бизнеса и общества. Все разработанные методики идентификации, трекинга, нюансы работы с

математическими алгоритмами могут не только помогать сокращать миллионные издержки крупным предприятиям, но и улучшать качество жизни обычного российского человека, будь то вопрос контроля экологически опасной эмиссии в атмосферу или обеспечение безопасности людей на улицах города. Видеоаналитика уже очень скоро станет привычным явлением в городах России", – подытожил выступление Фарид Нигматуллин.

Также выступили: Алексей Казаков, Pre-sale Engineer, ООО "РЭЙДИКС" с темой: "ПО RAIDIX для построения быстрых программных СХД: российские алгоритмы на службе государства и бизнеса"; Василий Сазонов, заместитель министра – директор департамента транспорта, Министерство транспорта и дорожного хозяйства Тульской области с докладом об опыте внедрения интеллектуальной транспортной системы в Тульской городской агломерации; Родион Оконов, заместитель руководителя Дирекции развития интеллектуальной транспортной системы, ГКУ ЦОДД Москвы с темой: "Цифровой двойник дорог и наземного транспорта"; Юрий Фурлетов, доцент, эксперт ИЦ НТИ Автонет, Московский политехнический университет с темой: "Перспективы применения систем автономного вождения в городском общественном транспорте".

Модератором сессии 4 "Цифровые технологии в экологии и мониторинге окружающей среды" выступила Евгения Дмитриева, президент Союза поддержки и развития тех-

нологических компаний, советник председателя, Российское экологическое общество.

Партнером сессии стала компания ООО "ВидеоМатрикс".

Свои доклады представили: Евгения Дмитриева, президент Союза поддержки и развития технологических компаний, советник председателя, Российское экологическое общество с темой: "Применение отечественных ИТ-продуктов для решения задач экологической повестки", Константин Созанский, технический руководитель направления "Марс-Мониторинг", ГК "ТРИАЛИНК" с темой: "Современные подходы к контролю качества воды", Фарид Нигматуллин, генеральный директор, ООО "ВидеоМатрикс" с темой: "Vmx Dequs: ECO – машинное зрение для контроля видимой эмиссии в атмосферу", Андрей Плавич, руководитель Центра развития сетей и решений на базе устройств интернета вещей, ПАО "МТС" с темой: "Цифровые решения: от микроклимата к комплексному мониторингу окружающей среды", Дмитрий Андреев, начальник управления по экологии и природопользованию, Администрация города Перми с презентацией о цифровизации управления зеленым фондом города Перми.

ИГ ComNews благодарит всех партнеров, спикеров и участников форума #SmartCityandRegion2023!

При поддержке:

МИНСТРОЙ РОССИИ

ЦЕНТР КОМПЕТЕНЦИЙ УМНЫЙ ГОРОД

2.03.2023

Организатор: COMNEWS CONFERENCES

Smart City & Region

Генеральный партнер: ОТЗВУК

Официальные партнеры: ТТК. ТрансТелеКом, МТС

Партнеры сессий: ИСКРАУРАЛТЕЛ, ТРИАЛИНК, video matrix, ЦРТ, ГРУППА КОМПАНИЙ, AT Consulting Восток, RAIDIX

Генеральные участники выставки: Engy

При поддержке:

ЭКОНОМИ.А, ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ГОРОДА МОСКВЫ, Администрация города Курска, Правительство Забайкальского края, МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ И СВЯЗИ КУЗБАССА, Цифровой Сибирь, Администрация города Курганова Курской области, Администрация Костромской области, Администрация города Ижевска Ижевской области, ИТМО, РУС-СОФТ, ССИ FRANCE RUSSIE, АРПП, ЯИТЫ

XXVII МЕЖДУНАРОДНЫЙ ФОРУМ МАС`2023

В Москве в Центральном выставочном комплексе "Экспоцентр" 14 апреля 2023 г. состоялся XXVII Международный форум МАС-2023 "Цифровая трансформация во благо человека". Его организаторами стали Международная академия связи (МАС) и АО "Экспоцентр". Форум прошёл в рамках состоявшихся 11-14 апреля 2023 г. Российской недели высоких технологий и 35-й Международной выставки информационных и коммуникационных технологий "Связь-2023".

Главной целью Форума МАС-2023 было обсуждение теории и практики цифровых преобразований для достижения конечной цели – повышения уровня и качества жизни людей. В работе Форума приняли участие академики МАС, представители государственных структур и ведомств, Регионального содружества в области связи (РСС), правительства Москвы, профессиональных общественных объединений, ученые научно-исследовательских и образовательных учреждений, руководители и специалисты операторов связи, разработчики и провайдеры телекоммуникационных решений и информационных систем.

Открыла Форум президент МАС, председатель Совета по профессиональным квалификациям в области телекоммуникаций, почтовой связи и радиотехники А.П. Оситис. Прозвучали приветствия участникам Форума от руководителя фракции ЛДПР в Государственной Думе Российской Федерации Л.Э. Слуцкого, первого заместителя председателя комитета Государственной Думы по обороне А.А. Журавлева, генерального директора Исполнительного комитета РСС Н.Н. Мухитдинова, председателя Профсоюза работников связи России А.Г. Назейкина, заместителя руководителя Федерального агентства по управлению государственным имуществом Р.В. Шередина, заместителя руководителя Департамента информационных технологий г. Москвы А.В. Горбатько и др.

Обсуждены следующие вопросы:

– Цифровые технологии – одно из основных средств современного развития во всех сферах жизни и деятельности, позволяющее развивать производство, сферу услуг, удовлетворить растущие потребности в доступе к информационным ресурсам, к разнообразному контенту, реализовать личные качества, обеспечить возможность получения множества иных благ.

– Практика использования цифровых технологий в госуправлении, образовании, медицине, на транспорте и в промышленности, в создании "умных" домов, и городов.

– Актуальные цифровые технологии на современном этапе развития для людей: искусственный интеллект, большие данные, квантовые технологии, интернет вещей, новые коммуникационные технологии, развитие всеобщего интернета.

– Развитие современных телекоммуникаций, как основа цифровой экономики, в социальной сфере, в интересах всех групп населения. Формирование и совершенствование национального информационного пространства, информационная безопасность. Вопросы обеспечения надежной и бесперебойной работы цифровой среды, обеспечения суверенности электронных коммуникаций в условиях санкций.

– Вопросы стандартизации, разработки российских отраслевых норм, стандартов, компонентов, программного обеспечения и других продуктов импортозамещения. Мет-



рология и использование российских средств измерения, контроля и управления для сетей связи.

– Арктика: устойчивое развитие на базе цифровых технологий.

– Формирование технической политики и концепций развития цифровых технологий и благ для людей.

На пленарное заседание были представлены следующие доклады:

Годунов Игорь Валентинович, заведующий кафедрой Антикоррупционной деятельности и общественного противодействия РГСУ, доктор юридических наук:

"Антикоррупционное образование и просвещение в эпоху цифровой трансформации";

Федулова Ирина Вилисовна, президент Московского отделения МАС:

"Текущий этап и перспективы развития цифровой трансформации будущего";

Судовцев Владимир Антонович, президент Женевского отделения МАС, академик МАС:

"Цифровые технологии – ключ к своевременному предоставлению новых услуг электросвязи/ИКТ";

Абасбейли Сируз Гусейнович, президент Азербайджанского отделения МАС:

"Развитие цифровых технологий в Азербайджане";

Яковлев Роман Владимирович, заместитель генерального директора по развитию ИКТ-проектов в Арктической зоне АО "Атомдата":

"Развитие телекоммуникационной инфраструктуры в Арктической зоне России";

Мухитдинов Нурудин Насретдинович, генеральный директор Исполнительного комитета РСС, академик МАС:

"Перспективы в области цифрового будущего";

Папаскири Тимур Валикович, врио ректора Государственного университета по землеустройству, д.э.н., профессор:

"Цифровая трансформация землеустройства как основа использования инфокоммуникаций в России";

Ефимова Анастасия Олеговна, директор по развитию ООО "СтройГарант Инжиниринг", генеральный директор ООО "AllianceGT", член научно-делового совета Уполномоченного по защите прав предпринимателей Т.В.Минеевой:

"Импортозамещение и адаптация продуктов девелоперов к новым условиям: создание городов будущего, опираясь на уроки прошлого и прогнозируя новые вызовы. Применение технологий нейронных сетей при проектировании умного города или промышленных парков";

Козлов Викентий Александрович, генеральный директор ООО "ПармаТел", академик МАС:

"Телекоммуникация в Арктике – настоящее и будущее";

Ефимов Сергей Павлович, генеральный директор НКО "Ассоциация операторов телефонной связи":

"От олигополии нескольких операторов к общегосударственной сети связи по единым правилам для рационального, пропорционального и эффективного развития всех сфер экономики страны в условиях внешних ограничений";

Григорьев Олег Александрович, председатель Российского национального комитета по защите от неионизирующих излучений, д.б.н., Кучма Владислав Ремирович, научный руководитель, член-корреспондент РАН, Институт комплексных проблем гигиены ФБУН "ФНЦ гигиены им. Ф.Ф. Эрисмана" Роспотребнадзора, д.м.н.:

"Об основных проблемах биомедицинского и гигиенического обеспечения электромагнитной безопасности населения в связи с реализацией дорожной карты по современным и перспективным сетям мобильной связи";

Шуб Виталий Элконович, руководитель Лидирующего Исследовательского центра 5G, Сколковский институт науки и технологий, академик МАС:

"Ключевые вопросы развития национальной широкополосной телекоммуникационной инфраструктуры";

Мачкин Петр Иванович, советник Международного Конгресса промышленников и предпринимателей, советник Международной академии транспорта:

"Формула социальной справедливости и её применение для расчета объективных и справедливых значений зарплат работников в отрасли связи Российской Федерации";

Свечникова Наталья Викторовна, к.ю.н., доцент кафедры гражданско-правовых дисциплин ФГБОУ ВО "РЭУ им. Г.В. Плеханова",

Гурко Антон Владимирович, к.ю.н., старший преподаватель кафедры гражданско-правовых дисциплин ФГБОУ ВО "РЭУ им. Г.В. Плеханова":

"Актуальные проблемы совершенствования законодательства о цифровых правах";

Воротилина Татьяна Викторовна, к.ю.н., доцент кафедры гражданско-правовых дисциплин ФГБОУ ВО "РЭУ им. Г.В. Плеханова",

Свечников Владимир Александрович, старший преподаватель кафедры гражданско-правовых дисциплин

ФГБОУ ВО "РЭУ им. Г.В. Плеханова":

"Развитие правового регулирования оборота цифровых прав в Российской Федерации";

Ефимова Ольга Александровна, аспирант Института законодательства и сравнительного правоведения при Правительстве Российской Федерации, старший преподаватель кафедры гражданско-правовых дисциплин ФГБОУ ВО "РЭУ им. Г.В. Плеханова":

"Правовой обычай в Интернете: вопросы теории и практики";

Новикова Галина Викторовна, доцент кафедры истории и философии образования МГУ имени М.В. Ломоносова:

"Понятийное мышление школьников - необходимое условие развития культуры цифровой коммуникации";

Чекаданова Мария Владимировна, филиал РТУ МИРЭА в г. Фрязино, доцент:

"Практика инфокоммуникаций в области обучения при внедрении продуктов цифрового производства";

Козадаева Любовь Анатольевна, ФГБУ НИИР, ведущий инженер:

"Регулирование и практика использования телефонных номеров в цифровой среде";

Парадеев Василий Андреевич, представитель АО "ИскраУралТЕЛ":

"Практическое применение цифровых, облачных технологий, 5G, IMS для быстрого запуска услуг в сетях связи нового поколения".

Вызвали интерес доклады, представленные в ходе работы секций "Цифровая метрология – необходимая составляющая цифровой трансформации", "Телекоммуникации в Арктике – настоящее и будущее", "Подготовка кадров для достижения технологического суверенитета высокотехнологичных отраслей".

На секции, образованной во исполнение Указов Президента России "О проведении в Российской Федерации Года педагога и наставника", "О праздновании 80-летия разгрома советскими войсками немецко-фашистских войск в Сталинградской битве" и его поручения о праздновании 80-летия полного снятия блокады Ленинграда, с сообщениями выступили ветераны связи, наставники молодежи, профессионалы и педагоги:

Назейкин Анатолий Георгиевич, председатель Профсоюза работников связи Российской Федерации, президент



Ассоциации профсоюзов транспорта и связи Российской Федерации. Активно работает в составе Российской трехсторонней комиссии по регулированию социально-трудовых отношений. Член совета директоров АО "Почта России". С 2000 года – доверенное лицо Президента Российской Федерации Владимира Владимировича Путина. Кандидат экономических наук, академик, вице-президент МАС. Имеет почётные звания "Мастер связи" и "Заслуженный связист России", награждён орденом Александра Невского, орденом "За заслуги перед Отечеством" IV степени и орденом Дружбы, награждён медалями "За освоение целинных земель", "За трудовую доблесть" и др.

Крупнов Александр Евгеньевич, академик МАС. Российский государственный деятель, председатель Государственного комитета Российской Федерации по связи и информатизации с 25 марта 1997 г. по 29 мая 1999 г. Кандидат технических наук. Имеет почётные звания "Мастер связи" и "Заслуженный работник связи Российской Федерации", награждён государственными и ведомственными наградами.

Ерохин Сергей Дмитриевич, академик МАС, ректор Московского технического университета связи и информатики. Доцент, кандидат технических наук. Имеет более 100 научных публикаций, награжден ведомственными наградами. В сферу научных интересов входят: информационная безопасность и критические информационные инфраструктуры, телекоммуникационные технологии и сети. Руководитель Комитета по профессиональному образованию Совета по профессиональным квалификациям в области телекоммуникаций, почтовой связи и радиотехники. Член Совета по развитию цифровой экономики при Совете Федерации Федерального Собрания Российской Федерации.

Муханов Андрей Юрьевич, академик МАС, проректор по молодёжной политике и воспитательной работе Московского технического университета связи и информатики. Награжден государственными и ведомственными наградами, присвоено звание "Почетный радист". Вел работу по организации деятельности российских делегаций в Международном союзе электросвязи и Всемирном почтовом союзе, по осуществлению взаимодействия с администрациями связи других стран. Действительный государственный советник Российской Федерации 3-го класса.

Мишенков Сергей Львович, академик МАС, доктор технических наук, профессор. Награжден государственными

и ведомственными наградами, присвоены почётные звания "Мастер связи" и "Почетный радист". Вел работу по защите международных интересов России в Международном союзе электросвязи. В сферу научных интересов входят проблемы дистанционного высшего образования связистов России, изучение влияния обработки сигналов на эмоциональное воздействие передачи звукового и телевизионного вещания. Имеет более 10 авторских свидетельств и более 250 научных публикаций. Государственный советник Российской Федерации 1-го класса.

Свечникова Наталья Викторовна, доцент, кандидат юридических наук, доцент ВАК, Член экспертного совета при Комитете Государственной Думы Российской Федерации по экономической политике, промышленности, инновационному развитию и предпринимательству. Входит в состав рабочей группы комиссии по правовым аспектам Союзного государства и Евразийского экономического союза Ассоциации юристов России и Белорусского республиканского Союза юристов. Автор более 170 научных публикаций, учебников и монографий. Стаж преподавательской деятельности 30 лет.

Воловик Александр Михайлович, вице-президент Российской академии естественных наук, доктор экономических наук, профессор, лауреат Государственной премии Российской Федерации в области культуры, лауреат международной Премии "Лидер инновации", президент Российского союза неправительственных организаций "Отечество", главный редактор журнала "Честь Отечества", лауреат премии Союза журналистов России "Золотое перо", член Союза писателей России, лауреат премии Союза писателей России "Верные сыны Отечества", президент Некоммерческой организации "Благотворительный фонд знака ордена святого Александра Невского "За труды и Отечества". Автор исторических книг "Ради жизни на земле", "Сказание о государстве Российском", "Александр Невский. Святой защитник земли Русской".

Всем желающим была предоставлена возможность стать участником Всероссийской акции "Письмо солдату" – "Подари тепло Защитнику Отечества".

В ходе Форума подведены итоги и проведено награждение лауреатов ежегодно проводимого МАС молодежного конкурса цифрового развития, инноваций и инновационных проектов "Новое поколение 2022/2023".



организаторы:
RUSSIA SECTION ED/MTT/AES JOINT CHAPTER
RUSSIA SECTION CAS CHAPTER
INSTITUTE OF RADIO AND INFORMATION SYSTEMS ASSOCIATION (IRIS)

МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ
**“2023 Systems of Signal Synchronization, Generating
and Processing in Telecommunications”**
SYNCHROINFO

28 – 30 июня 2023
г. Псков, Россия

The papers which are discussed at the conference can be divided into the following chapters:

- 1) Synchronization Systems and Devices;**
- 2) Signal Generating and Shaping Devices;**
- 3) Signal Processing Devices.**
- 4) Special chapter: “Problems of microwave electronics” named after V.A. Solntsev**
- 5) Photonics and mathematics for moving objects**



All accepted and presented Papers following the conference will be submitted for inclusion into IEEE Xplore

Materials are available in English

<http://media-publisher.ru/en/conference/>